

**School of Information Systems**

**A Socio-Technical Security Risk Assessment Methodology for  
Information Systems Access**

**Wedige Hasala Peiris**

**This thesis is presented for the Degree of  
Doctor of Philosophy  
of  
Curtin University**

**June 2014**



## Declaration

To the best of my knowledge and belief this thesis contains no material previously published by any other person except where due acknowledgment has been made.

This thesis contains no material which has been accepted for the award of any other degree or diploma in any university.

Signature:  .....

Date: 17/06/2014 .....

## Table of Contents

<b>List of Figures.....</b>	<b>vi</b>
<b>List of Tables.....</b>	<b>xii</b>
<b>Abstract.....</b>	<b>xiii</b>
<b>Acknowledgements .....</b>	<b>xiv</b>
<b>1. Introduction.....</b>	<b>1</b>
1.1 Significance of the Insider Threat Problem to the Information Systems Security Discipline .....	2
1.2 Key Terms and Definitions.....	3
1.2.1 Information Systems Security.....	3
1.2.2 Information Security Threats and Vulnerabilities.....	3
1.2.3 Information systems security risks .....	4
1.2.4 Insider Threat .....	4
1.2.5 Information Systems Access and Access Control .....	6
1.3 Research Approach.....	6
1.3.1 Research Topic and the Objective .....	6
1.3.2 Overview of the research method.....	8
1.4 Structure of this Thesis.....	9
<b>2. Literature Review.....</b>	<b>10</b>
2.1 Socio-Technical Aspects of Information Systems Security .....	11
2.1.1 Socio-technical aspects of information systems .....	11
2.1.2 Socio-technical nature of problems in the information systems security domain .....	17
2.2 Information System Access – Models and Principles .....	22
2.2.1 Access Authorisation Principles.....	23
2.2.2 Access Control Models .....	26
2.3 Information Systems Security Risk Assessment .....	37
2.3.1 Information systems security risk assessment standards .....	37
2.3.2 Information systems security risk analysis models .....	40
2.3.3 Information systems security risk analysis methods .....	49
2.3.4 Information systems security risk assessment metrics .....	51
2.4 Conclusions.....	52
2.4.1 Summary and the Research Gap .....	52
2.4.2 Applicable models from other disciplines and research directions.....	53
<b>3. Research Methodology .....</b>	<b>56</b>
3.1 Research Questions and Objectives .....	56
3.2 Research Paradigm .....	57
3.2.1 Rationale for the use of design science as the research paradigm .....	57
3.2.2 Additional design science research requirements.....	60

3.3	Research Process Models.....	63
3.3.1	Design science research process models.....	63
3.3.2	Stages of the research project.....	67
3.4	Research Evaluation.....	70
3.4.1	Activity 4: Evaluate initial artefacts (first evaluation).....	71
3.4.2	Activity 7: Evaluate artefacts (final evaluation).....	71
3.5	Chapter Summary.....	72
<b>4.</b>	<b>Data Collection Methods.....</b>	<b>73</b>
4.1	Collection of Socio-Technical Threat Event Data.....	73
4.2	Collection of Organisational Data for Artefact Testing.....	86
4.2.1	Selection of Organisations.....	86
4.2.2	Overview of Organisations.....	87
4.2.3	Data collection methods.....	89
4.3	Collecting Professional Opinions on the Artefacts.....	93
4.4	Chapter Summary.....	93
<b>5.</b>	<b>The Risk Assessment Model, Metrics and Method.....</b>	<b>95</b>
5.1	Insider Threats and Related Socio-technical Access Risks.....	95
5.2	The Risk Assessment Model.....	97
5.2.1	Modelling important entity types and relationships between them.....	97
5.2.2	Modelling intrinsic risk characteristics of entities.....	99
5.2.3	Diagrammatic representation of the Risk Assessment Model.....	105
5.3	Metrics for the assessment of risks occurring due to information resource access authorisations.....	106
5.3.1	Employee having exclusive access to information resources.....	106
5.3.2	Employee having exclusive administrative access to information resources.....	112
5.3.3	Employee having access to resources not required for their tasks.....	115
5.3.4	Employee has access to two dependent information resources.....	119
5.4	Metrics for the assessment of risks occurring due to task assignments.....	126
5.4.1	Employee exclusively assigned to tasks.....	126
5.4.2	Employee performs two dependent tasks.....	130
5.5	Metrics for the assessment of risks occurring due to knowledge requirements.....	133
5.5.1	Employee having exclusive knowledge to operate an information resource.....	133
5.5.2	Employee having exclusive knowledge to perform a task.....	139
5.6	Metrics for the assessment of risks occurring due to social relationships combined with resource authorisations or task assignments.....	142
5.6.1	An employee has indirect access to information resources.....	142

---

5.6.2	An employee has transitive access to dependent information resources .....	148
5.6.3	An employee obtains transitive assignment to dependent tasks .....	153
5.6.4	A closely associated group of employees control a resource.....	156
5.6.5	A closely associated group of employees perform a task .....	158
5.7	Discussion and Summary of Metrics .....	160
5.8	Risk Assessment Method.....	175
5.8.1	Risk assessment activities carried out in the research .....	175
5.8.2	Risk assessment method recommended for the security professionals.....	177
5.9	Chapter Summary.....	177
<b>6.</b>	<b>Assessment and Visualisation of Risks .....</b>	<b>179</b>
6.1	Analysis workflow and tools used .....	179
6.2	Assessment of risks due to resource access authorisations.....	180
6.2.1	Risks due to agents having exclusive access to resources.....	180
6.2.2	Risks due to agents having exclusive privileged access to resources .....	185
6.2.3	Risks due to agents having access to resources not required for the tasks.....	191
6.2.4	Risks due to agents having access to two dependent information resources .....	196
6.3	Assessment of risks due to task assignments.....	201
6.3.1	Risks due to agents performing tasks exclusively.....	202
6.3.2	Risks due to agents performing two dependent tasks .....	207
6.4	Assessment of risks due to knowledge requirements.....	214
6.4.1	Risks due to agents having exclusive knowledge to operate an information resource.....	214
6.4.2	Risks due to agents having exclusive knowledge to perform a task.....	219
6.5	Assessment of risks due to social relationships combined with resource authorisations or task assignments.....	225
6.5.2	Risks due to agents having indirect access to information resources .....	228
6.5.3	Risks due to agents having transitive access to dependent information resources .....	241
6.5.4	Risks due to agents obtaining transitive assignment to dependent tasks.....	249
6.5.5	Risks due to closely associated group of agents controlling a resource.....	257
6.5.6	Risks due to a closely associated group of agents performing a task .....	261
6.6	Summary and Discussion of the Results.....	266
6.6.1	Risks occurring due to resource access authorisations .....	266
6.6.2	Mitigation of risks occurring due to resource access authorisations .....	269
6.6.3	Risks occurring due to task assignments .....	270

---

6.6.4	Mitigation of risks occurring due to task assignments .....	270
6.6.5	Risks occurring due to knowledge requirements .....	272
6.6.6	Mitigation of risks occurring due to knowledge requirements .....	272
6.6.7	Risks occurring due to social relationships combined with resource authorisations or task assignments .....	273
6.6.8	Mitigating risks occurring due to social relationships combined with resource authorisations or task assignments .....	278
6.7	Chapter Summary .....	279
<b>7.</b>	<b>Evaluation and Conclusions .....</b>	<b>281</b>
7.1	Evaluation carried out by Information Security Professionals.....	281
7.1.1	Background of the Evaluators.....	281
7.1.2	Evaluation of the results produced by following the methodology .....	283
7.1.3	Evaluation of the risk assessment model .....	287
7.1.4	Evaluation of the risk assessment method.....	290
7.1.5	Evaluation of the risk assessment metrics.....	291
7.1.6	Discussion of the evaluators' Opinions.....	292
7.2	Evaluation Using the Three Case Studies .....	295
7.2.1	Evaluation of the results produced by applying the methodology.....	295
7.2.2	Evaluation of the risk assessment model .....	296
7.2.3	Evaluation of the risk assessment method.....	297
7.2.4	Evaluation of the risk assessment metrics.....	299
7.3	Compatibility with Existing Risk Assessment Standards and Frameworks.....	299
7.4	Research Summary and Conclusions .....	306
7.5	Limitations of the Research .....	307
7.6	Future Research .....	309
7.7	Research Contributions.....	312
7.7.1	Theoretical contributions of the research .....	312
7.7.2	Practical contributions of the research .....	313
	<b>References .....</b>	<b>315</b>
	<b>Appendix A.....</b>	<b>334</b>
	<b>Appendix B .....</b>	<b>339</b>

# List of Figures

Figure 1-1: Arrangement of chapter sub-topics.....2

Figure 1-2: Topics and concepts covered in the thesis and relationships between them .....7

Figure 2-1: Arrangement of chapter sub-topics.....10

Figure 2-2: Socio-Technical Systems (STS) model of to Bostrom and Heinen (1977b) .....12

Figure 2-3: Topics in information systems access .....22

Figure 2-4: Different implementations of Separation of Duty according to Simon and Zurko (1997).....25

Figure 2-5: Example for Denning’s (1976) Lattice Model of Information Flow .....28

Figure 2-6: Role Based Access Control (RBAC) based on Ferraiolo and Kuhn (1992) .....31

Figure 2-7: Basic ABAC Model as defined in NIST SP 800-162 (Hu et al. 2014).....33

Figure 2-8: Example risk-matrix given in NIST SP 800-30 Revision 1 (National Institute of Standards and Technology 2012) .....40

Figure 2-9: An example Attack Tree illustrated by Ray and Poolsapassit (2005) .....41

Figure 2-10: Example SCADA fault-tree illustrated by Lewis (2006, 232) .....42

Figure 2-11: Example Privilege Graph illustrated by Dacier et al. (1996).....43

Figure 3-1: Arrangement of chapter sub-topics.....56

Figure 3-2: Design science research process model proposed by Vaishnavi and Kuechler (2004).....63

Figure 3-3: Design science research process model proposed by Peffers et al. (2008, 54) .....64

Figure 3-4: Design science research process model proposed by Venable (2006b, 17) .....65

Figure 4-1: Arrangement of chapter sub-topics.....73

Figure 5-1: Arrangement of chapter sub-topics.....95

Figure 5-2: Causes of Socio-technical Access Risks .....96

Figure 5-3: Diagram illustrating the entities, relationships and intrinsic risk properties of entities (attributes) of the risk assessment model. ....105

Figure 5-4: A simple example to demonstrate the ERA metric.....106

Figure 5-5: A simple example to demonstrate the VNA metric .....116

Figure 5-6: A simple example to demonstrate the ADR metric .....120

Figure 5-7: A simple example used to illustrate ETA metrics.....127

Figure 5-8: A simple example used to illustrate the ADT metrics .....130

Figure 5-9: Simple example used to demonstrate EKR metrics .....134

Figure 5-10: A simple example used to demonstrate EKT metrics .....139

Figure 5-11: A simple example used to illustrate IAC metrics.....144

Figure 5-12: A simple example to demonstrate TAR metrics.....149

---

Figure 5-13: A simple example used to illustrate TAT metrics .....	154
Figure 5-14: Example used to illustrate the ACR metrics .....	157
Figure 5-15: Simple example used to demonstrate ACT metric.....	159
Figure 5-16: The risk assessment activities followed in the research and the assessment method recommended for information security professionals .....	176
Figure 6-1: Arrangement of chapter sub-topics .....	179
Figure 6-2: Information resources that score top-five ERA( $r_j$ ) values in Organisations 1,2 and 3 .....	180
Figure 6-3: Agents who score top-five ERA( $a_i$ ) values of organisations 1,2 and 3 .....	182
Figure 6-4: Heat-map representations of the exclusive access risks per resource access authorisation of the three organisations. ....	183
Figure 6-5: Resource access networks of the three organisations.....	184
Figure 6-6: EAA( $r_j$ ) metric scores of information resources of organisations 1, 2 and 3.....	186
Figure 6-7: EAA( $a_i$ ) values of agents of organisations 1, 2 and 3.....	187
Figure 6-8: Heat-map representations of exclusive privileged access risks per resource access authorisation of the three organisations.....	188
Figure 6-9: Resource access networks of the three organisations only showing the privileged access authorisations. ....	190
Figure 6-10: VNA( $a_i$ ) metric scores of agents in Organisations 1, 2 and 3 .....	191
Figure 6-11: Heat-map representations of risks due to agents having access to resources not required for their tasks. ....	193
Figure 6-12: Multi-partite networks of Organisations 1, 2 and 3 consisting of agent, resource and task nodes. ....	194
Figure 6-13: Multipartite networks illustrating resource access authorisations and task assignments of three agents receiving high VNA( $a_i$ ) risk scores.....	195
Figure 6-14: ADR( $a_i$ ) metric scores of agents of Organisation 1,2 and 3.....	196
Figure 6-15: Bipartite networks of Organisations 1, 2 and 3 consisting of agent and resource nodes. ....	198
Figure 6-16: Heat-map representations of risks due to agents having access dependent information resources. ....	200
Figure 6-17: Selected sub-graphs from Organisation 1,2 and 3.....	201
Figure 6-18: ETA( $t_p$ ) values of the tasks receiving the top-five metric scores in organisations 1, 2 and 3.....	202
Figure 6-19: The top-ten ETA( $a_i$ ) risk scores of the agents in Organisations 1,2 and 3.....	203
Figure 6-20: Heat-map representations of the exclusive task assignment risks of Organisations 1, 2 and 3. ....	205
Figure 6-21: Task assignment networks of the three organisations. ....	206
Figure 6-22: ADT( $a_i$ ) risk values of the agents in organisations 1,2 and 3.....	207

Figure 6-23: Heat-map representations of the dependent task assignment risks of Organisations 1 and 2. ....	208
Figure 6-24: Heat-map representations of the dependent task assignment risks of Organisation 3.....	209
Figure 6-25: Task assignment networks of the three organisations. ....	210
Figure 6-26: Selected sub-networks of Organisation-1 illustrating task assignment and task dependency links related to the tasks (i) <i>AP-Inv</i> (ii) <i>AP-Pay</i> and (iii) <i>CM-B</i> . ....	211
Figure 6-27: Selected sub-networks of Organisation-2 illustrating task assignment and task dependency links related to the tasks (i) <i>Grn</i> and (ii) <i>Issue Crd</i> . ....	212
Figure 6-28: Selected sub-networks of Organisation-3 illustrating task assignment and task dependency links related to the tasks (i) <i>Inv &amp; Rcn</i> and (ii) <i>Backup</i> .....	213
Figure 6-29: Top-five $EKR(a_i)$ risk values of the agents in organisations 1,2 and 3. ....	215
Figure 6-30: Heat-map representations of the risks due to agents having exclusive knowledge to utilise resources of Organisations 1, 2 and 3. ....	216
Figure 6-31: Network diagrams representing Agent $\rightarrow$ Resource, Agent $\rightarrow$ Knowledge and Resource $\rightarrow$ Knowledge networks of the three organisations. ....	218
Figure 6-32: The sub-networks visualising the resource access relationships that score high $EKR(a_i, r_j)$ scores in Organisations 2 and 3. ....	219
Figure 6-33: Top-ten $EKT(a_i)$ risk values of the agents in organisations 1,2 and 3.....	220
Figure 6-34: Heat-map representations of the risks due to agents having exclusive knowledge to perform tasks of Organisations 1, 2 and 3. ....	221
Figure 6-35: Network diagrams representing Agent $\rightarrow$ Task, Agent $\rightarrow$ Knowledge and Task $\rightarrow$ Knowledge networks of the three organisations. ....	223
Figure 6-36: The sub-networks visualising the task assignments that score high $EKT(a_i, t_p)$ scores in the three Organisations.....	224
Figure 6-37: $IAC(a_i)$ metric scores of the agents in three organisations calculated using the formal reporting relationships .....	229
Figure 6-38: Heat-map representations of the $IAC(a_i, r_j)$ scores of all agent, resource combinations in Organisations 2 and 3 calculated considering the formal reporting relationships. ....	230
Figure 6-39: Sub-networks illustrating the shortest resource access pathways of agents - <i>Jnr. Mgr. Pol</i> and <i>Snr. Mgr. 1</i> in Organisation-2. ....	231
Figure 6-40: Agents receiving the top-ten $IAC(a_i)$ metric scores in the three organisations (calculated using advice relationships) .....	232
Figure 6-41: Heat-map representations of the $IAC(a_i, r_j)$ scores of all agent, resource combinations in three organisations calculated considering the advice relationships. ....	233
Figure 6-42: Sub-networks illustrating the shortest resource access pathways of three agents who have high indirect access potential through the advice networks.....	234
Figure 6-43: Agents receiving the top-ten $IAC(a_i)$ metric scores in the three organisations (calculated using the information exchange relationships) .....	235

Figure 6-44: Heat-map representations of the $IAC(a_i, r_j)$ scores of all agent, resource combinations in three organisations calculated considering the information exchange relationships. ....	236
Figure 6-45: Sub-networks illustrating the shortest resource access pathways of three agents who have high indirect access potential through the information exchange networks. ....	237
Figure 6-46: Agents receiving the top-ten $IAC(a_i)$ metric scores in the three organisations (calculated using the friendship links between agents) .....	238
Figure 6-47: Heat-map representations of the $IAC(a_i, r_j)$ scores of all agent, resource combinations in three organisations calculated considering the friendship links. ....	239
Figure 6-48: Sub-networks illustrating the shortest resource access pathways of two agents who have high indirect access potential through the information exchange networks. ....	240
Figure 6-49: Sub-networks illustrating the transitive access to dependent resource risks via the formal reporting networks of Organisations 2 and 3. ....	242
Figure 6-50: Agents receiving non-zero $TAR(a_i)$ metric scores in the three organisations (calculated using the advice relationships between agents) .....	243
Figure 6-51: Heat-map representations of the $TAR(a_i, r_j)$ scores of all agent, resource combinations in organisations 1 and 2 calculated considering the advice relationships. ....	243
Figure 6-52: Example from Organisation-2 illustrating the transitive access to dependent information resources. ....	244
Figure 6-53: Agents receiving non-zero $TAR(a_i)$ metric scores in the three organisations (calculated using the information exchange relationships between agents) .....	245
Figure 6-54: Heat-map representations of the $TAR(a_i, r_j)$ scores of all agent, resource combinations in three organisations calculated considering the information exchange relationships. ....	246
Figure 6-55: Agents receiving non-zero $TAR(a_i)$ metric scores in the three organisations (calculated using the friendship networks in organisations) .....	247
Figure 6-56: Heat-map representations of the $TAR(a_i, r_j)$ scores of all agent, resource combinations in three organisations calculated considering the friendship networks. ....	248
Figure 6-57: Agents receiving non-zero $TAT(a_i)$ metric scores in the three organisations (calculated using the formal reporting relationships) .....	249
Figure 6-58: Heat-map representations of the $TAT(a_i, t_p)$ scores of all agent, task combinations in three organisations calculated considering formal reporting networks. ....	250
Figure 6-59: Agents receiving non-zero $TAT(a_i)$ metric scores in the three organisations (calculated using the advice relationships) .....	251
Figure 6-60: Heat-map representations of the $TAT(a_i, t_p)$ scores of all agent, task combinations in three organisations calculated considering advice networks. ....	252

Figure 6-61: Agents receiving non-zero $TAT(a_i)$ metric scores in the three organisations (calculated using the information exchange networks) .....	253
Figure 6-62: Heat-map representations of the $TAT(a_i, t_p)$ scores of all agent, task combinations in three organisations calculated considering information exchange networks. ....	254
Figure 6-63: Agents receiving non-zero $TAT(a_i)$ metric scores in the three organisations (calculated using the friendship networks) .....	255
Figure 6-64: Heat-map representations of the $TAT(a_i, t_p)$ scores of all agent, task combinations in three organisations calculated considering friendship networks. ....	256
Figure 6-65: Information resources receiving non-zero $ACR(r_j)$ metric scores in the three organisations (calculated using the information exchange networks) .....	257
Figure 6-66: Sub-networks illustrating resource access and information exchange links related to three resources that score high $ACR(r_j)$ values. ....	258
Figure 6-67 : Information resources receiving non-zero $ACR(r_j)$ metric scores in the three organisations (calculated using the friendship networks) .....	259
Figure 6-68: Sub-networks illustrating resource access and friendship links related to three resources that score high $ACR(r_j)$ values. ....	260
Figure 6-69: Tasks receiving non-zero $ACT(t_p)$ metric scores in the three organisations (calculated using the information exchange networks) .....	262
Figure 6-70: Sub-networks illustrating task assignment and information exchange links related to three tasks that score high $ACT(t_p)$ values. ....	263
Figure 6-71: Tasks receiving non-zero $ACT(t_p)$ metric scores in the three organisations (calculated using the friendship networks) .....	264
Figure 6-72: Sub-networks illustrating task assignment and friendship links related to three tasks that score high $ACT(t_p)$ values. ....	265
Figure 6-73: The risk score variations among resource access authorisations (agent $\rightarrow$ resource) receiving the top-ten risk values for the three metrics – (i) $ERA(a_i, r_j)$ , (ii) $VNA(a_i, r_j)$ and (iii) $ADR(a_i, r_j)$ .....	267
Figure 6-74: The risk score variations among task assignments (agent $\rightarrow$ task) receiving the top-ten risk values for the two metrics – (i) $ETA(a_i, t_p)$ and (ii) $ADT(a_i, t_p)$ . ....	271
Figure 6-75: The variations in the top-ten risk values for the two metrics – (i) $EKR(a_i, r_j)$ and (ii) $EKT(a_i, t_p)$ . ....	273
Figure 6-76: The frequency of occurrence (number of agent $\rightarrow$ resource combinations) of the $IAC(a_i, r_j)$ risk scores through the four different types of social networks. ....	274
Figure 6-77: Indirect access pathways via the friendship network of Organisation-2 that result in highest risk scores. ....	276
Figure 6-78: The frequency of occurrence (number of agent $\rightarrow$ resource combinations) of the $TAR(a_i, r_j)$ risk scores through the four different types of social networks. ....	277
Figure 7-1: Arrangement of chapter sub-topics .....	281
Figure 7-2: Distribution of evaluators participated from each organisation sector. ....	282

---

Figure 7-3: Number of evaluators from organisations of different size (based on the number of employees).....	282
Figure 7-4: Job roles of evaluators in their organisations. ....	283
Figure 7-5: Evaluators' opinions on the usefulness of the results in the assessment of socio-technical access risks in organisations. ....	284
Figure 7-6: Evaluators' opinions on the applicability of the results in improving the overall access risk awareness of the organisations. ....	285
Figure 7-7: Evaluators' opinions on the effectiveness of the results in communicating access risks to the decision makers. ....	286
Figure 7-8: Evaluators' opinions on how well the risk assessment model represents important socio-technical interactions in organisations. ....	287
Figure 7-9: Evaluators' responses for the time taken to collect necessary data required to instantiate the model. ....	288
Figure 7-10: Evaluators' opinions on the ease of model instantiation using the available software tools. ....	289
Figure 7-11: Evaluators' opinions on the ease of executing the risk assessment method using the software tools provided. ....	290
Figure 7-12: Evaluators' opinions on the applicability of the metric scores in quantifying access risks in organisational contexts (validity of the metrics). ....	291
Figure 7-13: Evaluators' opinions on the accuracy of the metrics in ranking the information systems access risks. ....	292
Figure 7-14: Distribution of $ERA(a_i, r_j)$ , $VNA(a_i, r_j)$ and $ADR(a_i, r_j)$ scores in Organisation-2.....	295
Figure 7-15: The risk assessment activities followed in the research and the assessment method recommended for information security professionals (re-illustration taken from Chapter 5).....	298
Figure 7-16: Activities involved in the ISO/IEC 27005:2011 Standard .....	300
Figure 7-17: The risk assessment process described in NIST SP 800-300: Revision 1 .....	302
Figure 7-18: The three main phases of the OCTAVE risk management methodology .....	303
Figure 7-19: Proposed components of a socio-technical risk assessment system that automates all functions from data collection to visualisation.....	311

# List of Tables

Table 1-1: Some common definitions of insider threat .....	5
Table 2-1: Socio-technical information system models and their applications .....	16
Table 2-2: Socio-technical models used by information systems security researchers and example applications .....	21
Table 2-3: Example Access Matrix (Lampson 1971; Graham and Denning 1972).....	27
Table 2-4: Comparison of Access Control Models Described in this Chapter .....	35
Table 2-5: Comparison of the risk assessment activities prescribed in three standards - ISO/IEC 27005:2011, NIST SP 800-30 Revision 1 and OCTAVE.....	39
Table 2-6: A comparison of models used in the information systems security risk analysis .....	46
Table 3-1: Some theoretical foundations used to create artefacts in this research .....	62
Table 3-2: A comparison of activities in the three design science process models .....	66
Table 3-3: Steps (activities) carried out in the research project and the corresponding phases in Venable’s (2006b) design science process model.....	67
Table 4-1 : Insider threat incident descriptions extracted from Cappelli et al. (2012) .....	74
Table 4-2: Access vulnerabilities that contributed to insider threat events given in Table 4-1 .....	81
Table 4-3: Summary of types of data collected and methods used .....	90
Table 5-1 : Cases listed in Table 4-1 categorised according to their underlying causes in Figure 5-2. ....	96
Table 5-2: The meta-matrix representation of organisations introduced by Carley (2002; 2003).....	97
Table 5-3: Meta-matrix representation of entities and relationships that are important in the assessment of socio-technical access risks.....	98
Table 5-4: Risks occurring due to information resource authorisations.....	106
Table 5-5: Risks occurring due to task assignments.....	126
Table 5-6: Risks occurring due to knowledge requirements.....	133
Table 5-7: Risks occurring due to social relationships combined with resource authorisations or task assignments .....	142
Table 5-8: Summary of the metrics presented in this chapter .....	162
Table 5-9: Equivalent activities in the research methodology to the activities in Figure 5-16.....	175
Table 6-1: The properties and applicability of social networks to each risk type .....	226
Table 7-1: Summary of theoretical contributions of this research .....	312

# Abstract

The research presented in this thesis is aimed at developing a socio-technical security risk assessment methodology for information systems access that would enable organisations to take effective insider threat mitigation decisions.

Recent high-profile insider threat events and industry surveys suggest that insider threat is a serious problem faced by organisations in terms of information systems security. Since malicious insiders by definition have some level of legitimate access to information resources of an organisation, information systems access risks can be considered as a major cause of insider threats. Because a completely closed system is useless, despite being very secure, information system access authorisations should be granted by weighing the risks against the access requirements. Access risk assessments also provide necessary information for security professionals to make effective insider threat mitigation decisions.

However, models available for controlling information systems access, as well as security risk assessment methodologies, are primarily technical ones. These access models and risk assessment methodologies are not suitable for the rapidly changing information security threat landscape. At the same time, researchers have emphasized the importance of socio-technical aspects in solving information systems security problems. In order to fill the research gap, a socio-technical security risk assessment methodology for information systems access is presented in this thesis.

The risk assessment methodology includes an access risk assessment model, method and metrics. The risk assessment model is based on a meta-matrix representation of important entity and relationship types for organisational information systems access. The model and metrics have been developed upon analysing previous insider threat event data. The information systems access security risk assessment methodology has been evaluated using two techniques – case studies conducted using the data collected from three organisations and by analysing opinions of information security professionals who participated in an evaluation workshop. The results of the evaluations suggest that the methodology would be very useful for organisations to assess access security risks. The risk assessment methodology also makes a significant theoretical contribution to the information systems security discipline by introducing a socio-technical risk modelling approach and metrics based on a network paradigm.

# Acknowledgements

Although the cover page of this thesis bares my name as the author, it simply wouldn't have been possible without the help, guidance and encouragement of some remarkable people. First and foremost, I am indebted to my principle supervisors - A/Prof. Helen Armstrong and Dr. Colin Armstrong for their patience and kind guidance every step of the way throughout my PhD journey. Their wisdom and excellent supervision enabled me to overcome the inevitable hurdles that are part and parcel of PhD research. I am also grateful to the other members of my supervision team – A/Prof. John Venable and Lt. Col. (Dr.) Ian McCulloh. Prof. Venable's guidance helped me to solve many methodological issues in the early stages while Dr. Ian McCulloh's network science expertise and insights were invaluable whenever I needed technical advice or evaluation of my research outcomes.

A special thank you goes to Mr. Lal Dias, CEO of Sri Lanka CERT|CC, for his support during the data collection and research evaluation. His endorsements assured organisations to grant me access to information that they would not normally share. Furthermore, it was very thoughtful of him to arrange workspace for me during the data collection phase and allowing me to conduct a workshop as a part of their Annual Cyber Security Week Events. I must also thank my former colleagues at Sri Lanka CERT|CC – Kanishka, Roshan, Rohana, Lakshan and Nilusha for their support. Kanishka was kind enough to negotiate with organisations under the Sri Lanka CERT|CC banner on my behalf.

I am forever grateful to my mother and late father for giving me the strength and courage to face challenges in life. My mother sacrificed her career and dedicated most of her time for us while my father had to endure being away from his beloved family, working overseas for long periods, primarily to fund our education. I must also thank my sister for encouraging me whenever I was down in confidence. It wouldn't be fair if I didn't mention my parents-in-law for their support as well as numerous other relatives and friends who helped me at various stages of this endeavour. I wouldn't list them individually to avoid missing someone's name.

Last but not least, I am very grateful for the support given by my loving wife – Thakshila and daughter - Anuki. Thakshila took over most responsibilities of raising a family and allowed me to focus on the research while encouraging me all the time. Anuki, despite her tender age, understood that her dad must not be disturbed at times to finish his work. I feel very lucky to have both of you in my life.

# 1. Introduction

Information systems security breaches have become a major problem and hardly a day passes without a news report of an adverse information security event. Organisations must protect themselves against two main classes of security threats – ones originating from outside the organisation, the others originating from within the organisation: referred to as insider threats. The latter category has created a lot of concern for organisations recently due to several high-profile insider data leaks such as Edward Snowden (Greenwald 2013) and WikiLeaks (Shane and Lehren 2010) incidents as well as recent industry reports highlighting the severity of the problem (recent statistics related to insider threats are presented in the next section).

The sources of insider threats are due to people having some level of legitimate access to information resources of an organisation. Information systems access has become an important aspect of security since the introduction of multi-user and time-sharing systems such as Multics in mid-1960s (Saltzer 1974; Glaser 1967). As a result, technical models for information systems access control started to emerge. The technical models used to control information systems access worked well in the early days since computing resources were accessed by a few specialised people concentrated in research organisations, universities or defence establishments.

The technical bias can be seen in the information systems security risk assessment methodologies. However, large-scale adoption of computer information systems has challenged technical models of information systems access and risk assessment. Today, organisations have to provide information systems access to employees, business partners, contractors and even customers. The traditional information security perimeters of organisations have disappeared with users accessing information resources from various locations using a range of devices. Making the situation even more complicated, organisations need to provide access to corporate information resources using devices owned by users – a concept known as Bring Your Own Device (BYOD) (Willis 2014). In response to this changing threat landscape, information security researchers have emphasised the importance of socio-technical aspects (Socio-technical aspects of information systems security are discussed in detail in Chapter 2). Although their mainstream adoption is still lagging, access control models that incorporate social and contextual aspects have also been proposed recently.

However, there is still a serious lack of socio-technical security risk assessment methodologies available for the security professionals. This research is based on the premise that availability of a socio-technical access risk assessment methodology would enable organisations to better understand risks that contribute to insider threat events. Therefore, this thesis aims to introduce a socio-technical access security risk assessment methodology that would enable organisations to make insider risk mitigation decisions more effectively.

This introductory chapter provides a brief overview of the thesis. It begins with a discussion of the significance of the insider threat problem and provides definitions of key terms used throughout the thesis. The chapter then presents an overview of the research approach and the structure of the thesis. Figure 1-1 illustrates the progression of chapter sub-topics.

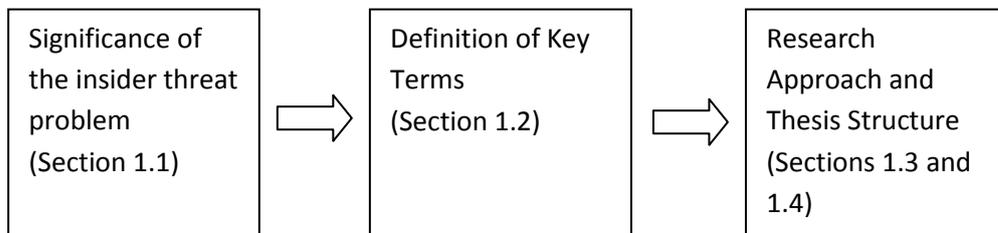


Figure 1-1: Arrangement of chapter sub-topics

## 1.1 Significance of the Insider Threat Problem to the Information Systems Security Discipline

Over the years, organisations have concentrated most of their efforts and resources to protect the availability, integrity and confidentiality of information resources from external adversaries. Due to the changes in the threat landscape described earlier and as pointed out by Gartner Research (Carpenter and Walls 2011) organisations need to focus on security risks originating from people within their trust boundary (in other words, risks due to insiders - people having legitimate access to information systems). Gartner has also labelled insider threats as one of the top-five issues for Chief Information Security Officers (Heiser and Scholtz 2009).

The seriousness of the insider threat problem is highlighted in the recent industry reports. In the 2013, US State of Cyber Crime Survey (Pricewaterhouse Coopers et al. 2013), conducted jointly by CSO Magazine, U.S. Secret Service, Software Engineering Institute - CERT Program at Carnegie Mellon University and Pricewaterhouse Coopers, 21% of the

respondents rated current and former employees as the greatest threat to information systems security of their organisation. External hackers were only rated marginally higher (22%) as the greatest threat while all other threat sources received much lower percentages. At the same time, 35% percent of the respondents believed insider attacks are more costly to the organisation as opposed to 31% percent who believed that outside attacks are more costly. The 2014 Global State of Information Security Survey (Pricewaterhouse Coopers et al. 2014) offers a more global perspective of the insider threat problem. According to that survey, 58% of the organisations have experienced a security incident due to either current or former employees. In contrast to this only 32% of the organisations reported incidents blamed on external hackers.

Despite the alarming statistics provided in the industry reports mentioned above, the status quo suggests that organisations still lack the capability to mitigate insider threats effectively. Moreover, most organisations' focus is still on preventing attacks from the outside. In the 2013 US State of Cyber Crime Survey (Pricewaterhouse Coopers et al. 2013) 61% of the participants believed that their organisations are either only minimally or moderately effective in managing insider threats. Therefore, there is a pressing need for the information systems security researchers to develop methodologies for the assessment, mitigation and detection of insider threats in organisations.

## **1.2 Key Terms and Definitions**

This section explains some key terms used throughout this thesis guided by the common definitions used in the information systems security discipline.

### **1.2.1 Information Systems Security**

ISO/IEC 27001:2005 Standard (International Organisation for Standardisation 2005a, 2) defines information security as “preservation of confidentiality, integrity and availability of information.” Therefore, confidentiality, integrity and availability are the three key properties that must be preserved in information systems in order to make them secure.

### **1.2.2 Information Security Threats and Vulnerabilities**

ISO/IEC 27002:2005 Standard (International Organisation for Standardisation 2005b, 3) defines a threat as “a potential cause of an unwanted incident, which may result in harm to a system or organisation” and a vulnerability as “a weakness of an asset or group of assets that can be exploited by one or more threats.” In terms of information systems security

threats, this research is concerned with one major type – insider threats – and presents a methodology to assess risks occurring due to information systems access vulnerabilities that could be exploited by insiders (insider threat is defined below in section 1.2.4).

### **1.2.3 Information systems security risks**

ISO/IEC 27002:2005 Standard (International Organisation for Standardisation 2005b, 2) defines information security risk as “combination of the probability of a (threat) event and its consequence.” The probability of a threat event and its consequence are also called the likelihood and impact respectively (National Institute of Standards and Technology 2012).

### **1.2.4 Insider Threat**

One problem highlighted by the researchers in relation to insider threats is the difficulty of providing a consistent definition (Bishop and Gates 2008; Bishop, Gollmann, et al. 2008; Bishop, Engle, et al. 2008; Hunker and Probst 2011). Some common definitions found in the literature are given in Table 1-1.

A key aspect of the definitions given in Table 1-1 is the criteria used to distinguish insiders from the external adversaries. According to Bishop and Gates (2008) two actions define an insider – misuse of legitimate access in violation of security policies and/or obtaining unauthorised access in violation of the access control policy (e.g., privilege escalation). Hunker and Probst (2011) provide four criteria that can be used to distinguish insiders – having access to information systems of the organisation, ability to represent the organisation to outsiders, having knowledge due to the involvement in information systems design despite not having access privileges any more and individuals trusted by the organisation. The first criterion specifies that an insider should have access to organisational information systems. The second (representing the organisation) and the last specify that organisations place a certain amount of trust in insiders. The third criterion includes former employees or contractors whose access have been terminated but still possess a significant amount of knowledge on the organisation’s information systems.

Therefore, it is clear that the ability to access information systems of an organisation is a key theme used to define insiders. Furthermore, organisations place a certain amount of trust on the individual when authorising access to information systems. Another important consideration is whether accidental or unintentional threat events are included under insider threats. Some definitions given in Table 1-1 state insider threats are intentional

(Cappelli et al. 2012; Bishop 2005) while others (Kissel 2013, 98) do not explicitly exclude unintended threat events.

Table 1-1: Some common definitions of insider threat

Source	Definition of Insider Threat
Glossary of Key Information Security Terms: NIST IR 7298 – Rev 1	Security threats due to “An entity with authorized access (i.e., within the security domain) that has the potential to harm an information system or enterprise through destruction, disclosure, modification of data, and/or denial of service.” (Kissel 2013, 98)
Technical Report by Pacific Northwest National Laboratory – U.S. Department of Energy	Security threats due to “members of an organization authorized to access its information system, data, or network with a degree of trust by the organization and who accept a commensurate level of scrutiny by the organization to deter possible abuse of these privileges.” (Greitzer et al. 2009, 2)
The CERT Guide to Insider Threat (Book)	“A malicious insider threat is a current or former employee, contractor, or business partner who has or had authorized access to an organization’s network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization’s information or information systems.” (Cappelli et al. 2012)
Research Paper	“The insider threat is the threat that the insider may abuse her discretion by taking actions that would violate the security policy when such actions are not warranted.” (Bishop 2005, 78)

This research defines insider threat based on the definition provided by Cappelli et al. (2012) since it characterises an insider based on information system access and excludes unintentional threat events. Therefore, in this research, insider threat is specified as malicious (i.e., intentional) threats to confidentiality, integrity or availability of information resources, originating from an individual or group who currently has or previously had legitimate authorisations to access information resources of an organisation. As discussed earlier ability to access information systems is the key characteristic that separate insiders from outsiders. Moreover, although unintentional mistakes or failures can result in negative consequences, they are not the primary focus of information security analysts.

### 1.2.5 Information Systems Access and Access Control

National Institute of Standards and Technology (NIST), USA, define access as the “ability to use any information system resource” (Kissel 2013, 2; Kuhn et al. 2001, 46). It is further elaborated as the “ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions” (Kissel 2013, 2). Furthermore, NIST define access control as the “Process of granting access to information system resources only to authorized users, programs, processes, or other systems” (Kuhn et al. 2001).

People interact with information systems (or use system resources) to perform tasks assigned to them. Therefore, this research considers information system access in a broader sense which includes assignment of people to business processes performed using information systems, in addition to their ability to interact with, use or control information resources. Such a broad definition of information system access is beneficial for a risk assessment performed with the intention of mitigating insider threats.

## 1.3 Research Approach

### 1.3.1 Research Topic and the Objective

This thesis is titled - *A Socio-technical security risk assessment methodology for information systems access*. Accordingly, the primary objective of this research is to develop a methodology that can be used to assess security risks occurring due to information systems access. The core concepts that form the rationale for this research and related topics covered in the thesis are illustrated as a network map in Figure 1-2. The top node of the diagram represents the insider threat problem discussed earlier. The grey, rounded rectangles from the top node to the node representing methodology developed in this research (i.e., thick rectangle in the centre) and the sequence of links connecting them represent the rationale for the development of the risk assessment methodology. The blue colour rectangles represent topics or concepts covered in the thesis. Their arrangement in to chapters is demarcated by the coloured rectangles marked with dashed lines. The links between the nodes of the diagram show how topics and concepts are related to each other. The following discussion explains some key aspects related to the thesis title.

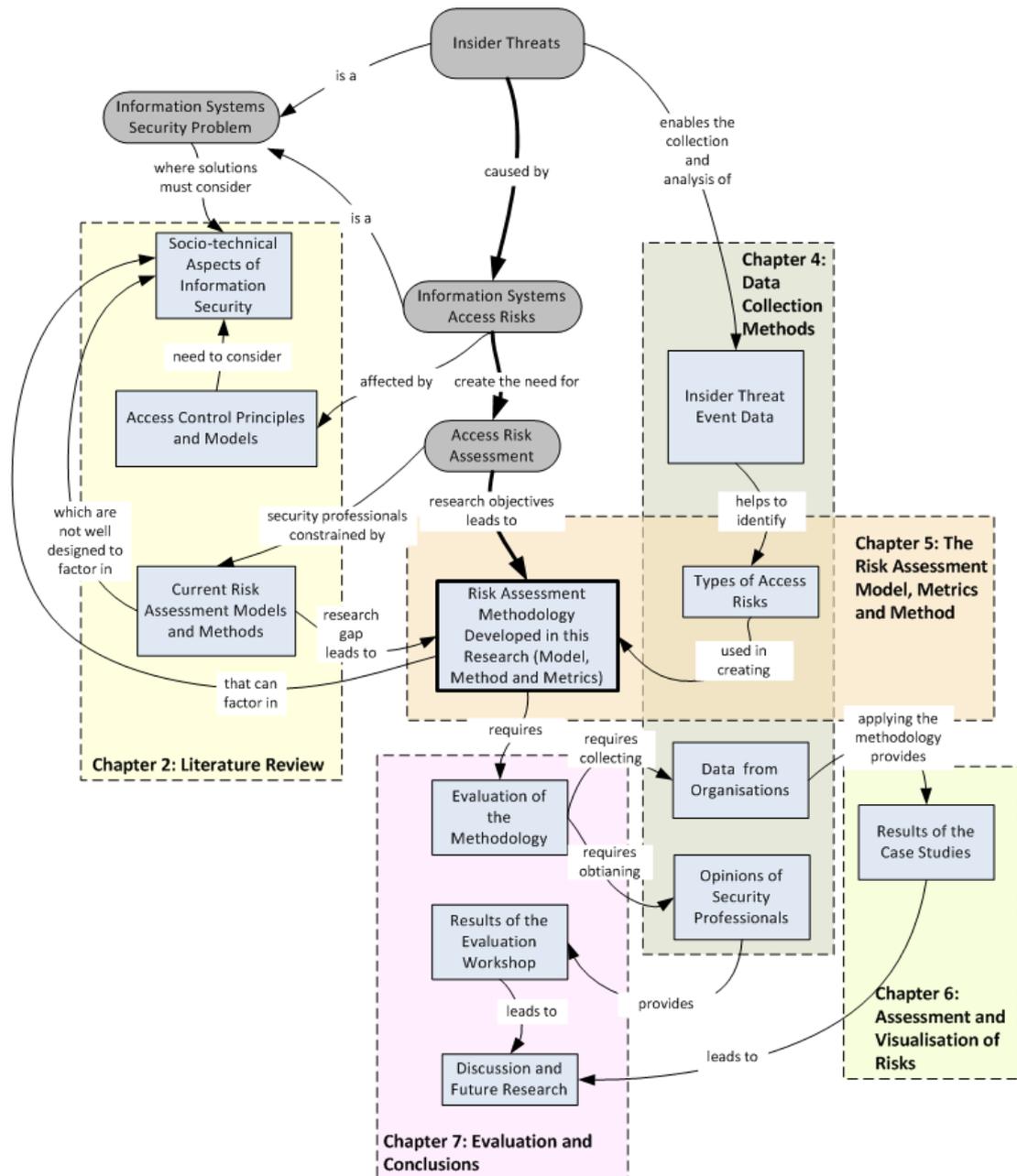


Figure 1-2: Topics and concepts covered in the thesis and relationships between them

### How does of access risk assessment help to mitigate insider threats?

An insider, by definition, is someone who has authorised access to information systems. Therefore, access authorisations given to individuals create risks that can lead to insider threat events (refer the relationship sequence between rounded rectangles in the middle of Figure 1-2). On the other hand, a completely closed information system is useless despite being very secure. Since organisations must grant individuals access to information systems and related business processes, one approach is to do so by knowing the risks. This way,

organisations can weigh the risks against requirements for granting access and enforce appropriate controls to mitigate the access risks. Therefore, information systems access risk assessments help organisations to mitigate insider threats by providing information required to make risk mitigation decisions. Furthermore, insider risk mitigation based on an access risk assessment approach has several advantages over deploying technical controls to detect insider threats:

1. Prevention is better than the cure – An access risk assessment would indicate the most likely and potentially damaging areas of concern. Formulating risk mitigation strategies based on the results of risk assessment can help prevent threat events from occurring. Furthermore, detection might be too late to prevent some adverse consequences.
2. As pointed out by Bishop, Gollmann, et al. (2008) insider threat detection will create false positives, which can have a detrimental effect on the organisation in terms of the employee morale, possible legal consequences and time/resource wastage.

### **Why should be the methodology termed “socio-technical”?**

Previous research (discussed in Chapter 2) has shown that information systems security is a socio-technical issue rather than purely a technical problem. Hence, the risk assessment methodology proposed in this thesis takes socio-technical aspects of information systems in to consideration.

### **1.3.2 Overview of the research method**

In order to develop an information systems access risk assessment methodology, the types of access vulnerabilities and related threats must be analysed first. As mentioned before, malicious insider is the threat source that exploits organisational information system access vulnerabilities. Therefore, as the first step of this research, real cases of insider threat events were analysed to identify the types of access vulnerabilities exploited by the insiders. As a result of this analysis, thirteen information system access vulnerability types, categorised in to four groups, were identified. The next phase involved developing a methodology (consisting of a risk assessment model, method and metrics) that could be used to assess security risks occurring due to those access vulnerabilities. Finally, the risk assessment methodology was evaluated using three case studies and a workshop held with

the participation of information systems security professionals. Chapter 3 discusses the research methodology in detail.

## **1.4 Structure of this Thesis**

Figure 1-2 illustrates how concepts and topics related to the research are arranged in to chapters excluding the Introduction (Chapter 1) and the Research Methodology (Chapter 3).

Chapter 2 presents a review of literature related to socio-technical perspectives of the problems in information systems security domain followed by a discussion of information systems access control models and the methodologies available for information systems security risk assessment. Chapter 3 provides an overview of the research paradigm adopted and the methodology followed to develop and evaluate the artefacts produced in this research. Since Chapter 3 describes the overall research process, it is not demarcated using the concepts or topics in Figure 1-2.

Chapter 4 of the thesis provides detailed descriptions of the data collection methods used. Data required for the research was gathered in three distinct phases – initial collection of insider threat event data, data collected to carry out case studies of three organisations and the data collected during the evaluation workshop involving information security professionals.

Chapter 5 of the thesis presents the proposed socio-technical risk assessment model, method and the metrics. Using three case studies of organisations, Chapter 6 illustrates how the assessment model, method and metrics can be used to assess and visualise organisational information systems access risks. The results produced in the three case studies are also used to evaluate the methodology. Chapter 7 of the thesis deals with the evaluation of the risk assessment methodology developed in the research. Evaluation was primarily carried out using the three case studies of organisations and a workshop conducted with the participation of information systems security professionals. Chapter 7 also discuss the conclusions made and a discussion of future research opportunities related to the topic.

Appendix A of the thesis contains the questionnaires used to collect data from organisations for the case studies while Appendix B contains the questionnaire administered at the end of the evaluation workshop.

## 2. Literature Review

As mentioned in the previous chapter, the aim of this research is to develop a methodology to assess socio-technical security risks in information systems access that would aid the mitigation of insider risks in organisations. This chapter reviews literature related to the above goal in order to analyse the progress made in this area and to identify any knowledge gaps that could be filled through this research. The literature review was guided by the following questions:

- What evidence is presented in the research literature to emphasise and illustrate the socio-technical nature of information systems security, including the insider threat problem?
- What models and theories have been proposed to represent socio-technical aspects of information systems security?
- What models and principles are used in the provision of controlled access to information systems?
- What models, methods and metrics have been proposed for information systems security risk assessment and can they be applied to perform a socio-technical security risk assessment of information system access?

Accordingly, the sub-topics presented in this chapter are arranged as illustrated in Figure 2-1.

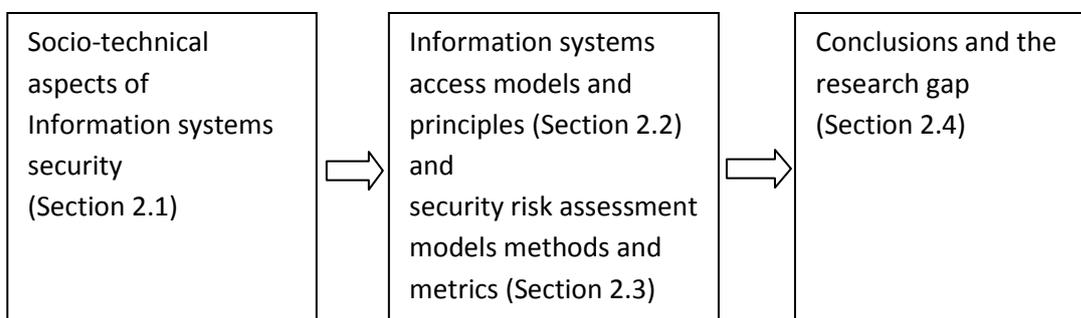


Figure 2-1: Arrangement of chapter sub-topics

## 2.1 Socio-Technical Aspects of Information Systems Security

As a precursor to the discussion of socio-technical aspects of information systems security, it is worth investigating what type of socio-technical models have been used in the more general domain of information systems and their applications. Therefore, this section begins with a literature review of the socio-technical models and theories used in the information systems domain and some of their applications. The chapter then progress toward a discussion of research dealing with the more specific topic of information systems security.

### 2.1.1 Socio-technical aspects of information systems

There is a wide spectrum of research publications that discuss the socio-technical aspects of information systems. This section describes four prominent socio-technical models presented in the research literature and their applications in the information systems discipline.

#### Socio-Technical Systems (STS) model

Majority of the research related to socio-technical aspects of information systems are based on the Socio-Technical Systems (STS) model which originated as a model for improving organisational design, especially with regards to the human aspects (Mumford 2003). The core principles of socio-technical design were compiled by Cherns (1976; 1987) while Clegg (2000) proposed a revised set of principles that consider advancements in the information and communications technologies used in organisations. According to Bostrom and Heinen (1977a) STS view of information systems consists of two aspects – technical component and the social component. Technical component consists of the hardware, software (*Technology*) and tasks performed by the system (*Tasks*) while the social component consists of attributes of people, relationships among them (*People*) and organisational task structure (*Structure*). The STS model proposed by Bostrom and Heinen (1977b) is illustrated in Figure 2-2.

The arrows in the diagram indicate interrelationships between each sub-component mentioned above. Since the sub-components have interrelationships between them, changes in one sub-component affect the others. Therefore, Bostrom and Heinen (1977a) emphasize that information system designers should analyse problems in both technological and social components and strive for joint optimisation of the two.

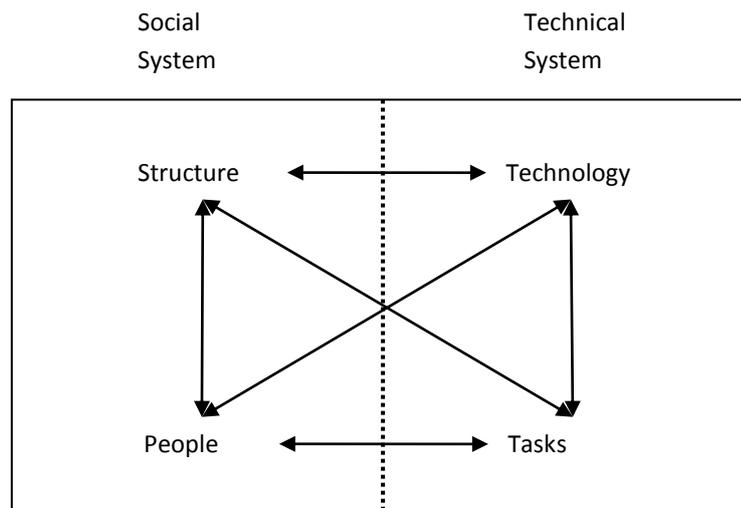


Figure 2-2: Socio-Technical Systems (STS) model of to Bostrom and Heinen (1977b)

Most research using the STS model is centred on exploring the reasons for information systems failures and finding better methodologies to develop them. In two related papers Bostrom and Heinen (1977b, 1977a) show that socio-technical factors play a significant role in the failure of Management Information Systems (MIS) implementations and present a case study of an information system development effort that utilise the STS model. Clegg et al. (1997) have interviewed information systems experts with a combined experience of over 14,000 organisations in the U.K. and found that social and organisational problems are behind most information system failures. Mumford (1983) has introduced a new information systems development methodology called *Effective Technical and Human Implementation of Computer-based Systems (ETHICS)*, which is also built on top of the STS model.

Other applications in the information systems domain also have been subject of research based on STS model. Lyytinen and Newman (2008) have developed a information systems change model using Socio-Technical Systems Theory. Lyytinen et al. (1998) use STS model to analyse four software development risk management approaches.

### **Actor-Network Theory (ANT)**

Actor Network Theory (ANT), pioneered by Latour (1988, 2005), Callon (1986) and Law (1992) is another socio-technical theory used to model information systems. The core principles of ANT as elaborated by Law (1992) include:

- Heterogeneous Networks - Social systems (e.g., society, organisations) consists of heterogeneous networks of people and other material objects. In these heterogeneous networks material objects are same as people in an analytic perspective. The social and technical aspects of an actor-network are inseparable and must be analysed at the same level.
- Actors are networks themselves – Actors in ANT, whether humans or other material objects, are generated by a network of heterogeneous interacting entities.
- Punctuation – Despite all actors themselves being actor-networks, they are seen at a particular level of abstraction ignoring the underlying granularity or the processes taking place within the actors.
- Translation – This is the process of formation of an actor-network as a series of alliances between actors.

The models created using the ANT are different from the STS models discussed earlier. First, the ANT treats social and technical aspects as essentially similar, inseparable components (Law 1992) as opposed to the distinction between the two in STS models. The units used in the analysis – actors can be *punctuated* at different levels of abstraction in ANT while STS analysis is performed at the level of social and technical components. The relationships between actors are also unstable and unreliable (Callon 1986) in ANT and the process of *translation* can reoccur at anytime to change the status quo. On the other hand, the STS model focuses on a rather stable set of interrelationships between the social and technical components. Finally, the analysis in ANT is inherently process oriented due to principles such as *punctuation* and *translation* (Law 1992) while STS model concentrates on the effects of the interrelationships between social and technical components. Despite these differences, it is possible to use STS and ANT concepts in a complementary manner to study socio-technical systems as Kaghan and Bowker (2001) illustrate.

Many applications related to information systems have been researched by utilising the Actor-Network Theory. Walsham (1997) as well as Tatnall and Gilding (2005) have pointed out the merits of using ANT in information systems research, particularly in ones concerned with the socio-technical aspects. Boomfield et al. (1992), using three case studies, have illustrated how ANT can be applied to analyse complex socio-technical requirements of the successful implementation of a resource management system. ANT has also been used to

investigate information system failures as demonstrated by Mahring et al. (2004). Other applications of ANT for research in the information systems discipline include analysis of information policies (Frohmann 1995), information infrastructures (Monteiro and Hanseth 1996) and Information and Communication Technology (ICT) strategy (Gao 2005).

### **Web of Computing Model**

Another socio-technical model of information systems, called the Web of Computing Model, has been introduced by Kling and Scacchi (1982). The Web of Computing Model (Kling and Scacchi 1982) of an information system consists of four components:

1. Lines of work and going concerns - These are tasks performed and goals of the organisation (includes both formal and informal ones)
2. Infrastructure of computing – According to Kling and Scacchi (1982) this means “resources which help support provision of a given service or product”. Infrastructure of computing includes not only hardware and software but skilled people and operational procedures as well.
3. Production lattices – This includes task and resource dependencies as a network of social relationships among people.
4. Macrostructures – Macrostructures are constraints in place due to organisational structure, business environment, policies, regulations and market conditions.

The model is called Web of Computing since it is centred on networks of people (called the production lattices) who utilize or contribute to information resources (called infrastructure of computing). Both these entity types and relationships between them are embedded in the larger organisational and industry contexts known as the macrostructures (Walsham et al. 1988). In some aspects, The Web of Computing Model is similar to the STS model described earlier. For example, the informal aspects of the *lines of work and going concerns* are equivalent to the relationships between the *people* component of the STS model illustrated in Figure 2-2 while the formal aspects are equivalent to the component labelled *structure* (organisational structure) in the same figure. *Infrastructure of computing* element of the Web of Computing Model is equivalent to the *Technology* component of the STS Model. Since the *Infrastructure of computing* includes skilled personnel, the *People* component of the STS model is also related to that. However, unlike the STS model, Web of Computing model specifies some of the micro-level socio-technical relationships as

illustrated by the component *production lattices*. Mapping the *production lattice* would involve mapping individual relationships between tasks, people and resources as well as associations between people arising due to these dependencies. Similar to the STS Model, Web of Computing also models the effects of stable relationships between social and technical elements of an organisation. Therefore, it is different from the ANT based models which focus on the process of forming alliances between socio-technical entities.

Another feature of the Web of Computing Model (Kling and Scacchi 1982) is the attempt to distinguish between formal and informal relationships. Authors argue that although formal job descriptions (people-task relationships) can be a starting point for *lines of work and going concerns* this component should ideally include informal relationships that occur between people due to tasks they perform. These may include friendships, informal authority, informal dependencies and other types of informal relationships.

Applications of the Web of Computing Model are mainly found in the field of information systems development. For example, Garg and Scacchi (1989) have developed an intelligent software hypertext system using a Web of Computing Model. Based on a similar model, Noll and Scacchi (2001) have developed a process-scripting language called PML that can be used to specify complex process requirements and relationships in organisations.

### **Socio-Technical Interaction Networks (STIN)**

Socio-Technical Interaction Network (STIN) Models, which is an enhancement of the Web of Computing Model, was first proposed by Kling et al. (2003) as a way of modelling scholarly electronic forums. STIN models consists of heterogeneous social and technological entities that are “highly intertwined” (Kling et al. 2003). STIN also assumes that socio-technical relationships between two entities can take multiple forms and entities are embedded in multiple, overlapping networks (Kling et al. 2003; Meyer 2006). STIN models share the concept of heterogeneous networks with the models based on the ANT. However, unlike the ANT models, STIN focus is on the effects of relationships in the socio-technical networks which are treated as rather stable by the analysts. In that way, STIN has the same focus as the STS models.

STIN models have been utilized in numerous studies in the field of information systems and most of them deal with the analysis of web-based collaboration forums. Examples include analysis of Electronic Scholarly Communication Forums by Kling et al. (2003), study of the formation and collaboration in complex Free and Open Source Software (FOSS)

development projects (Scacchi 2005) and an analysis of a web-based collaboration system for science and math teachers (Barab et al. 2004). Furthermore, Eschenfelder and Chase (2002) have used STIN models to investigate post implementation issues of four web-based information systems.

### Summary of the socio-technical aspects of information systems

The four models presented in this section and their applications cited illustrate that importance of the socio-technical aspects of information systems have been acknowledged by the research community. Table 2-1 presents a summary of the socio-technical models of information systems discussed in this section and their applications.

Although the four models offer three different perspectives (Note that STIN is an enhancement of the Web of Computing Model) of information systems as shown in Table 2-1, two common features of the socio-technical nature can be extracted from them. First, Socio-technical models of information systems consist of social and technical entities that are related to each other. How well the social and technical aspects are intertwined (whether they are just interrelated as in STS model or inseparable in to social and technical sub-systems as in ANT based models) varies from one model to another. Second, the behaviour and the properties of the system are a result of the relationships between social and technical entities.

Table 2-1: Socio-technical information system models and their applications

Model	Some Salient Features	Example Applications in the Information Systems Discipline
Socio-Technical Systems (STS) Model (Bostrom and Heinen 1977b, 1977a)	<ul style="list-style-type: none"> <li>▪ Information systems consist of related social and technical components.</li> <li>▪ Social and technical components can be elaborated separately but must be optimised jointly to successfully develop and implement information systems.</li> <li>▪ Concerned with the effects of stable interrelationships between social and technical components</li> <li>▪ Social and technological agencies are different but interrelated</li> </ul>	<ul style="list-style-type: none"> <li>▪ Reasons for information systems failures (Bostrom and Heinen 1977b, 1977a; Clegg et al. 1997)</li> <li>▪ Information systems development methodologies (Mumford 1983, 2000)</li> <li>▪ Information systems change (Lyytinen and Newman 2008)</li> </ul>

*table continued on next page.....*

Table continued from previous page .....

Model	Some Salient Features	Example Applications in the Information Systems Discipline
Actor Network Theory (ANT) (Latour 1988, 2005; Callon 1986; Law 1992)	<ul style="list-style-type: none"> <li>▪ Information systems consists of heterogeneous social and technical actors that are treated at the same level analytically (social and technical components are inseparable)</li> <li>▪ Concerned with the process of forming actor-networks through principles such as punctuation and translation</li> <li>▪ Social and technological agencies are the same and inseparable.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Analysing information system failures (Mahring et al. 2004)</li> <li>▪ Information systems development (Bloomfield et al. 1992)</li> <li>▪ Analysis of information policies (Frohmann 1995), information infrastructures (Monteiro and Hanseth 1996), and ICT strategy (Gao 2005)</li> </ul>
Web of Computing Model (Kling and Scacchi 1982) and Socio-Technical Interaction Networks (STIN) (Kling et al. 2003)	<ul style="list-style-type: none"> <li>▪ Information systems consist of heterogeneous social and technical entities that are highly intertwined. (Social and technical aspects are inseparable)</li> <li>▪ Various socio-technical relationships are embedded in multiple, overlapping networks.</li> <li>▪ Concerned with the effects of socio-technical relationships which are considered stable</li> <li>▪ Social and technical agencies can be separately identified but they are heavily intertwined</li> </ul>	<ul style="list-style-type: none"> <li>▪ Information systems development (Garg and Scacchi 1989)</li> <li>▪ Analysis of web-based collaboration forums (Kling et al. 2003; Scacchi 2005; Barab et al. 2004; Eschenfelder and Chase 2002)</li> </ul>

### 2.1.2 Socio-technical nature of problems in the information systems security domain

Importance of socio-technical factors in information systems implies that ensuring the security of information systems is also a socio-technical problem. In their review of research literature, Dhillon and Backhouse (2001) point out that researchers have increasingly considered socio-organisational perspectives in information systems research although such a focus is lacking in the information security research community. A similar conclusion has been made in the survey of information security research literature by Beznosov and Beznosova (2007). According to them, ninety-four percent (94%) of the research papers published in the information systems security domain focus on the technical aspects while only a very small fraction address the human and social issues. On the other hand, the same

researchers have discovered through a search of the Google News Archives that 41 percent of reported security incidents had social or human causes. Siponen (2007) also points out that there is a large bias towards technical aspects amongst the information systems security research community. They argue that technical controls alone cannot provide effective security for information systems. A similar view is expressed by Hitchings (1995) who points out, using results of a survey, that majority of the information security breaches have not occurred due to technical factors and most exploits require little technical sophistication. Hitchings (1995) claims that there is a deficiency in the traditional approaches to designing and implementing information systems security since they ignore the human aspects and advocates a soft-systems (Checkland 1989) approach instead.

Despite the criticism, some researchers have applied socio-technical concepts to advance the theory and practice of information systems security. Therefore, the next three sub-topics review information systems security research that utilise the socio-technical models discussed earlier followed by a brief overview of other socio-technical approaches found in information security research literature.

### **Information systems security research utilising the Socio-Technical Systems (STS) Model**

Although many research efforts claim taking a socio-technical perspective of information systems security there are actually a very few that explicitly use the STS Model. Evangelidis (2004) has proposed a framework, called FRAMES, for the risk assessment (including security risk assessment) of e-Government Services which is explicitly based on the Bostrom and Heinen's (1977b, 1977a) STS model of information systems. The FRAMES (Evangelidis 2004) framework consists of four components – customers, e-Service, organisational level (the public organisation providing the service) and inter-organisational level (other organisations that support the development of e-Services). According to the framework, three types of socio-technical interrelationships exist among the four components mentioned above – between customers and the front-end of the e-Service platform, between organisational level and the back-end of e-Service platform and between the inter-organisational level and the back end of the e-Service platform. In another research based on the STS model, Werlinger et al. (2009) have performed a socio-technical analysis of the challenges in information systems security management. They classify security management challenges identified through interviews of IT professionals into three categories – human, organisational and technological. The interrelationships between these

security management challenges have been mapped out to present a holistic picture and to identify opportunities for improvement.

### **Information systems security research utilising the Actor Network Theory (ANT)**

Hedström et al. (2010) have demonstrated how ANT can be used to understand socio-technical factors contributing to information security breaches. They present a case-study of a computer system compromise and analyse the events leading to it using ANT concepts such as translation and inscription. A more formal approach is taken by Pieters (2011) in developing a hyper-graph based reference model for the analysis of information system security vulnerabilities. Pieters (2011) emphasize vulnerability pathways typically exploited in insider attacks are socio-technical. Therefore, they use the concept of heterogeneous actors specified in ANT to model both humans and technical artefacts. However, there is no evidence to suggest that they use other ANT concepts to explore the event sequence required to exploit a particular vulnerability. Bonner and Chiasson (2005) use an ANT based approach to investigate the information security related topic of privacy. They use an ANT model to demonstrate the complex interactions that occur during the development of privacy standards. Naturally, researchers using ANT based approaches in information systems security are interested in explaining the processes behind security related outcomes (these outcomes can be negative ones such as attacks or positive ones such as the development of standards) and the complex socio-technical interactions involved.

### **Security research based on Web of Trust and Socio-Technical Interaction Networks (STIN)**

Although information systems security researchers have not directly acknowledged the use of Web of Trust or STIN Models in their research, strikingly similar concepts can be observed in the security research literature. For example, the ontology proposed by Massacci et al. (2007) for the development of socio-technical security requirements use actors such as people, job roles, goals (strategic objectives of people), tasks and resources as well as relationships between them. The use of heterogeneous actors and multiple types of relationships between them is a key characteristic of STIN Models. They demonstrate how the ontology can be used by software developers to capture security requirements early in the systems development lifecycle. Strens and Dobson (1993) present another socio-technical approach for security requirements analysis using the concept of responsibility modelling. The modelling framework proposed by them consists of three entities – agents, activities and resources which are linked together through relationships which is again a similar conceptualisation to a STIN.

### **Other socio-technical approaches used in information systems security research**

There are many research publications that cannot be classified under the four socio-technical models of information systems presented in this chapter. Some of these research publications use a macro ergonomic approach, which according to Kleiner (2006) has its theoretical roots in Socio-technical Systems Theory. In one such study, Kraemer et al. (2009) investigate social and organisational factors that create pathways to security vulnerabilities using two focus groups of red teams (teams that identify vulnerabilities in systems). The researchers have identified nine social and organisational themes that are common in the vulnerability pathways. Another macro ergonomics based research by Carayon and Kraemer (2002) propose a conceptual model for information systems security, which consists of five components – people (information system users and administrators), organisational factors (includes security policies, security culture in organisation etc.), technology (Hardware and software), tasks (tasks performed by people), and environment (characteristics of the physical environment). This model has been further enhanced in a follow-up research effort (Kraemer and Carayon 2007).

Systems dynamics modelling is another approach used by information systems security researchers to investigate social and organisational aspects. This approach has been used mainly in research related to insider threats. CERT Program run by the Software Engineering Institute of the Carnegie Mellon University has used real insider threat case-study data to create system dynamics models for insider IT sabotage (Band et al. 2006; Moore et al. 2008; Cappelli et al. 2012), theft of intellectual property (Moore et al. 2011; Hanley 2011) and insider fraud (Cummings et al. 2012). Such systems dynamics models, through the mapping of causal relationships between socio-technical factors, enable researchers to generalise how various factors influence insider attacks. Furthermore, Moore et al. (2013) demonstrate how systems dynamics models can be used to monitor insider risk and provide early warnings to the decision makers.

### **Summary and Discussion of Socio-Technical Aspects of Information Systems Security**

Two facts become clear from the research focusing on the socio-technical aspects of information systems security. First, although technical aspects of information systems security have been topics of interest for a long time, researchers have only recently realised the importance of socio-technical aspects. For instance, first research publications on access control models and mechanisms have appeared in early 1970s (a discussion on

access control models appear later in Section 2.2.2) as opposed to most of the research cited above, majority of which have been published after year 2000. This is in stark contrast to information systems research where socio-technical topics have emerged much earlier. Second, just as in information systems research, information systems security researchers have different perspectives on what is meant by “socio-technical”. The different socio-technical perspectives (models and theories used) adopted by the information systems security researchers and examples of their applications are given in Table 2-2.

Table 2-2: Socio-technical models used by information systems security researchers and example applications

<b>Socio-technical model or theory</b>	<b>Salient features of the model used by the information systems security researchers</b>	<b>Example applications in the information systems security domain</b>
Socio-Technical Systems (STS) (Bostrom and Heinen 1977b, 1977a)	Security researchers have used STS to characterise information systems as socio-technical systems and identify social components, technical components and relationships between them.	Risk assessment of e-Government Applications (Evangelidis 2004) Socio-technical challenges in information security management (Werlinger et al. 2009)
Actor-Network Theory (ANT) (Latour 1988, 2005; Callon 1986; Law 1992)	Security researchers have used ANT to characterise information systems as heterogeneous networks of entities where both humans and technological artefacts are treated the same.  The main focus of researchers has been the processes or events that lead to security related outcomes.	Factors that contribute to the unfolding of information security breaches.(Hedstrom et al. 2010) Reference model for the analysis of information system security vulnerabilities (Pieters 2011) Process of privacy standard development (Bonner and Chiasson 2005)
Web of Computing and Socio-Technical Interaction Networks (STIN) (Kling and Scacchi 1982; Kling, McKim, and King 2003)	Security researchers have used Web of Computing and STIN models to characterise information systems as types of actors and relationships between them.	An ontology for the development of socio-technical security requirements (Massacci et al. 2007) Responsibility modelling for security requirements analysis (Strens and Dobson 1993)
Macro ergonomics (Kleiner 2006)	Security researchers’ focus is on socio-technical factors of organisations that affect information systems security.	Social and organisational factors that create pathways to security vulnerabilities (Kraemer et al. 2009)  Conceptual framework for investigating human and organisational factors affecting information security (Carayon and Kraemer 2002; Kraemer and Carayon 2007)
Systems Dynamics (Coyle 1996)	Researchers use systems dynamics models to map causal relationships that influence insider threat events	Models of insider threats in organisations (Moore et al. 2008; Moore et al. 2011; Cappelli et al. 2012; Cummings et al. 2012)

Some of the socio-technical models such as ANT have been used to investigate the processes or events that contribute to security outcomes while other such as STS and STIN have been used to model different entities and relationships important for information systems security. However, all researchers adopting socio-technical approaches seem to agree that both social and technical components as well as relationships between them must be considered in order to solve problems within the scope of the information systems security domain.

The research literature taking a socio-technical perspective in analysing problems in the information systems and information systems security domains have been discussed so far this chapter. Next, it is important to investigate what models and principles have been proposed to provide controlled access to information resources and whether socio-technical aspects are considered under them.

## 2.2 Information System Access – Models and Principles

Information system access is defined by the National Institute of Standards and Technology (NIST), U.S.A as the “ability to make use of an information system resource” (Kissel 2013, 4). In order to protect the availability, integrity and confidentiality of information resources, an organisation must provide controlled access to the users. There are two aspects important for providing controlled access to information resources as illustrated in Figure 2-3.

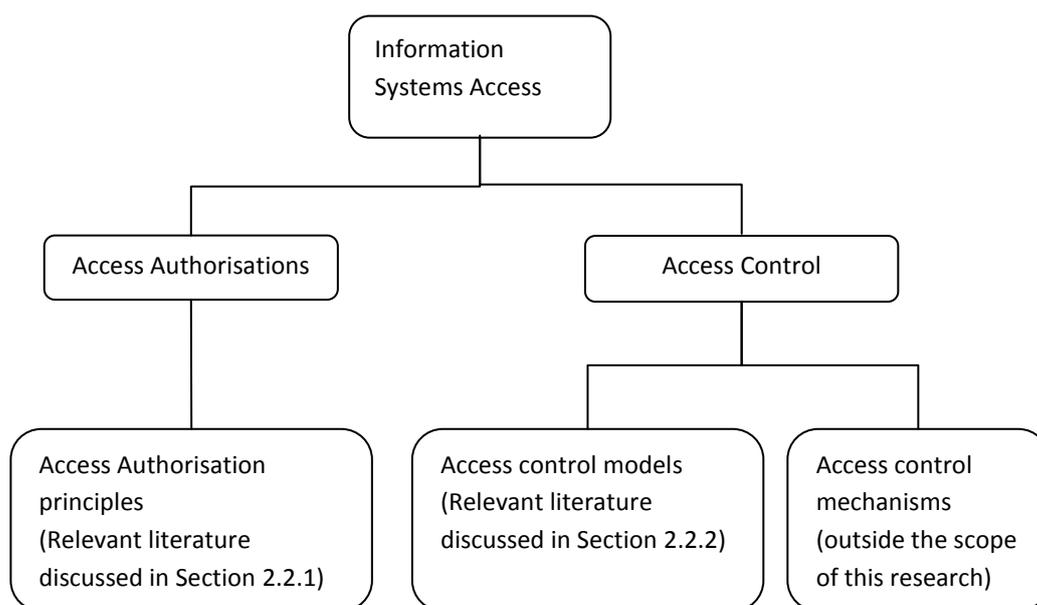


Figure 2-3: Topics in information systems access

First, the organisation must decide on a set of access authorisations dictate who gets access to what information resources, when and at what level. Although access authorisations are granted according to the needs specific to organisations and information systems, there is a set of principles or best practices to guide the security professionals. These principles are discussed in Section 2.2.1.

The other aspect deals with access control which is the process of either granting or denying access to resources based on the authorisations (Kissel 2013). Out of the two aspects, the topic of access control has been heavily researched under two categories – access control models and access control mechanisms or technologies. Access control models are higher-level abstractions on how controlled access could be achieved and access control mechanisms or technologies are typically software or hardware designs that use one or more access control models (Sandhu 1994; Samarati and de Vimercati 2001). Since access control mechanisms are outside the scope of this research, that topic will not be discussed here.

### **2.2.1 Access Authorisation Principles**

Although access authorisations are typically granted according to requirements specific to organisations there are principles which guide the information security professionals. Some of the commonly used access authorisation principles include least privilege (Saltzer and Schroeder 1975; Schneider 2003), separation of duties (Ferraiolo and Kuhn 1992) and dual control (Ward and Smith 2002).

#### **Principle of Least Privilege**

In an access authorisation perspective, principle of least privilege demand that users to be assigned minimum amount of privileges to perform their tasks and no more (Ferraiolo and Kuhn 1992; Sandhu et al. 2000; Sandhu et al. 1996; Schneider 2000; Kissel 2013). Another similar but subtly different perspective of least privilege is offered in some information systems security literature (Saltzer and Schroeder 1975; Schneider 2003) which state that users must only use the minimal subset of privileges available to them in a achieving a task.

Despite least privilege being an accepted authorisation security principle for a long time research points out many instances where this principle is being violated. A research carried out by Motiee et al. (2010) have found that 69% of the participants did not enforce this

principle in the Microsoft Windows Operating System they were using. Cappelli et al. (2012) describe some insider threat event which occurred as a result of the non-enforcement of this principle (a detailed analysis of these insider threat events are presented in Chapter 4).

### **Principle of Separation of Duties**

Principle of separation of duties is mainly aimed at preserving the integrity of commercial information systems (Clark and Wilson 1987). According to this principle a single person is not allowed to complete a set of tasks related to the same business function in order to mitigate the risk of fraud (Simon and Zurko 1997; Clark and Wilson 1987). As pointed out by Clark and Wilson (1987) separation of duties allow information systems to maintain external consistency by separating system functions that can create a conflict of interest and requiring different users to operate these functions.

Two main implementations of the principle of Separation of Duties is found in the literature – static and dynamic separation of duties (Ferraiolo and Kuhn 1992; Sandhu et al. 1996). Static separation of duties, also called strong exclusion, prohibits the assignment of a single user for two conflicting roles that are made mutually exclusive (Simon and Zurko 1997; Ferraiolo and Kuhn 1992). However, as pointed out by Nash and Poland (1990) sometimes static separation of duties is too rigid for the requirements of the organisations. In dynamic separation of duties a user can be assigned two conflicting roles and the integrity is preserved by dynamically constraining the initiation or transactions of the roles (Simon and Zurko 1997; Sandhu et al. 2000). Simon and Zurko (1997) describe four mechanisms available for implementing dynamic separation of duties. In the first mechanism, called the simple dynamic separation of duty (Ferraiolo et al. 1995), a user is not allowed to initiate two conflicting roles at the same time. The second method, object-based dynamic separation of duty (Nash and Poland 1990) allows user to assume any role and to execute transactions under two conditions – user must have authorisations to perform the transaction on the specific object and user has not executed any other transaction on the same object. Operational Separation of duty (Ferraiolo et al. 1995), the third dynamic mechanism, allows a role to perform transactions provided that the role is not authorised to perform all transactions related to a business function. The fourth dynamic mechanism, called the history based separation of duty (Simon and Zurko 1997) combine the second and third mechanisms and operates based on the access history of the users. These different implementations of separation of duty are indicated in Figure 2-4.

As in the case of least privilege, many instances where organisations have failed to implement separation of duty controls have been found. According to Cappelli et al. (2009) almost half the cases of data integrity violations in order to commit fraud they have discovered occur due to violations of separation of duty.

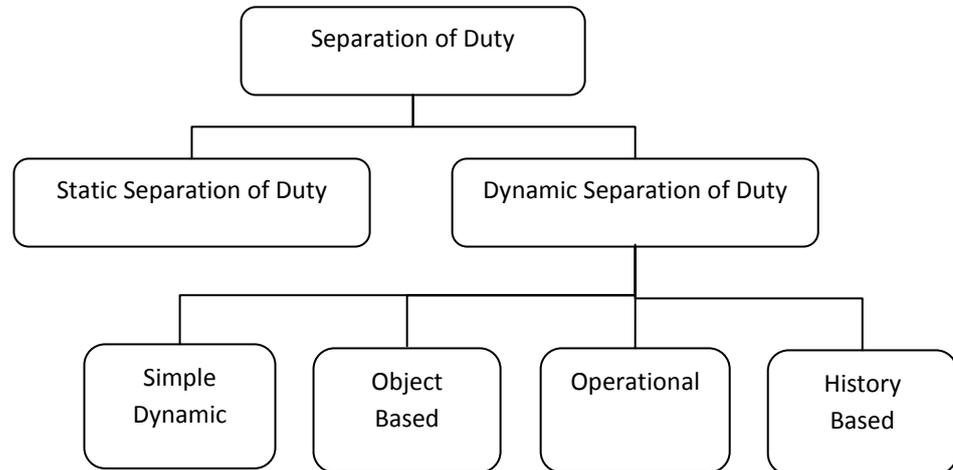


Figure 2-4: Different implementations of Separation of Duty according to Simon and Zurko (1997)

### Principle of Dual Control

Saltzer and Shroeder (1975) claimed that a protection mechanism requiring two keys to unlock is more secure than the one that requires one key. This is the basis of the principle of dual control which calls for a sensitive task or transaction to be carried out with the authorisation of two or more people (Ward and Smith 2002). Principle of dual control is closely aligned with the principle of separation of duty. In fact, Saltzer and Shroeder (1975) termed it “separation of privilege”. However, there is one important difference between the two principles. While separation of duties involves dividing a business function into separate tasks and allocating different users to perform these separate tasks, dual control requires two users performing or authorising the same sensitive task.

The three security principles discussed above – least privilege, separation of duty and dual control guide organisations in authorising information system access. The next topic discusses the literature related to another aspect of information system access illustrated in Figure 2-3 – access control models.

### 2.2.2 Access Control Models

Access control models are high-level, formal representations illustrating how controlled access to information resources can be achieved (Samarati and de Vimercati 2001). This section discusses several prominent access control models found in the research literature.

#### **Access Matrix and the Discretionary Access Control Model (DAC)**

Researchers (Graham and Denning 1972; Lampson 1971; Sandhu 1994; Anderson 1972) have identified the need for access control models which are independent of the information system context and the implementation mechanisms. One of the first models of information system access control is the access matrix proposed by Lampson (1971). Other important contributions by Lampson (1971) include the introduction of the access control model elements (called subjects and objects) and the concept of the information owner. In an access matrix representation, information resources (either passive entities such as files or active entities such as software processes) are modelled as objects. Elements accessing the information resources (software processes) are modelled as subjects (Note: Lampson (1971) uses the term domain instead of subjects). These two model elements have been adopted in almost all subsequent access control models in research literature. The concept of an information owner – an entity responsible for creating and controlling an information resource – is another important feature of this model. In an access matrix row headings represent subjects while column headings represent objects. Each cell in the access matrix specifies the permissions subjects have on the corresponding objects. An example access matrix is illustrated in Table 2-3. Since Lampson's Model (1971) is an abstraction of a closed software system, subjects (software processes) also become objects accessed by other subjects. Although all subjects are software processes, the objects can include passive entities such as files. Graham and Denning (1972) have proposed a more formalised version of the Lampson's Access Matrix Model and introduced the concept of "protection state", which is a particular access configuration of the system. The access-matrix forms the basis of the specification of the popular Discretionary Access Control (DAC) Model (Samarati and de Vimercati 2001; U.S. Department of Defense 1985) which is a further development of the initial model by Lampson (1971). The model is termed discretionary since the access rights to objects are configured in the access matrix at the discretion of the corresponding information resource owners.

Table 2-3: Example Access Matrix (Lampson 1971; Graham and Denning 1972)

	Subject 1	Subject 2	Subject 3	Object 1	Object 2	Object 3
Subject 1	Owner (Control)	Execute	Owner (Control)	Owner	Read	
Subject 2		Owner (Control)		Read		Read Write
Subject 3		Execute			Read Write	

As pointed out by Graham and Denning (1972) it is important to prove a given access control model provides a secure state for an information system to operate. They (Graham and Denning 1972) demonstrated that the DAC Model based on the access matrix can only provide a guaranteed state of security if all the subjects are trustworthy. Theoretically, subjects can be made trustworthy in a closed software system model provided that the software processes do not contain any security vulnerabilities. But this requirement cannot be fulfilled since the software processes always execute tied to identities of human users who are not entirely trustworthy. For example, a human user can use a software process to copy information in a certain object *A* (provided he has the required privileges) and make that information available to other users who did not originally have access to object *A*, by creating a new object *B* and copying the contents of *A* to *B*. Since the user is the owner of the new object *B*, he can readily grant permissions to *B* thereby violating the original restrictions placed on object *A* by its owner. Harrison et al. (1976) have used a more formal approach to analyse the security provided by the access matrix. According to them it cannot be proven that a given sequence of actions by subjects would preserve the security state of a chosen configuration of an access matrix.

### The Lattice Model

The problems in the DAC Model described above are mainly information flow vulnerabilities since it allows information in a given object to be leaked into other objects. In order to mitigate such information flow vulnerabilities Denning (1976) proposed a lattice based model for securing information flows. Lattice model (Denning 1976; Sandhu 1993) consists of five types of elements:

- Objects which are either static or active information resources
- Subjects which are software processes (active resources)
- Set of security classes (also called security classifications or security labels)

- A class-binding operator that specifies the security class of information obtained when information belonging to two or more classes are combined
- A flow relation which indicates information flow from one object to another

Lattice Model (Denning 1976) specifies four axiomatic assumptions and information flows are only allowed from a lower security class to a higher security class. These information flows between classes can be illustrated using lattice diagrams. For example, let's assume an information system with two security classes public (P) and confidential (C). As a further refinement, assume that confidential information is divided into three categories employee data ( $E_c$ ) and customer data ( $C_c$ ) financial data ( $F_c$ ). The information flow from lower classes to higher classes can be illustrated using the lattice diagram in Figure 2-5 where arrows indicate permitted information flows. As illustrated new security classes are obtained by combining information in other classes (e.g., information in  $E_c$  and  $F_c$  can be combined to create new class  $E_cF_c$  which has a higher security level). Information belonging to the lowest class – Public (P) is allowed to flow freely into all other classes (P forms a lower bound for security classes). However, transitive information flows such as (e.g., from P to  $E_cF_c$ ) are not indicated in a lattice diagram.

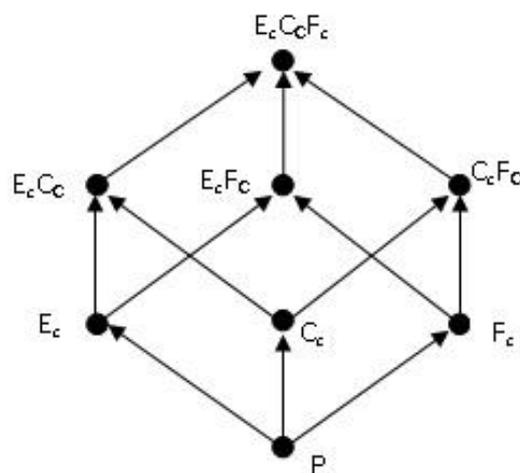


Figure 2-5: Example for Denning's (1976) Lattice Model of Information Flow

### Mandatory Access Control Model (MAC)

Bell and La Padula (1973) have combined a concept similar to secure information flows described in the lattice model and the access matrix to propose a model called the Mandatory Access Control (MAC). In the MAC model authorisations obtained by

referencing the access matrix alone are not enough to for a subject to be given access to an object. In fact, two other model elements add an additional protection mechanism on top of the access matrix – security classification (with reference to subjects this is called a clearance) and categories associated with subjects and objects. Bell and La Padula (1973) have defined two rules that preserve confidentiality using security classifications of subjects and objects. The first rule, called the security condition, states that a subject is only allowed read information from an object if the clearance of the subject is higher than or equal to the classification of the object. The second rule, called the \*- property, states that a subject can only write data to an object if the classification of the subject is less than or equal to the classification of the object. The first rule prevents subjects from reading data from higher classifications while the second rule prevents subjects from leaking data in to objects of lower classifications. Together, these two rules enforce the conditions that satisfy the information flow requirements of the lattice model.

One major problem with the above specification of the MAC model is that it only preserves the confidentiality of an information system. It does not prevent information from objects having lower classifications flowing in to objects having higher classifications. In order to provide integrity using the MAC model, Biba (1977), has proposed two rules. The first rule, which is the complement of the security condition described above, states that a subject is only allowed to read information from an object if the clearance of the subject is lower than or equal to the classification of the object. The second rule, which is the complement of the \*- property described above, states that a subject can only write data to an object if the clearance of the subject is greater than or equal to the classification of the object. It is clear that combining both confidentiality rules of Bell and La Padula (1973) and Integrity rules of Biba (1977) in to a single model will inhibit any information flow between objects of different classification levels. Therefore, some researchers (Sandhu 1993; Lipner 1982) have suggested using a model with separate integrity and confidentiality classifications.

### **Clark - Wilson (1987) Model**

The MAC Model has been developed primarily targeting the military information systems. Therefore, Clark and Wilson (1987) argue that it does not represent the requirements of the commercial information systems. According to them integrity is the primary security concern for commercial information systems and such systems do not conform to the mandatory standards of the MAC Model. The alternative model they

propose consists of five types of elements – users, transformation procedures (TP), Integrity Verification Procedures (IVP), Constrained Data Items (CDI) and Unconstrained Data Items (UDI) (Clark and Wilson 1987). TPs are analogous to subjects and IVPs are a special type of subjects responsible for validating the integrity of the data objects. CDIs and UDIs are analogous to objects. The difference between the two model elements arise since UDIs correspond to unverified user inputs while CDIs have their integrity verified. A set of certification rules govern the integrity of the model elements while enforcement rules guide authorisations. Unlike in the Access Matrix, there is a strict distinction between subjects (TP, IVP) and objects (CDI, UDI) in the Clark-Wilson Model since subjects are not treated as objects. There is also a clear decoupling between information system users and subjects. One set of authorisation rules grant TPs (subjects) access to CDIs (objects). A second layer of authorisation rules specify which TPs (subjects) each user is allowed to access and the CDIs (objects) those subjects can access on behalf of the users.

### **Chinese Wall Model**

Another model named the Chinese Wall Model (Brewer and Nash 1989) has been developed targeting commercial information systems. In the Chinese Wall Model subjects directly represent users of a system where as objects represent information stores. Objects are categorised according different conflict of interest classes which is analogous to categories in the Bell – La Padula (1973) Model. Security labels attached to each object consists of two parts – the conflict of interest class and the client organisation identifier. In a given conflict of interest class, a subject is only allowed to access objects belonging to one organisation. This is achieved by maintaining a matrix similar to an access matrix. However, the matrix in the Chinese Wall Model is empty at the initialisation. During the first access attempt a user is free to access any object belonging to any conflict of interest class and the matrix is updated to reflect this access. For any subsequent access by the same subject, the system checks the matrix and access is granted only if one of two conditions are satisfied – either the requested object has to belong to a client for which the subject already has access or it should belong to a conflict of interest class not previously accessed by the subject. This way a subject can never gain access to the information belonging to two different client organisations in the same conflict of interest class. The role of the access matrix is to keep track of successful access attempts instead of specifying authorisations of subjects. Since there can be occasions where an employee needs to access data belonging to two separate client organisations in the same conflict of interest class, the model

specifies a separate low-security category called the sanitised information. This category holds data objects of all client organisations in an anonymous form. However, this requirement may be difficult to achieve in a practical scenario. A serious limitation of the Chinese Wall Model is that it is mainly focused on protecting client information held by an organisation. This may suit some organisations such as consultancy firms as illustrated by Brewer and Nash (1989) but it does not provide adequate controls to model a general case. However, researchers (Brewer and Nash 1989) demonstrate refinements that make the Chinese Wall Model compatible with other general models such as Bell-La Padula (1973) and Clark-Wilson (1987).

One problem with all the access control models discussed so far is that they do not scale well according to the requirements of large organisations with thousands of users and information resources (Ferraiolo et al. 1995). For example, in a discretionary access control model access matrix needs modification for each new user and information resource. Similar modifications must be carried out when a user is reassigned privileges or leaves an organisation. The Role Based Access Control Model described next offers a solution to this administrative burden.

### Role Based Access Control (RBAC)

Another access control model, which is being widely used, is the Role Based Access Control (RBAC) (Ferraiolo and Kuhn 1992). There are three main modelling elements in RBAC – users who access information resources, roles which can be viewed as either job functions or sets of transactions users are allowed to perform, and objects which are passive information containing entities. The distinct feature of RBAC is the separation of users and roles as model elements. This allows two layers of assignments to take place in RBAC as illustrated in Figure 2-6 – users are assigned for roles and roles are authorized to perform specific transactions on objects.

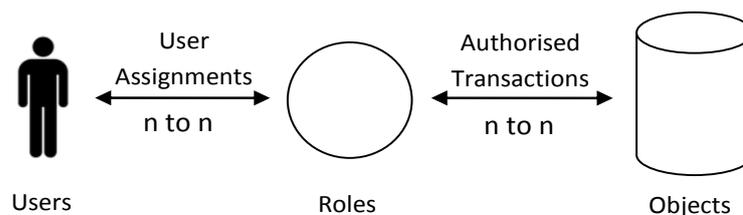


Figure 2-6: Role Based Access Control (RBAC) based on Ferraiolo and Kuhn (1992)

Role assignments for users are many to many relationships – users may have multiple roles and a given role may be assigned to more than one user. Similarly, many-to-many relationships exist between roles and objects. The transactions used in RBAC could be permissions (such as read or write) bound to specific objects or sets of actions similar to a transformation procedures in the Clark-Wilson Model (1987). Researchers (Ferraiolo et al. 2001; Sandhu et al. 1996; Sandhu et al.2000) have also proposed enhancements to the RBAC model to include role hierarchies and constraints enforcing separation of duties.

As pointed out by Ferraiolo et al. (1995), RBAC does not suffer from the administrative burden of the access control models described earlier since organisations are structured around job roles. Adding a new user is straightforward as assigning him to the relevant roles and there is no need to change the permissions of all information resources since the permissions are bound to the role. However, RBAC does not support the use of intrinsic characteristics of the users (e.g., whether a contractor or an internal employee) other than the job role, intrinsic characteristics of the object (e.g., criticality of the resource) or contextual features (e.g., whether access request is coming from the local network or a remote network) in making access decisions. Incorporation of such characteristics in deciding whether to permit or deny access is vital for preventing insider threats.

### **Attribute Based Access Control (ABAC)**

Attribute Based Access Control (ABAC) (Wang et al. 2004; Yuan and Tong 2005; Hu et al. 2014) is a more recent development proposed to overcome some of the limitations of the earlier access control models. All the access control models discussed so far assign static permissions for subjects (or roles in the case of RBAC) to access objects. In ABAC, specific access control policies created using a policy definition language, such as the eXtensible Access Control Markup Language (XACML) (Godik et al. 2002), provide rules to determine whether access could be granted or denied to the requested object thereby eliminating the need for the static assignment of permissions (Hu et al. 2014; Yuan and Tong 2005). Therefore, ABAC is sometimes called Policy-Based Access Control (PBAC) (Karp et al. 2009). Access control policies in ABAC can incorporate three types of attributes to specify the access control rules – subject attributes (e.g., whether the subject is a contractor or an internal employee), object attributes (e.g., criticality of the information resource), and environmental attributes (e.g., whether access request is coming from the local network or a remote network) (Yuan and Tong 2005). The ABAC mechanism decides whether to grant or deny access by checking these attributes against the access policies as illustrated in

Figure 2-7. Therefore, ABAC model provides better protection against insider threats by using contextual factors in making dynamic access control decisions. As shown by Jin et al. (2012), ABAC is also compliant with the earlier access control models such as DAC, MAC and RBAC.

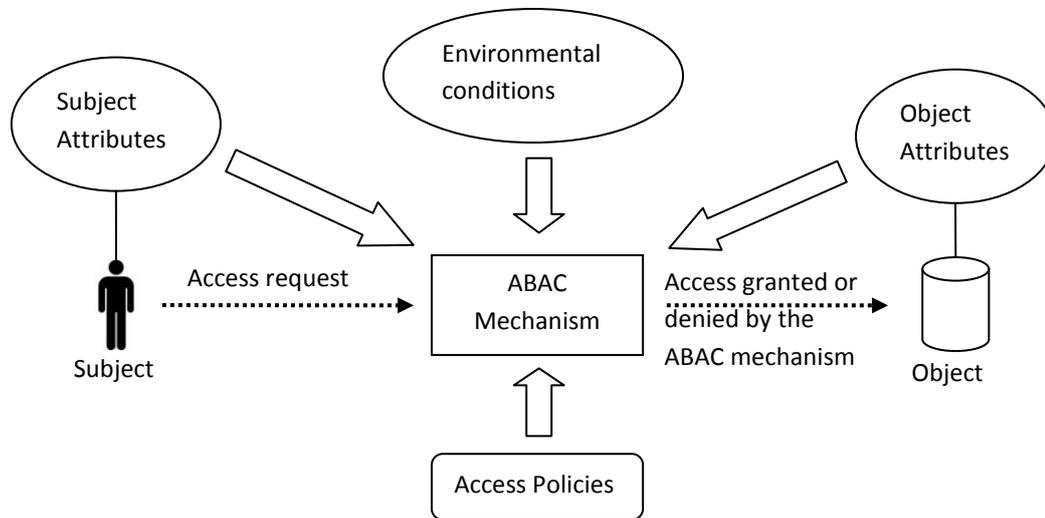


Figure 2-7: Basic ABAC Model as defined in NIST SP 800-162 (Hu et al. 2014)

### Risk-Adaptable Access Control (RAdAC)

Risk-Adaptable Access Control (RAdAC) is an enhancement of ABAC model that was originally proposed by the National Security Agency, U.S.A targeting military information systems (McGraw 2009). The primary enhancement proposed in RAdAC model is the introduction of a risk-based dynamic access control decision process. According to the model presented by McGraw (2009) the access control mechanism (this would replace the ABAC mechanism illustrated in Figure 2-7) makes the decision based on two factors:

1. The security risk of access calculated real-time based on factors such as criticality or sensitivity of the information resource, trust level of the user, job role of the user and other contextual attributes. (Note that these factors are categorised as subject attributes, object attributes and environmental conditions in the ABAC model)
2. The operational need to access information

Another enhancement in the RAdAC is the access policies that can dynamically weigh security risk and the operational need criteria. McGraw (2009) also propose the use of heuristics based on past access decisions to continuously improve the access policies and the decision making process. A more formal framework for RAdAC has been proposed by

Kandala et al. (2011) while some of the methods that could be used for the risk assessment are presented by Cheng et al. (2007b; 2007a) and Ni et al. (2010).

### **Discussion of access control models**

A comparison of all access control models discussed so far is presented in Table 2-4. All access control models depend on correct authentication of the user and using a unique user identification (Sandhu and Samarati 1996). Although objects always relate to information resources in access control models the definitions of subjects differ. In the DAC, MAC and Clark-Wilson models subjects represent software processes while in Chinese Wall, RBAC, ABAC and RAdAC models subjects denote information system users. Some access control models such as MAC primarily focus on the confidentiality aspect while others like the Clark-Wilson model enforce the integrity of information systems. The specification of authorizations also differ between access control models - DAC model uses a single layer of authorisation by using the access matrix, MAC model has an additional step based on the security labels (attributes), RBAC has a two layer authorisation process, Chinese Wall Model allows for dynamic authorizations based on previous object access and ABAC/RAdAC allows dynamic authorisations based on a range of factors. All models are flexible regarding the granularity of objects – they can be databases, files or even individual data fields within a data store.

It is clear that historically security researchers relied on closed, technical abstractions of information systems to develop access control models. They deliberately left out contextual factors of users and organisations from their models. As discussed earlier, in the Discretionary Access Control (DAC) Model Graham and Denning (1972) state that the required level of protection can only be provided if the subjects are always trustworthy. They recommended the problem of the untrustworthy subjects to be handled through “external regulation” and the deployment of separate mechanisms for detecting violations. Similarly, Clark and Wilson (1987) argue that the access control models should ensure the internal consistency, which only accounts for the technical component of the information systems. They recommend security principles, such as separation of duty for the preservation of external consistency meaning that human and organisational aspects are left out from the access control model specification. However, researchers have gradually realised the importance of including contextual factors in access control models. The concept of roles played by the users has been introduced in the Role Based Access Control Models (Ferraiolo and Kuhn 1992). The more recent models – ABAC (Hu et al. 2014) and

RAAdAC (McGraw 2009) allow the inclusion of a range of contextual factors through subject attributes, object attributes and environmental factors.

Table 2-4: Comparison of Access Control Models Described in this Chapter

Model	Model Elements	Authorisations	Diagrammatic Representation
Access Matrix based DAC Model (Lampson 1971; Graham and Denning 1972)	<ul style="list-style-type: none"> <li>Subjects – Software processes executing on behalf of users</li> <li>Objects – All subjects and other data sources such as files and databases</li> <li>Users are implicit in the model and a subject is always bound to a single user</li> </ul>	<ul style="list-style-type: none"> <li>Access matrix specify which subjects have access to which objects</li> <li>Common authorisations include read, write, execute and control</li> <li>Static assignment of authorisations</li> </ul>	
Lattice based MAC Model (Denning 1976; Bell and LaPadula 1973)	<ul style="list-style-type: none"> <li>Subjects – Software processes executing on behalf of users</li> <li>Objects – Entities which contain information</li> <li>Attributes of objects: Security classification and category</li> <li>Attributes of users: Security clearance of users and need-to-know criteria (list of categories user is authorised for)</li> <li>Subjects operate with the clearance and categories bound to the user.</li> </ul>	<ul style="list-style-type: none"> <li>Two levels of authorisations</li> <li>The first level uses an access matrix and is identical to the DAC model</li> <li>Second level checks the users clearance and need-to-know criteria against the classification and category of the object</li> </ul>	
Clark and Wilson (1987) Model	<ul style="list-style-type: none"> <li>Transformation Procedures (TP) – equivalent to subjects in DAC and MAC models</li> <li>Constrained Data Items (CDI) and Unconstrained Data Items (UDI) – Equivalent to Objects</li> <li>Integrity Verification Procedures (IVP) – Special type of TP responsible for verifying integrity of CDIs</li> <li>Users</li> </ul>	<ul style="list-style-type: none"> <li>Users are authorized to access TPs and these TPs are authorised to manipulate specific CDIs.</li> <li>Authorisations are maintained in a set of relations in the form: (user, TP1(CDI1, CDI2,...CDIn), .... TPn (CDI1, CDI2,...CDIn))</li> </ul>	

table continued on next page.....

table continued from previous page...

Model	Model Elements	Authorisations	Diagrammatic Representation
Chinese Wall Model (Brewer and Nash 1989)	<ul style="list-style-type: none"> <li>Subjects- Users</li> <li>Objects – Information stores</li> <li>Security Label: This label consists of two parts – conflict of interest class and client company ID.</li> </ul>	<ul style="list-style-type: none"> <li>Authorisations are defined dynamically based on the security labels accessed by the subject previously.</li> <li>A matrix of subjects and objects is used to record access information</li> </ul>	
Role Based Access Control (RBAC) (Ferraiolo and Kuhn 1992)	<ul style="list-style-type: none"> <li>Users</li> <li>Roles – Job functions or groups of transactions performed by users</li> <li>Objects – Information stores</li> </ul>	<ul style="list-style-type: none"> <li>Users are assigned for roles</li> <li>Roles are authorised to perform transactions on objects</li> </ul>	
Attribute Based Access Control (ABAC) (Hu et al. 2014) and Risk-Adaptable Access Control (RAAdAC) (McGraw 2009)	<ul style="list-style-type: none"> <li>Subjects – Users</li> <li>Objects – Information resources</li> <li>Subject attributes</li> <li>Object attributes</li> <li>Access policies</li> <li>Environmental conditions</li> <li>Access control mechanism</li> </ul>	<ul style="list-style-type: none"> <li>No static authorisations</li> <li>Dynamic authorisations based on subject attributes, object attributes, environmental conditions and access policies specified.</li> </ul>	

The trend towards the inclusion of contextual factors in access control models is a parallel development with the increased research on socio-technical aspects of information systems security. Similarly, any access risk assessment carried out with the aim of mitigating insider threats must also factor in socio-technical and contextual aspects. The next section evaluates research literature on information systems security risk assessment (which includes access risk assessment) and evaluates whether the proposed risk assessment methodologies incorporate socio-technical factors.

## 2.3 Information Systems Security Risk Assessment

Organisations typically approach information systems security risk assessments in a top-down manner. First, they select standards or high-level methodologies (simply referred to as standards from this point onwards) prescribed for information security risk assessment based on factors such as compliance or regulatory requirements, available expertise as well as time and resource constraints. The frameworks specified in the standards are then executed using lower-level methods, models and metrics to analyse security risks. This section begins with a discussion of high-level information systems security risk assessment standards followed by an analysis of lower-level methods, models and metrics available for security risk analysis with a particular focus on their suitability for modelling socio-technical aspects related to information systems access.

### 2.3.1 Information systems security risk assessment standards

Well established standards guide organisations in performing information systems security risk assessments. Numerous standards are used by information systems security professionals and it is not practical to present all of them in this literature review. Therefore, three of the most frequently used and widely accepted standards are discussed here:

- ISO/IEC 27005:2011 - *Information technology - Security techniques - Information security risk management* standard (International Organisation for Standardisation 2011)
- NIST SP 800-30 Revision 1– *Guide for Conducting Risk Assessments* (National Institute of Standards and Technology 2012)
- OCTAVE - *Operationally Critical Threat, Asset, and Vulnerability Evaluation* (Alberts et al. 2003).

#### ISO/IEC 27005:2011

The core risk assessment activities embedded in the wider risk management framework of ISO/IEC 27005:2011 (International Organisation for Standardisation 2011) consists of three phases – *risk identification, risk analysis and risk evaluation*. Risk identification phase is concerned with identifying information resources, security threats to them, potential vulnerabilities and existing controls. Risk analysis deals with the analysis of risks and

estimation of the level of risk either qualitatively or quantitatively. Risk evaluation is concerned with making risk mitigation decisions based on the risk values obtained from the previous risk analysis phase.

### **NIST SP 800-30 Revision 1**

In the NIST SP 800-30 Revision 1 (National Institute of Standards and Technology 2012) standard risk assessment activities are divided into five distinct phases. The first phase deals with the identification of security threats and potential threat sources. The second phase is concerned with identifying vulnerabilities that may be exploited by the threat sources and the predisposing conditions that either increase or decrease the likelihood of threat events. Determining the likelihood of occurrence of threat events envisaged in phase one while considering the vulnerabilities and predisposing conditions elaborated in phase two is performed under the third phase of the standard. The fourth phase deals with determining the adverse impacts of threat events while the risk is determined based on the impact (determined in stage 4) and likelihood (determined in stage 3) during the fifth phase.

### **OCTAVE**

The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) is a risk management methodology developed by the Software Engineering Institute of the Carnegie Mellon University, USA (Alberts et al. 2003) consisting of three main phases. The first phase, called *build asset-based threat profiles*, creates profiles of threats, vulnerabilities and information assets using data collected from managers and other staff members. The second phase - *identify infrastructure vulnerabilities*, deals with the identification of key IT infrastructure assets and the analysis of their vulnerabilities in a technological standpoint. Actual risk assessment and the development of strategies to mitigate the identified risks is carried out under the third phase termed *develop security strategy and plans*.

### **Summary of information systems risk assessment standards**

The security standards for information systems security risk assessment described above consist of similar set of activities. The mapping between the activities of the three information systems security risk assessment standards are given in Table 2-5, where similar activities appear across the same row.

Table 2-5: Comparison of the risk assessment activities prescribed in three standards -ISO/IEC 27005:2011, NIST SP 800-30 Revision 1 and OCTAVE

<b>ISO/IEC 27005:2011 (International Organisation for Standardisation 2011)</b>	<b>NIST SP 800-30 Revision 1 (National Institute of Standards and Technology 2012)</b>	<b>OCTAVE (Alberts et al. 2003)</b>
Risk identification	Identify threat sources and events	Build asset-based threat profiles (Phase 1)
	Identify vulnerabilities and predisposing conditions	and Identify infrastructure vulnerabilities (Phase 2)
Risk analysis	Determine likelihood of occurrence	Develop security strategy and plans (Phase 3)
	Determine Impact	
	Determine risk	
Risk Evaluation	<i>Note: Formulating a risk responses is part of the wider risk management framework prescribed by NIST</i>	

All the risk assessment standards described above provide a high-level framework of activities to be followed while being flexible on the lower-level risk analysis methods, models and metrics to be used. ISO/IEC 27005:2011 standard does not provide any guidance of lower-level risk analysis models, methods or metrics. NIST SP 800-30 Revision 1 provides some detailed guidelines in its appendices based on a impact-likelihood matrix method (National Institute of Standards and Technology 2012) although analysts are free to select methods and models of their choice within the broader framework. The OCTAVE methodology also provides optional guidelines on the risk assessment procedure and the threat models but organisations can use lower-level methods and models of their choice as long as they are compliant with the fifteen *OCTAVE Criteria* (Albert and Dorofee 2001).

Out of the three standards, OCTAVE methodology is more prescriptive toward the inclusion of social and organisational aspects since there is a phase dedicated to organisational analysis. However, in all three standards, inclusion of the socio-technical factors is entirely dependent on the choice of the analyst as well as the availability of suitable risk models, analysis methods and metrics. The following sections present the

analysis methods, models and metrics proposed by the researchers for information systems security risk assessment and discuss their ability to incorporate socio-technical aspects.

**2.3.2 Information systems security risk analysis models**

Numerous models have been proposed for modelling threats, vulnerabilities and risks affecting information systems. The ISO/IEC 31010:2009 (International Organisation for Standardisation 2009) and SA/NZS HB 89:2013 (Standards Australia/Standards New Zealand 2013) describe some of the models used for organisational risk analysis in general. This section discusses some of the prominent models used for information systems security risk analysis.

**Simple Risk Matrix Models**

NIST SP 800-30 Revision 1 (National Institute of Standards and Technology 2012) provides guidelines on using a risk matrix model based on likelihood and impact of criteria of a possible threat event. The cells of the risk matrix are assigned risk levels, in either qualitative or semi-quantitative manner, depending on the values of the impact and likelihood criteria denoted in rows and columns. The example risk matrix given in NIST SP 800-30 Revision 1 (National Institute of Standards and Technology 2012) is illustrated in Figure 2-8.

Likelihood (Threat Event Occurs and Results in Adverse Impact)	Level of Impact				
	Very Low	Low	Moderate	High	Very High
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

Figure 2-8: Example risk-matrix given in NIST SP 800-30 Revision 1 (National Institute of Standards and Technology 2012)

**Attack Tree Models**

Attack Tree Model, introduced by Bruce Schneier (1999), is primarily a threat modelling approach that can be used to analyse information systems security risks. Attack Trees model the end goals of an attacker as root nodes and actions that lead to the goal state as child nodes. The pathways in a tree starting from a leaf node to the root represent possible

attack paths. In an Attack Tree, two child nodes can be combined using AND/OR logic to specify the condition which leads to its parent state. The nodes of the tree can be assigned likelihood criteria, either qualitatively or quantitatively, to calculate the cumulative likelihood of an attack path. Attack Trees have been widely used in information system risk analysis. Byres et al. (2004) and Ten et al. (2007) demonstrate the use of Attack Trees for the vulnerability assessment of Supervisory Control and Data Acquisition (SCADA) systems. Ray and Poolsapassit (2005) have used Attack Trees for the dynamic insider risk assessment so that alarms could be raised if the risk increases beyond a certain threshold. In their model, each attack step (node) is assigned a probability of an attacker reaching the state. As an insider progress through the steps (nodes), toward the ultimate goal of system compromise (denoted by the root), Attack Tree can be used to calculate a cumulative probability of success and action could be initiated if the cumulative probability reaches a threshold. Figure 2-9 illustrates an example Attack Tree presented by Ray and Poolsapassit (2005).

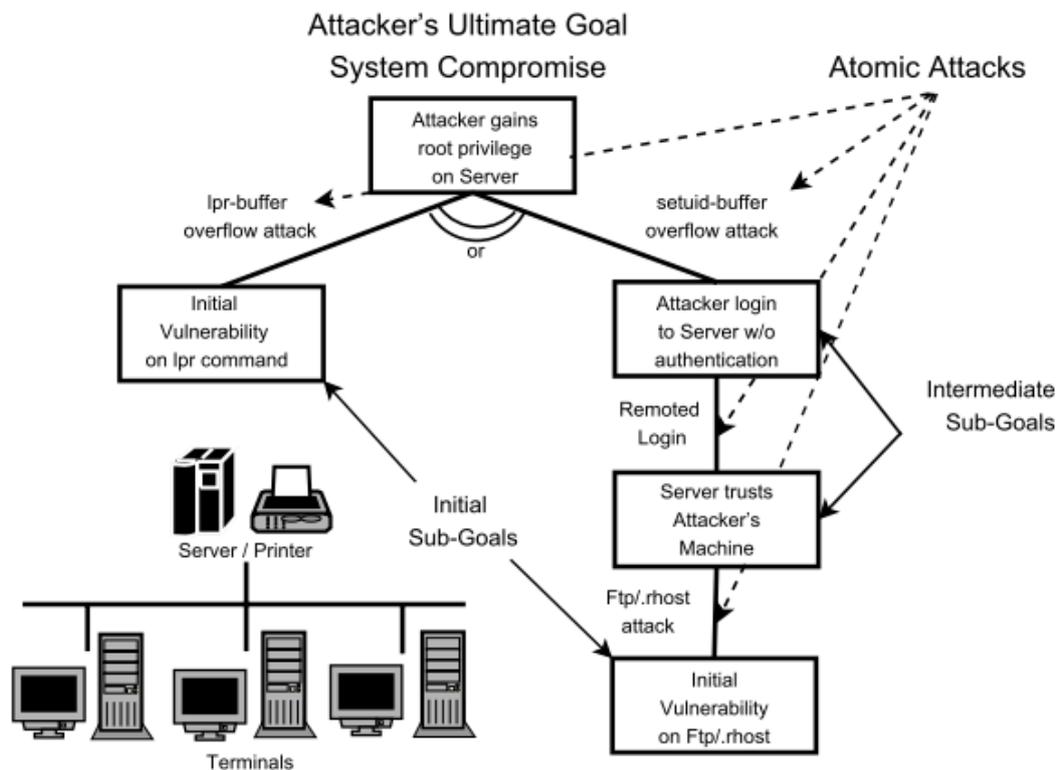


Figure 2-9: An example Attack Tree illustrated by Ray and Poolsapassit (2005)

### Fault Tree and Event Tree Models

Fault Trees (Lewis 2006; Clemens 2002) are a very similar conceptualisation to the Attack Trees. The difference between the two models is that Attack Trees model attack states in

the perspective of an attacker while the Fault Trees model threats or vulnerabilities that could cause a compromise in the perspective of the defender. Fault Tree mapping is initiated from a compromised state (fault), which becomes the root node and branches down by listing the causes that could result in the compromise. Similarly to the Attack Trees, probability of occurrence can be associated with each node of a Fault Tree to calculate the overall risk of a compromise. Therefore, Fault Trees can be used to calculate the likelihood of adverse security events.

Event Trees (Lewis 2006; Satoh and Kumamoto 2009), on the other hand, map consequences of a compromise as a sequence of events starting from the initial compromised state, which becomes the root node. All possible states, both positive and negative, that could occur after the initial security events are listed along with their conditional probabilities. Since Event Trees enumerate consequences of adverse security events, they can be used to calculate the probability of occurrence of each consequence. If the impact of each consequence is estimated, risks associated with each consequence can be calculated. Volume 17 of the OCTAVE Method Implementation Guide (Alberts and Dorofee 2001) contains some example Event Trees used to enumerate the consequences of security events and qualitative specification of their impacts. Lewis (2006) illustrates how Fault Trees and Event Trees can be combined to analyse security risks in SCADA systems. Satoh and Kumamoto (2009) provide another example application of event and Fault Trees in the analysis of information systems security risks. An example Fault Tree for SCADA failures, illustrated by Lewis (2006, 232), is give in Figure 2-10.

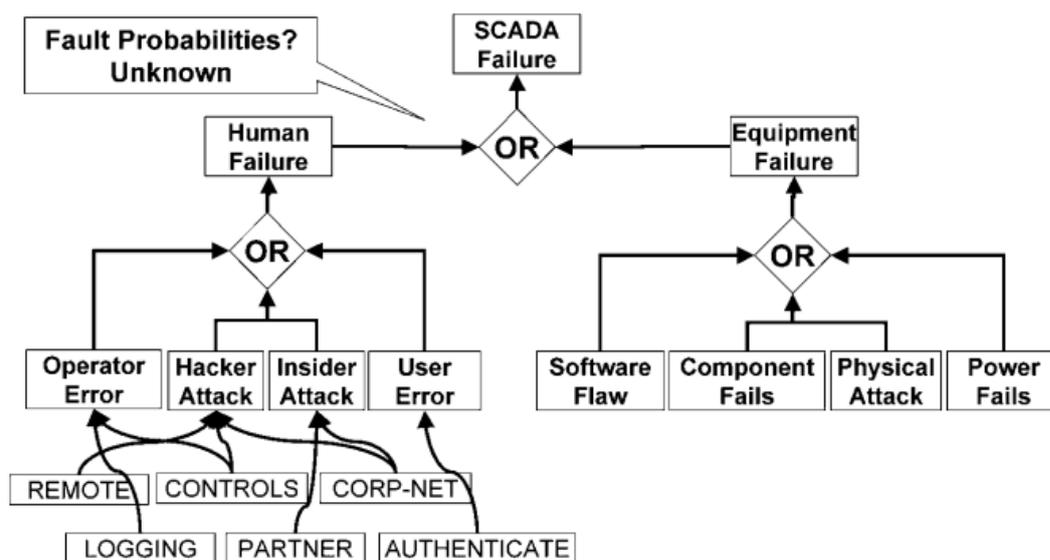


Figure 2-10: Example SCADA fault-tree illustrated by Lewis (2006, 232)

### Privilege Graphs and Attack Graph Models

Privilege Graphs (Dacier and Deswarte 1994; Dacier et al. 1996) and Attack Graphs (Phillips and Swiler 1998) are two modelling techniques that can be utilised to model information systems security threats. Both Privilege and Attack Graphs use very similar model specifications – attack states are represented by nodes and steps taken by an attacker to move from one stage to another are modelled as links. Attack and Privilege Graph Models estimate the likelihood of an attack succeeding using metrics based on the path lengths of the graphs. Parameters such as the time taken for an attack to be executed and the effort required are used to estimate the probability of the state transitions or the links weights (Dacier et al. 1996; Phillips and Swiler 1998). Since these two graph models are always instantiated in relation to one or more attack types or threats, they are primarily threat modelling approaches. The two models are also similar to Attack Trees described earlier since they enumerate attack states. However, unlike in Attack Trees, likelihood criteria in Privilege and Attack graphs are associated with links. Also, it is theoretically possible for them to have cycles due to the properties of the graph structures. Although researchers (Dacier et al. 1996; Phillips and Swiler 1998) have not attempted to assign impacts of the security events to the Privilege and Attack Graphs, such an assignment would facilitate the calculation of risks associated with each attack path. Figure 2-11 shows an example Privilege Graph illustrated by Dacier et al. (1996).

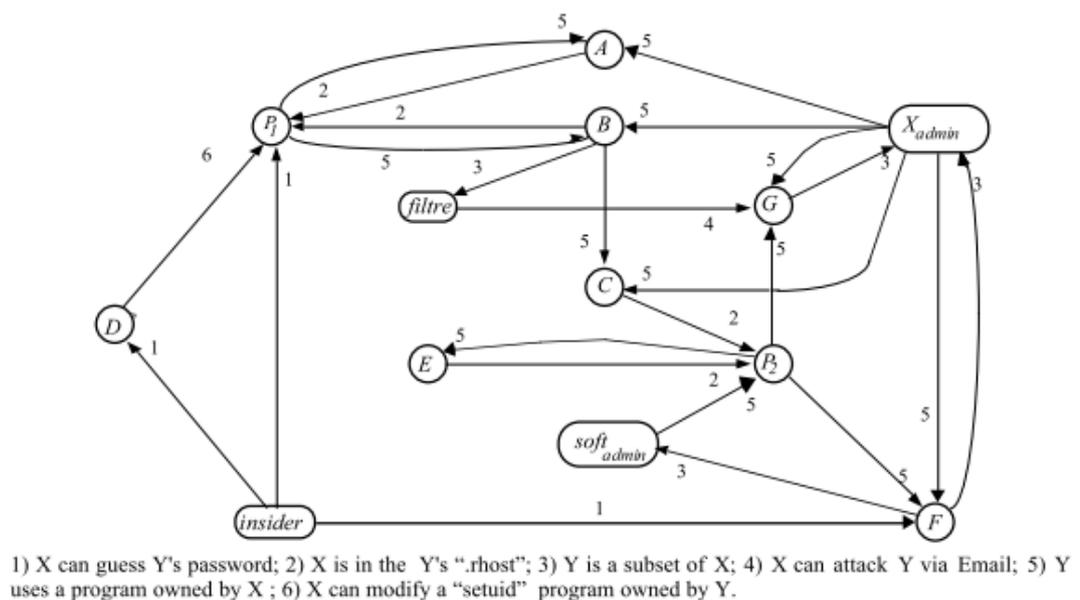


Figure 2-11: Example Privilege Graph illustrated by Dacier et al. (1996)

### **Other Graph Models**

In addition to Attack Graphs and Privilege Graphs, many other types of graph-based models proposed for security risk analysis can be found in the research literature. For example, a modelling approach known as Key Challenge Graphs have been introduced by Chinchani et al. (2004, 2005), which address some shortcomings in Privilege and Attack Graphs. Nodes of a Key Challenge Graph are used to model “any physical entity on which some information or capability can be acquired” (Chinchani et al. 2005). This is somewhat similar to the definition of a node in Privilege and Attack Graphs, but it gives the flexibility to represent any information resource of an organisation. The edges in Key Challenge Graphs are also more generic since they model either access or communication paths. Similar to the link weight criteria of the two graph models described earlier, costs of violating security controls are represented as link weights in the Key Challenge Graphs. Furthermore, attack costs in Key Challenge Graph Models do not depend on the attack path since attackers actions are not confined to a single path across a graph. Instead, the cumulative attack cost is calculated based on the number of compromised hosts and the cost of breaching security controls in each of them.

Another graph-based modelling approach has been proposed by Althebyan and Panda (2007) for the real-time detection of insider threats. Their model uses two types of graph structures – Knowledge Graphs and Dependency Graphs. Knowledge Graphs consist of two types of nodes – information objects and knowledge units acquired from the information objects. Links denote either relationships between knowledge units or bi-partite relationships between knowledge units and corresponding objects. On the other hand, Dependency Graphs denote relationships between information objects such as one object accessing another. The risk values for clusters of documents accessed by a given user are calculated based on the number of documents in the cluster and their relative importance.

### **Bayesian Network Models**

A Bayesian Network Model is an acyclic, directed graph where nodes represent variables and links represent causal relationships or dependencies between the variables (Weber et al. 2012). Since each node is associated with a conditional probability that depends on others, Bayesian Networks are ideal for the estimation of likelihood criteria of threat events using the information available to the analyst.

For example, Ekelhart et al. (2009) have proposed a risk management framework that uses Bayesian Network Modelling to estimate the likelihood of a threat event. The model uses three variables – initial estimated likelihood of the threat event, likelihood of other threats that affect the threat event of concern and likelihood of and adversary exploiting the related vulnerabilities. Maglogiannis et al. (2006) have used a Bayesian Network Model of a patient monitoring system to find out the threats that create the highest risks to the system.

Many researchers have utilized Bayesian Networks to estimate the likelihood of threats modelled as Attack Graphs. A good example for this approach is the risk assessment model proposed by Dantu et al. (2004). Since Attack Graphs represent states of an attack characterised by factors such as connections between hosts involved, sequence of vulnerabilities exploited and attacker capabilities, Dantu et al. (2004) treat them as Bayesian Networks. They demonstrate the calculation of Bayesian Probabilities associated with different attack paths of the network given the initial likelihood estimates. The calculated probabilities can be compared to predict the most likely path that an attacker with given capabilities would take. An information resource is associated with many attack paths as well as many attacker profiles (attackers with different capabilities can attempt to compromise the same resource). Dantu et al. (2004) point out that if all these attack probabilities are calculated, they can be used to deduce a risk measure for the information resource. Frigault and Wang (2008) also combine Attack Graphs and Bayesian Networks for the purpose of assessing the likelihood of exploitation paths.

### **Summary and discussion of models for information systems security risk analysis**

Table 2-6 presents a comparison of the models used for information systems security risk analysis. It is clear that, except for the very high-level matrix models, most models used in the information security risk analysis use either tree or graph based conceptualisations. The risk-matrix based approach is useful once an analyst have other methods to measure the impact and likelihood of threat events. On the other hand, tree and graph based models are used to estimate the likelihood and impact of threat events. Therefore, it is important to analyse whether the models available for estimating the impact and likelihood can incorporate socio-technical factors and their applicability in risk assessments focusing on information systems access.

Table 2-6: A comparison of models used in the information systems security risk analysis

<b>Model</b>	<b>Salient features of the model</b>	<b>Risk metrics used</b>	<b>Applications</b>
Simple risk-matrix (As specified in NIST 800-30 by the National Institute of Standards and Technology (2012))	Uses a matrix of likelihood and impact of attacks as the two axes. Each cell is assigned a risk level based on the impact and likelihood.	Risk metrics are based on two criteria - likelihood and impact.  They can be either qualitative or semi-quantitative	Recommended in the guidelines given in NIST 800-30. Broadly Applicable for all types of information systems security risk assessments.
Attack Trees (Schneier 1999)	Root node represent end goal of the attacker  Child nodes represent activities that lead to the attack  Attack path is a path from any leaf node to the root  One Attack Tree per attacker goal	Risk metric can be qualitative or quantitative.  Risk metric is based on the attack cost (relative likelihood criteria) associated with each node	Risk assessment of SCADA systems - Byres et al. (2004), Ten et al. (2007)  Insider risk assessments - (Ray and Poolsapassit 2005)
Fault Trees	Root node represent final compromised state of a system  Child nodes represent causes or vulnerabilities that contributed to the compromise  One Fault Tree per fault	Typically used with quantitative risk metrics (probabilistic risk assessments)  However, qualitative risk metrics are possible	Risk assessment of SCADA systems – (Lewis 2006)  Generic security risk assessments (Sato and Kumamoto 2009)
Event Trees	Root node represent the compromised state (threat event)  Child nodes represent all possible consequences of the threat event  One Event Tree per threat event	Risk metric is based on likelihood (probability of occurrence)	Examples given in the OCTAVE Method Implementation Guide (Alberts and Dorofee 2001)

Table continued on next page.....

Table continued from previous page .....

<b>Model</b>	<b>Salient features of the model</b>	<b>Risk metrics used</b>	<b>Applications</b>
Attack Graphs (Phillips and Swiler 1998) and Privilege Graphs (Dacier et al. 1996)	<p>Nodes represent attack states</p> <p>Links represent attacker's actions used to step from one state to another</p> <p>Link weights represent cost of moving from one state to another (e.g., time taken, effort required)</p>	<p>Quantitative risk metrics used</p> <p>Risk metric is calculated based on cumulative cost along attack paths (depends on the attack path length)</p>	<p>Generic security risk assessments -</p> <p>Attack graphs (Phillips and Swiler 1998)</p> <p>Privilege Graphs (Dacier et al. 1996)</p>
Key Challenge Graphs (Chinchani et al. 2004)	<p>Nodes represent any physical entity that process or store information</p> <p>Links represent communication or access paths</p> <p>Link weights represent cost of breaching security controls</p>	<p>Quantitative risk metrics used</p> <p>The risk metric is the cumulative cost of threats which depends on the number and cost of hosts compromised</p>	<p>Insider risk assessments (Chinchani et al. 2005, 2004)</p>
Bayesian Networks	<p>Acyclic, directed graphs.</p> <p>Nodes represent model variables</p> <p>Links represent causal relationships or dependencies between variables</p> <p>Each node is associated with a conditional probability</p>	<p>A quantitative risk metric can be deduced based on Bayesian probabilities</p>	<p>Generic risk assessments (Dantu et al. 2004; Ekelhart et al. 2009; Frigault and Lingyu 2008)</p>

It is clear from the discussion of access control models, presented in Section 2.2.2, that the newer models such as ABAC and RAdAC incorporate factors such as subject attributes, object attributes as well as other contextual and organisational factors. The models used for information system access risk analysis should be able to incorporate similar factors.

Attack Trees can be used to map possible states of a threat event in either a technical or a socio-technical perspective. However, none of the Attack Tree Models found in the literature shows how subject characteristics, object characteristics and contextual factors can be used in risk calculations. One possibility is to model these characteristics as attributes of tree nodes and using them to calculate the likelihood of occurrence of each state. Another problem with Attack Trees is the difficulty of modelling relationships between various entities such as subjects and objects. Since one Attack Tree is instantiated per attacker goal, it is primarily a threat centric conceptualisation of information system security risks. Threat centric nature of Attack Trees poses two challenges in terms of scalability. First, the number of attacker end goals (or threat event types) faced by an organisation can be very large, each requiring a separate Attack Tree. Second, there can be a large number of ways to execute a socio-technical access threat event making the individual Attack Trees very complex, making it difficult to analyse them and to formulate effective mitigating strategies. Fault Tree and Event Tree models also suffer from similar problems.

Privilege and Attack Graphs are also threat centric models that map states of an attack. A list of vulnerabilities related to the particular organisation must be known before the model instantiation to use Attack and Privilege Graphs. However, one objective of the socio-technical access risk assessment is to identify and analyse security risks in a given access configuration and it is difficult for the analyst to have a set of access vulnerabilities identified beforehand. Furthermore, Attack and Privilege Graph models are designed to represent breaches centred on escalation of access privileges. However, 43% of the insider breaches reported to CERT|CC have occurred using the legitimate account privileges of the malicious insiders (Randazzo et al. 2005). Most of these insider attacks have occurred due to the allocation of excessive privileges and lack of procedural controls such as separation of duties.

Key Challenge Graphs, specifically proposed for insider threat analysis, provide a higher-level abstraction of organisational information systems access than Attack or Privilege Graphs. Therefore, Key Challenge Graphs are better suited for representing socio-technical aspects. However, Key Challenge Graph models are also threat centric, requiring the analyst to be knowledgeable about the organisational information system access vulnerabilities before the model instantiation. Key Challenge Graphs also do not specify how attributes of subjects, objects and other contextual factors can be included in the risk calculations.

When Bayesian Network models are used for security risk analysis in combination with the Attack Graphs, they suffer from the same problems associated with the graph-based approaches described above. Another difficulty arises in the assignment of apriori probabilities required for the Bayesian Analysis since it is difficult to estimate the likelihood criteria related to threats and vulnerabilities before performing the analysis.

A key problem in all the tree and graph based models discussed so far is that they are threat centric modelling approaches. Hence, they do not provide any means of modelling information systems in a holistic, socio-technical manner in order to facilitate the identification of vulnerabilities (cf. socio-technical models of information systems in section 2.1.1), which is a pre-requisite for any meaningful risk analysis. Therefore, risk analysis models for information systems access security should ideally allow a vulnerability centric approach. Such models will enable analysts to identify socio-technical vulnerabilities in information systems access and calculate the risks by considering the potential likelihood and impact of the identified vulnerabilities.

### **2.3.3 Information systems security risk analysis methods**

A high-level abstraction of the method to be followed in the assessment of information systems security risks are specified in risk assessment standards. Most standards consist of similar set of activities and Table 2-5 provides a comparison of the steps specified in three widely used standards. Using the terminology defined in ISO/IEC 27001:2011 (International Organisation for Standardisation 2011) the *risk identification* and *risk evaluation* phases of risk assessment involve similar set of activities most of the time. However, different activities may be carried out under the risk analysis step depending on the models used. This section discusses the risk analysis methods used with the models described in the previous section (2.3.2).

The analysis methods to be followed with the simple risk matrix models (National Institute of Standards and Technology 2012) are straightforward. Once the likelihood and impacts of the identified risk have been calculated, the risk matrix is used to determine the level of risk either in a qualitative or semi-quantitative manner (refer Figure 2-8 for an example risk matrix).

In Attack Tree Models (Schneier 1999), a tree structure is instantiated for each identified threat event (end goals of the attacker). The general Attack Tree modelling approach

proposed by Schneier (1999) recommend three main steps for the instantiation of Attack Trees – representing the end goal of the attacker as the root node; modelling pre-requisite steps for reaching the end goal as multi-level child nodes; and assigning each child node with a probability, either in a qualitative or quantitative manner, based on criteria such as likelihood or cost of the attack step. Once Attack Trees are instantiated, cumulative likelihoods along attack paths can be calculated to find the most likely (or the lowest cost) attack paths. The likelihood (or cost) value associated with the most likely (or lowest cost) attack path can be used as a risk measure of the particular threat event. However, some researchers have used variations of the above method for different applications of Attack Trees. Ray and Poolsapassit (2005) recommend instantiating an Attack Tree per user in their dynamic insider risk assessment methodology. They also define algorithms for Attack Tree pruning and calculation of attack risks based on probability levels. Lewis (2006) demonstrate how fault and Event Trees can be instantiated in a similar manner to the Attack Trees to analyse SCADA system risks.

Attack, Privilege and Key Challenge Graph modelling approaches consists of two generic steps - Instantiating the models and analysing them to calculate the risks. However, researchers use different techniques to instantiate the graph-based models. Phillips and Swiler (1998) automate the generation of Attack Graphs using three types of inputs - attack templates that represent generic attack patterns, configuration files that detail the configuration of hosts/network and attacker profiles specifying attacker skill sets and the tools he possesses. Taking a more platform specific approach, a software tool for scanning vulnerabilities in Unix based systems and generating Privilege Graphs has been developed by Dacier et al. (1996). Ortalo et al. (1999) have demonstrated this method using a real example. On the other hand, Key Challenge Graph Methodology (2004) relies on security analysts to perform manual model instantiation with the aid of tools available for systems mapping.

There is significant variation among the analysis techniques used with the graph-based risk analysis models. Dacier et al. (1996) calculate a metric called Mean Time To Failure (MTTF) that estimates the mean time taken for an attack to be successful. Markov Chain Models (Ching and Michael 2006) are used for this purpose after applying Petri Nets (Peterson 1981) for Privilege Graph simplification. Phillips and Swiler (1998) recommend three analysis applications of Attack Graphs – discovering attack paths that carry the lowest costs to the attacker, determining countermeasures that are more cost effective to the

defender and simulation of attacks. They (1998) propose the use of Dijkstra's (1959) Shortest Path First (SPF) algorithm to determine the attack paths with the least cost (more likely attack paths). In order to find a set of cost effective countermeasures, researchers (Phillips and Swiler 1998) suggest using what-if analysis to see if a certain configuration would increase the attack cost or not. In order to find the least cost attack, Chinchani et al. (2005) have proposed an algorithm that create permutations of various attack sequences.

### **Discussion of information systems security risk analysis methods**

Review of the risk analysis methods suggests that a wide spectrum of methods and techniques have been proposed depending on the analysis model used and the research objectives. One problem with the majority of the analysis methods is that they primarily calculate risk based on the least cost or shortest attack paths. While finding shortest attack paths may be beneficial quantifying some types of socio-technical information system access risks, such as an insiders' capability to indirectly access information, analysis methods should ideally cover a wider range of risks.

#### **2.3.4 Information systems security risk assessment metrics**

It is widely acknowledged that information security risk management must be guided by the use of appropriate metrics. Savola (2007) quote a management adage – "*you cannot manage what you can't measure*" while emphasising the importance of risk metrics. Jansen (2009) point out that metrics are essential to make objective security risk mitigation decisions. NIST SP 800-55 Revision 1: Performance Measurement Guide for Information Security (Chew et al. 2008) mention four benefits of using security metrics in general – increased accountability by assisting the identification of vulnerabilities and controls applied incorrectly, enabling the measurement of the effectiveness of the security processes and controls, can be used to demonstrate the compliance with laws and regulations and providing quantitative information to aid risk-based security decision making.

A research paper by Courtney (1977) first introduced a quantitative risk assessment metric that assigns monetary values to the security risks. The risk metric calculation proposed by Courtney (1977), based on the impact and likelihood of threat events, is still widely used although the practicality of the assignment of monetary values have been questioned by the security professionals. Jaquith (2007, 33) point out several problems in

the monetary value based metric, typically called the Annualised Loss Expectancy (ALE). According to him, it is very difficult to assign a monetary value to adverse impacts of security threat events. There are many consequences of an adverse security event and it is difficult to define a general case or assign dollar figures to all of the consequences. The lack of industry data further complicates the loss estimation task. Moreover, the other risk assessment metrics found in the research literature such as mean time to failure (Dacier et al. 1996) and attack path cost (Phillips and Swiler 1998) are too narrowly focused to quantify a range of socio-technical access vulnerabilities. At the same time, qualitative indicators of security risks have also been criticised (Jaquith 2007; Munteanu 2006) due to their lack of objectivity. For example, declaring impact of a threat event using risk levels such as high, low and moderate would heavily depend on the subjective interpretations of the analysts.

Therefore, it is desirable to have quantitative risk metrics for the assessment of information system access risks. However, risk metrics based on the assignment of monetary values are inappropriate due to the socio-technical nature of risks as well as the reasons given above.

## **2.4 Conclusions**

### **2.4.1 Summary and the Research Gap**

This literature review started with a discussion of socio-technical aspects of information systems and information systems security (Section 2.1). It is clear that researchers have been emphasising the socio-technical nature of information systems for a long time. Although there is significant variation among the socio-technical models of information systems proposed by the researchers, two common features of the models can be deduced. First, socio-technical models of information systems consist of social and technical entities that are related to each other (How well they intertwine depends on the model used). Second, behaviour and properties of an information system (note that this includes security related properties and behaviour) are a result of the relationships between social and technical entities. This chapter also reviewed the literature related to socio-technical aspects of information systems security and concluded that importance of socio-technical aspects have been acknowledged by the security researchers although the models and conceptualisations they use differ as in the case of socio-technical information system models.

Information system access control models have also gradually evolved to include human, organisational and contextual aspects. Information systems security risk assessment standards on the other hand are high-level frameworks and the inclusion of the socio-technical aspects in a risk assessment mainly depends on the analysts' selection of the lower-level risk assessment models, methods and metrics. However, currently available information systems security risk analysis models are primarily threat-centric and do not facilitate the discovery of socio-technical security vulnerabilities, which is a pre-requisite for any effective risk assessment. The current risk analysis methods and techniques are also geared towards finding the most likely or least cost (in the perspective of the attacker) attack paths and they are not suitable for the analysis of a wide spectrum of socio-technical information system access security risks. At the same time, the risk analysis methods should enable the calculation of quantitative risk metrics that help organisations to make effective security risk mitigation decisions. Based on the two common features of socio-technical information system models and the points discussed above, following requirements of an information system access security risk assessment methodology can be derived:

- Risk assessment model should be able to model important relationships between social and technical entities (subjects, objects and other organisational and contextual factors) involved in the information systems access.
- The risk assessment model should enable the reasoning of behaviour (security related interactions) and properties (e.g., security vulnerabilities, risk level) of the information systems occurring as a result of the relationships between social and technical entities.
- Risk assessment model and method should also facilitate the definition and calculation of a wide range of quantitative risk metrics, which are helpful in making security risk mitigation decisions.

Since none of the risk assessment methods, models and metrics reviewed under this chapter are consistent with the above criteria, a clear research gap exists to develop a suitable methodology, which is the main goal of this research.

#### **2.4.2 Applicable models from other disciplines and research directions**

Developments in the field of network science provide some useful models and methods that could be used to analyse complex interrelationships between various entities. Many

diverse applications of network science are found in the research literature. Some examples include analysis of terrorist networks (Walther and Christopoulos 2012; Krebs 2002; Carley et al. 2003; McCulloh and Carley 2008), political networks (Christopoulos 2006), networks of regulatory agencies (Christopoulos and Quaglia 2009) and online social networks (Pfeffer et al. 2013; Pfeffer and Carley 2012a). Some of the above network science applications relate the structural features to phenomena under investigation while others explore more dynamic aspects. For example, Christopoulos and Quaglia (2009) relate the structural positions of entities in an inter-organisational network to their relative ability to influence regulatory outcomes while McCulloh and Carley (2008) discuss methods to detect change in dynamic networks.

Networks science models and methods have also been proposed for organisational dependency and vulnerability analysis. Krackhardt and Carley (1998) have proposed a network model - called PCANS - that can be used to map the interdependencies between socio-technical entities in an organisation. Their model consists of three entity types – people, tasks and resources as well as relationship types between them. Using a similar model, Carley (2000) proposes the analysis of organisational vulnerabilities in an information security perspective. Carley (2002) has developed the PCANS model further to introduce a representation known as the *meta-matrix* that can be used to characterise entity types in an organisation and relationships between them. An example meta-matrix representation given by Carley (2002) is illustrated in Table 5-2 of Chapter 5. McCulloh et al. (2013) demonstrate how meta-matrix representations can be used to analyse organisational vulnerabilities with the help of metrics.

Meta-matrix models (2002) satisfy the requirements specified in Section 2.4.1 for an information systems access security risk assessment methodology. First, meta-matrix representations can be used to model subjects, objects and other related entity types as well as relationships between them. Modelling such entity and relationship types is important for characterising socio-technical aspects of information systems security. Second, networks instantiated using meta-matrix representations can be used to analyse and reason about security vulnerabilities and risks. This is possible since various structural properties of networks such as centrality (Freeman 1978), clustering (Watts and Strogatz 1998) and structural holes (Burt 1992) can be associated with vulnerabilities and risks. Third, a large number of quantitative metrics have been defined to analyse networks. Wasserman and Faust (1994) provide definitions of common network metrics while Pfeffer

and Carley (2012b) have proposed more computationally inexpensive algorithms to calculate centrality metrics useful for the analysis of larger networks. Furthermore, Carley et al. (2012) document numerous metrics that can be used with networks modelled using meta-matrix representations. Another advantage of using network science techniques is the ability to represent risks visually using network diagrams. Pfeffer (2013) discusses basic concepts of network visualisation in relation to communication networks. In terms of practical implementation of a risk assessment methodology, software tools such as ORA (Carley and Reminga 2004) and Pajek (Batagelj and Mrvar 2002) are available for network analysis and visualisation. Moreover, software libraries such as NetworkX (Hagburg et al. 2008) enable researchers to define new metrics to suit their needs.

### 3. Research Methodology

In order to produce valid results, a research project should state clear objectives and adopt a suitable research paradigm and a methodology. Hence, as a precursor to the presentation of the research outcomes, this chapter discusses the research objectives, epistemological paradigm adopted in this research, the rationale for selecting that paradigm, the research process used and techniques employed to evaluate the research outcomes. Progression of the sub-topics in the chapter is shown in Figure 3-1.

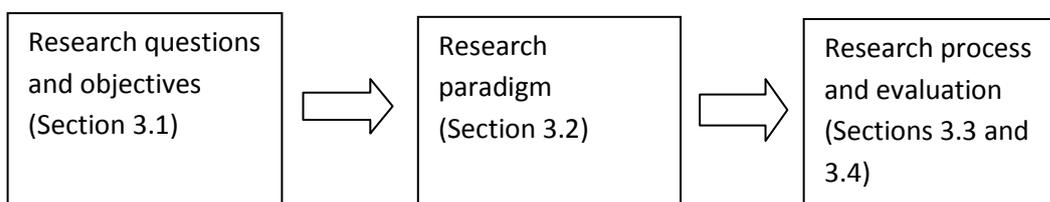


Figure 3-1: Arrangement of chapter sub-topics

#### 3.1 Research Questions and Objectives

The primary objective of this research is to develop a methodology that can be used to assess security risks occurring due to organisational information systems access. The methodology developed in this project provides necessary information for security professionals to mitigate security risks caused by people who have legitimate access to information systems, called insiders. The methodology consists of a risk assessment model, method and metrics.

Accordingly, the high-level research question of this research can be stated as:

- What models, methods and metrics are appropriate for the assessment of security risks occurring due to organisational information systems access?

In order to answer the above question following research sub-questions must be answered:

- Which entity and relationship types must be included in a security risk assessment model of information systems access?
- What factors should be integrated into metrics that can be used to quantify risks related to information systems access?

- What activities (steps) must be carried out to assess security risks related to information systems access?

## **3.2 Research Paradigm**

Research could be carried out based on one of several epistemological paradigms such as positivism, interpretivism, critical research (Orlikowski and Baroudi 1991; livari et al. 1998; Chen and Hirschheim 2004) and design science (March and Smith 1995; Hevner et al. 2004). A researcher's choice of epistemological paradigm is taken primarily based on the research objectives. Positivist research, popular with natural scientists, is mainly aimed at developing hypothesis and then making generalisations by testing that hypothesis whereas interpretivism calls for more subjective interpretations of the phenomena related to human beings rather than attempting to produce generalised laws (Saunders et al. 2011). Critical research takes a critical view of the existing social systems in order to bring change and to overcome inherent conflicts or inequality (Orlikowski and Baroudi 1991). The aim of the design science research paradigm is to create useful artefacts in order to solve important problems (March and Smith 1995; Hevner et al. 2004). This research adopts a design science research paradigm due to the reasons described next.

### **3.2.1 Rationale for the use of design science as the research paradigm**

The following sub-topics describe the rationale for adopting design science as the epistemological paradigm for this research.

#### **Reason 1: Research creates useful artefacts**

As mentioned previously, the aim of design science research is to create artefacts to solve important problems (March and Smith 1995; Hevner et al. 2004). The objectives of this research deals with the creation of artefacts, namely a risk assessment model, method and metrics (together called the risk assessment methodology). These artefacts solve the problems not addressed by existing security risk assessment methodologies as described in the literature review (Chapter 2). The research objectives do not attempt to test a hypothesis (thus eliminating the possibility of a positivist approach) or try to understand and give meaning to human phenomena (thus eliminating the possibility of an interpretivist approach). Hence, the good alignment between the research objectives and primary aim of the design science paradigm gives the most compelling reason for its adoption in this research.

It is useful to articulate the type of artefacts produced in this research in relation to the design science paradigm. According to March and Smith (1995) and Hevner et al. (2004), there are four types of artefacts produced in design science research – constructs, models, methods and instantiations. Constructs refer to the domain specific language and symbols used to define problems or specify solutions where as models use constructs to represent the relationships in a real-world scenario (March and Smith 1995). Methods typically describe the steps in a process of solving a problem while instantiations are real-world realisations of constructs, models and methods (March and Smith 1995). In the information systems security discipline instantiations typically consist of software and hardware systems or tools.

In this research, the risk assessment model developed is an abstraction of entities, their attributes and relationships describing the socio-technical interactions important for security of organisational information systems. Rather than mapping the relationships among the problem and solution domains it provides an abstract representation of the problem space for the definition of metrics and presentation of results in a meaningful manner. The method developed in the research describes the steps to be followed in the risk assessment – starting from collecting necessary data to the presentation of results. Although the third type of artefact produced in the research - the risk assessment metrics, do not fall under the four artefact categories mentioned by March and Smith (1995), they are an important output of this research. Metrics could be conceptualised as artefacts that produce quantitative results by utilising the risk assessment model as well as some additional graph-theoretical and mathematical constructs. The results produced by the metrics are an essential part of the solution space since they guide the security analysts in the estimation and mitigation of risks. Despite not being mentioned under the objectives, this research also produced instantiations of the metrics and the underlying assessment model in the form of software tools. This prototype software tools can be labelled as the fourth type of artefact produced in the research.

### **Rationale 2: Artefacts created in the research are a solution to an important problem**

Another essential characteristic that defines the design science paradigm is that such research attempts to solve important organisational problems (Hevner et al. 2004; Venable 2006b; Peffers et al. 2008; Vaishnavi and Kuechler 2004). This research also meets the above requirement since it makes a contribution toward solving an important problem in the information systems security domain. Organisations currently do not carry out socio-

technical information security risk assessments since available methodologies take a technical perspective. However, such a socio-technical risk assessment is required due to the recent evolutions in the security threat landscape resulting in the emergence of high profile insider threat events. As pointed out by Gartner IT Research (Carpenter and Walls 2011), organisations need to focus on security risks originating from people within their trust boundary (i.e., insiders such as employees). Since the insiders of an organisation have legitimate access to information systems, a purely technical security assessment is futile in mitigating insider threats. Instead, organisations need methodologies to carry out socio-technical risk assessments and artefacts created in this research provide a solution to this problem.

Furthermore, according to Hevner et al. (2004), design science research should be framed with respect to a constituent community. In the case of this research, the constituent community who would benefit from the created artefacts (since these artefacts solve an important problem faced by them) include information security managers, information security auditors, chief information security officers or anyone who has the responsibility of ensuring the availability, integrity and confidentiality of information systems.

It is also important to distinguish design science research from a regular design task in relation to problem solving. Hevner et al. (2004, 81) point out that regular design tasks apply the existing knowledgebase to create artefacts that solves a particular instance of a problem whereas design science research offer solutions to “unsolved problems” using “unique and innovative ways”. Walls et al. (1992, 42) argue that design science research should address “meta-requirements” using “meta-design”. As pointed out by Venable (2006b) this refers to solving a class of problems using a class of artefacts rather than just solving an instance of a problem using existing knowledge. Three features required in a socio-technical risk assessment methodology for information systems access security were deduced in the literature review (refer Chapter 2, section 2.4.1). Developing a methodology that fulfils the three requirements is a problem that remained unsolved by previous research. The solution developed in this research is indeed a unique one since the models, metrics and the method presented in the next chapter has not been applied before for the purpose of socio-technical risk assessment of information system access. Furthermore, the methodology presented in this research is used to assess a class of risks rather than just one risk. There are a thirteen metrics presented in the next chapter belonging to four

classes of risks. If required, information security professionals can use the same risk assessment model and method to develop further metrics or modify the presented metrics to match their organisational risk concerns. Therefore, this research also complies with the problem requirements of design science paradigm envisaged by Walls et al. (1992) and Venable (2006b).

### 3.2.2 Additional design science research requirements

In their seminal paper, Hevner et al. (2004) specify the following guidelines to characterise design science research:

1. Design as an artefact
2. Problem relevance
3. Design evaluation
4. Research contributions
5. Research rigor
6. Design as a search process
7. Communication of research

The first two criteria have been already discussed under section 3.2.1 as the primary reasons for the adoption of the design science paradigm. The third criterion – *design evaluation* is discussed in detail under topic 3.4 – research evaluation. The rest of this sub-topic discusses the remaining design science guidelines (numbered 4-7 in the above list) and how this research fulfils each of them.

#### Research Contributions

Hevner et al. (2004) point out that design science research should make contributions in terms of artefacts and enhancement of the knowledgebase. As mentioned previously, artefacts should offer solutions to “unsolved problems” using “unique and innovative ways” (Hevner et al. 2004, 81). How this criterion is fulfilled by the artefacts produced in this research has been discussed already.

The other type of research contribution relates to the enhancement of the knowledgebase. However, Hevner et al. (2004) do not clearly elaborate what type of contributions to the knowledgebase are acceptable. Nevertheless, numerous researchers (Walls et al. 1992; Markus et al. 2002; Venable 2006b; Kuechler and Vaishnavi 2008) have argued that design science research contributions to the knowledgebase should occur in the form of theories. In terms of the type of theories applicable in design science, Walls et al. (1992) and Kuechler and Vaishnavi (2008) share the view that design theories should be prescriptive while Venable (2006b) argues that design theories should be predictive in nature. These predictive theories, termed “utility theories” by Venable (2006b) predict that the use of certain artefacts generated in a design science research project will provide utility in solving a particular class of problems. Since this research uses Venable’s (2006b) design science process model, due to reasons described later (under section 3.3), theory will be primarily expressed as utility theories. A detailed explanation of the theory formation at each stage of the research is given under the description of research process in section 3.3.

### **Research Rigor**

According to Hevner et al. (2007), rigor in design science is achieved by the use of existing knowledgebase in the construction and evaluation of artefacts. The artefacts constructed in this research are based on existing theories in the knowledgebase. Some of the foundational theories used in the artefacts produced in this research are given in Table 3-1.

### **Design as a search process**

Design as a search process criterion emphasizes the iterative nature of design science research. Hevner et al. (2004) point out that in the information systems discipline it is often difficult to find an ideal solution. This is especially true in the case of information systems security where there has to be a balance between usability and security of information systems. Hevner et al. (2004) recommend carrying out design science research in an iterative manner over several cycles of artefact creation and evaluation until a satisfactory design is achieved. This idea is also incorporated in to all the design science research process models (Vaishnavi and Kuechler 2004; Peffers et al. 2008; Venable 2006b) described in the next section. The research process followed in this project, summarised in

Table 3-3, clearly illustrates the iterative nature of the steps carried out. For example, the initial metrics used for the analysis were taken from the existing network science measures. New metrics were developed later, using the knowledge gained through the evaluation of the initial metrics.

Table 3-1: Some theoretical foundations used to create artefacts in this research

<b>Assumption used or artefact produced</b>	<b>Theories and previous research that provide the basis for the assumption or artefact</b>
Assumption: Information systems security (particularly insider threats and access security) is a complex socio-technical problem.	<p>Socio-technical nature of information systems have been discussed under the socio-technical systems theory (Bostrom and Heinen 1977b, 1977a), Web of Computing Model (Kling and Scacchi 1982) and Socio-Technical Interaction Networks (Kling et al. 2003). Some other notable contributions include Cherns (1976), Clegg (2000) and Mumford (2000).</p> <p>Some of the notable contributions emphasizing the socio-technical aspects of information systems security are: Dhillon and Backhouse (2001), Kraemer et al. (2009), Werlinger et al. (2009)</p> <p>Cappelli et al. (2012) and Cappelli et al. (2009) emphasize socio-technical nature of insider risks.</p>
Artefact: Risk assessment model and method	Risk assessment model and method are based on network analysis and modelling methods (Wasserman and Faust 1994; McCulloh, Armstrong, and Johnson 2013) and more specifically, the concept of meta-networks (Carley 2002)
Artefact: Risk assessment metrics	Foundations for the risk assessment metrics are provided by network metrics already in the knowledgebase. Some notable ones used are: (Ashworth and Carley 2006; Carley et al. 2012; Freeman 1978; Watts and Strogatz 1998)

### Communication of research

According to Hevner et al. (2004) design science research should be communicated to both technical and managerial audiences. The primary research communication of the project is this thesis which is a more technically oriented document. The researcher also carried out an evaluation workshop attended by both a technical and managerial audience. During this evaluation workshop participants received hands-on training to use the artefacts created in the research.

### 3.3 Research Process Models

This section describes the available process models for design science research and the details of the research activities carried out according to the chosen process model.

#### 3.3.1 Design science research process models

According to March and Smith (1995) design science research consists of two distinct phases – *build* and *evaluate*. Build phase deals with the creation of artefacts while they are evaluated in the evaluate phase. The two-stage design science process is endorsed by Hevner et al. (2004) as well. However, the above frameworks do not provide sufficient guidance to be used as design science process models.

On the other hand, Vaishnavi and Kuechler (2004), Peffers et al. (2008; 2006) and Venable (2006a, 2006b) have proposed detailed process models for design science research. The research process model proposed by Vaishnavi and Kuechler (2004) consists of the five steps shown in the mid-section of Figure 3-2.

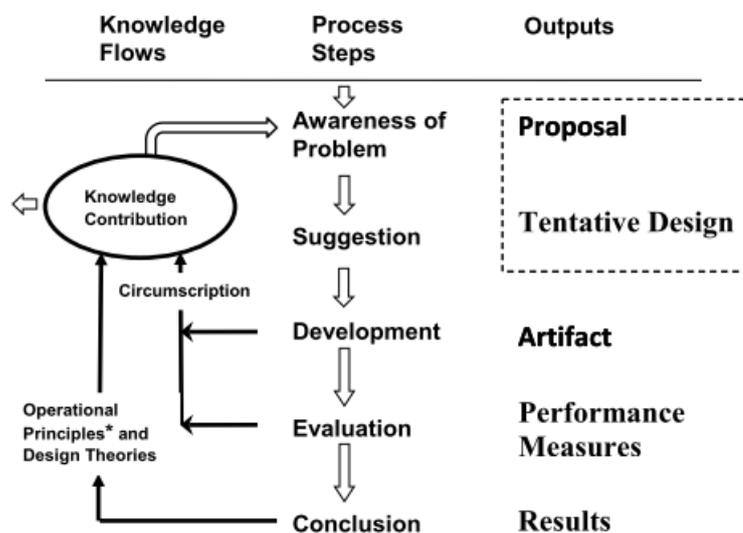


Figure 3-2: Design science research process model proposed by Vaishnavi and Kuechler (2004)

The first step - *awareness of the problem* deals with clarifying and defining the problem to be solved and results in the production of a research proposal. This step again highlights the problem solving nature of design science research. A solution for the problem is envisaged using existing knowledgebase in the next phase termed *suggestion*, which results in a tentative design. Vaishnavi and Kuechler (2004) point out that such a tentative design often forms part of the proposal as well. Therefore, the first two steps in the process model are highly interrelated. The third phase, termed *development*, deals with creating the

artefacts that embody the solution. The developed artefacts are then evaluated in the *evaluation* phase. The evaluation improves understanding of the problem and limitations of the envisaged solution. Therefore, there is a feedback loop from the evaluation phase to the problem awareness and suggestion phases of the research process allowing iterations of these steps. After one or several iterations, the final stage of the research – *conclusion* is reached either due the discovery of an acceptable solution or project termination due to some other constraint (e.g., project reaching its deadline).

The design science research process model proposed by Peffers et al. (2006; 2008) is illustrated in Figure 3-3. The first phase of the model, called *Identify problem and motivate*, encapsulates analysing and defining the problem as well as justifying why it should be solved. The objectives of a solution to this problem are envisaged under the second phase - *define objectives of a solution*. The artefact embodying the solution is created under the next phase termed – *design and development*. Following this step, there are two phases that deal with the artefact evaluation. The first one, called *demonstration*, is used to show that the artefact can be used to solve the problem. The next phase, called *evaluation* is where more formal evaluation takes place by testing the artefact against the solution objectives. The final phase of this model is termed *communication*. Under this phase, the problem, proposed solution and research results are communicated to the wider community using scholarly publications.

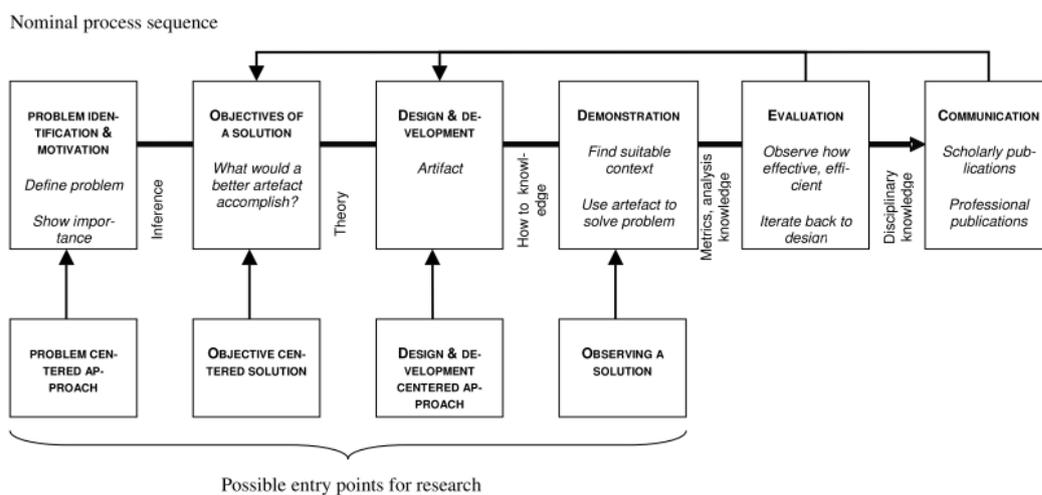


Figure 3-3: Design science research process model proposed by Peffers et al. (2008, 54)

Model proposed by Peffers et al. (2006; 2008) also support revisiting steps iteratively as indicated by the feedback loop in Figure 3-3. Furthermore, the research can be initiated at

any phase using a problem-centred, objective-centred, design and development-centred or client/context initiated approach.

The design science research process model proposed by Venable (2006b) is illustrated in Figure 3-4. As illustrated in the figure, theory building is a central activity in the Venable's (2006b) model. It is a fully iterative model where researcher can follow the activities in any order and revisit any activity according to the requirements. However, a typical design science research project would start from the problem diagnosis phase where the researcher analyses the problem and its causes. Based on the problem analysis researcher would usually form a *utility theory* predicting that a certain technology artefact would be useful in solving the problem (Venable 2006b). This activity falls under the theory building phase. Researchers can then move in to technology design/invention phase where artefacts are created followed by the technology evaluation phase where artefacts are evaluated. Again, there is no strict order to follow and the researcher can move between these steps iteratively.

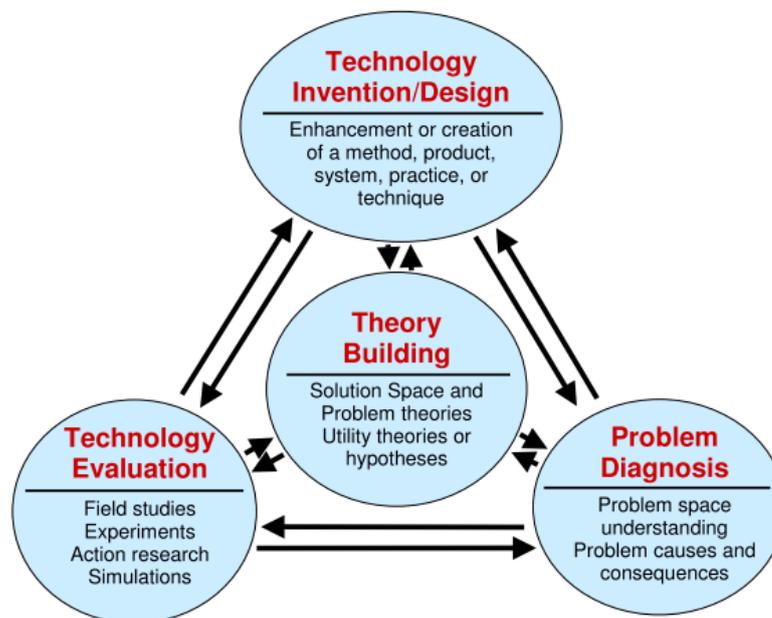


Figure 3-4: Design science research process model proposed by Venable (2006b, 17)

Although three distinct design science process models have been discussed here all of them incorporate a similar set of activities. A comparison of activities in the three design science process models are given in Table 3-2. As shown in the table *awareness of the problem* phase in Vaishnavi and Kuechler's (2004) model is equivalent to the combination of *Identify problem and motivate* and *define objectives of a solution* phases in the model by

Peffer et al. (2008). The same phases are also similar to *problem diagnosis* activity in Venable’s (2006b) model. Similarly, other stages of the three process models can be compared across rows in Table 3-2. There are couple of notable differences between the models as well. Theory building is a central activity in Venable’s (2006b) model, which can occur before or after any other stage of the design science research process. Therefore, theory building activity is depicted as one column spanning the length of Table 3-2 under Venable’s (2006b) model. Theory building in the other two design science models are more implicit and they seem to be indicated by *design theories* (output of conclusion phase) in Vaishnavi and Kuechler’s (2004) model and *disciplinary knowledge* (output of evaluation phase) in the model by Peffer et al. (2008). The other major difference is that there is no phase equivalent to *conclusion* or *communication* in Venable’s (2006b) model.

Table 3-2: A comparison of activities in the three design science process models

		Process Model		
		Vaishnavi and Kuechler(2004)	Peffer et al. (2006; 2008)	Venable (2006b, 2006a)
Research Phase	Awareness of problem	Identify problem and motivate	Define objectives of a solution	Problem Diagnosis
		Suggestion		
	Development	Demonstration	Technology Evaluation	
	Evaluation			Evaluation
		Conclusion		

Since Venable’s (2006b) model is fully iterative it was preferred as a better match for the requirements of this research where artefacts were developed in iterative stages in order to manage complexity. Furthermore, Venable’s (2006b) model facilitates the explicit communication of theoretical contributions of the research at each stage.

### 3.3.2 Stages of the research project

This section explains the activities carried out in each stage of the research project.

Table 3-3 gives a summary of research activities and the phases they correspond to in Venable's (2006b) design science research model while description of each stage is given below. Note that the table lists iterative activities carried out in a linear manner for ease of representation.

Table 3-3: Steps (activities) carried out in the research project and the corresponding phases in Venable's (2006b) design science process model.

<b>Research phase according to Venable's (2006b) model</b>	<b>Summary of activities carried out in each stage of the research</b>
Problem diagnosis	<b>Activity 1: List and categorise details of insider threat events</b> This activity was carried out in order to analyse and identify the type of information system access risks and their causes
Theory building	<b>Activity 2: Initial theory building</b> Initial utility theory was formed for the application of socio-technical risk assessment methodology. Carried out the Initial conceptualisation of artefacts.
Technology design/invention	<b>Activity 3: Develop an initial methodology</b> Developed an initial risk assessment model and explored the use of existing metrics. Developed an initial risk assessment method.
Technology evaluation	<b>Activity 4: Evaluate initial artefacts</b> Artefacts developed in step 3 were evaluated using data collected from one organisation.
Theory building	<b>Activity 5: Reform theory</b> Restated theory based on the evaluation of initial artefacts
Technology design/invention	<b>Activity 6: Enhance model and metrics</b> Enhanced the model and metrics based on the evaluation of initial artefacts carried out in Activity 4 and refinements identified in Activity 5.
Technology evaluation	<b>Activity 7: Evaluate artefacts</b> Carried out the final evaluation of the risk assessment methodology
Theory building	<b>Activity 8: Finalise and report theoretical contributions</b> Finalised theoretical contributions and reported them

**Activity 1: List and categorise details of insider threat events**

The high-level problem that served as the motivation for this research is the prevalence of insider threats in organisations which is a result of poor mitigation of information system access risks. According to the researcher's view, poor mitigation of information system access risks is due to lack of holistic (socio-technical) access risk assessment methodologies since the current ones are technology focused. As a precursor to the development of a new risk assessment methodology, researcher needed to identify common type of socio-technical access security risks and their causes.

Therefore, under the problem diagnosis phase of this research, insider threat event data collected from public sources were analysed and categorised in order to identify the common types of information systems access security risks and socio-technical vulnerabilities that cause these risks. Forty cases of insider threat events were analysed, details of which are given in Table 4-1 and Table 4-2 in Chapter 4. All the underlying socio-technical access vulnerabilities were grouped in to four broad categories given in Table 5-1 in Chapter 5. Overall, there are thirteen different socio-technical access vulnerabilities identified in this research.

**Activity 2: Initial theory building**

According to Venable (2006b) formation of initial utility theory precedes the creation of artefacts. The high-level utility theory which guides the development of socio-technical access risk assessment methodology can be stated as:

*A socio-technical risk assessment methodology would help organisations to effectively assess information system access risks that contribute to insider security breaches*

In addition to the utility theory three components (artefacts) of the risk assessment methodology were conceptualised:

- Risk assessment model
- Risk assessment method
- Risk assessment metrics

A description of these artefacts was given earlier under section 3.2.1. Some of the existing theories that were incorporated in conceptualising these artefacts are given in Table 3-1.

### **Activity 3: Develop an initial methodology**

This stage involved designing and instantiating the artefacts conceptualised in the preceding activity. It is important to note that the artefacts created during this activity were the first (initial) versions of the artefacts presented in Chapter 5. The initial risk assessment model did not contain any intrinsic properties (i.e., attributes) of the entities such as agents and resources. Furthermore, the model and metrics did not account for social relationships between agents. Moreover, no new risk assessment metrics were defined during this stage. Instead, network science metrics that were already there in the knowledgebase were selected based on their applicability in access risk assessment. The model and metrics were instantiated using existing network analysis tools.

### **Activity 4: Evaluate initial artefacts**

This stage dealt with the evaluation of the initial versions of the artefacts developed during activity 3. This was a more formative evaluation that was carried out using real data collected from an organisation. Details of the artefact evaluation are discussed under the next topic (Section 3.3).

### **Activity 5: Reform theory**

The formative evaluation carried out under activity 4 identified some limitations in the artefacts designed initially. Some of the most important limitations were:

- It was clear that relationships among people had to be included in the risk assessment model to account for all socio-technical risk types identified during Activity 1.
- Identified the need to include intrinsic risk properties of people and information resources to eliminate some ambiguities in the results produced by the metrics.
- Identified the need to develop new metrics that take in to account both relationships and intrinsic properties of entities.

**Activity 6: Enhance model and metrics**

During this stage major changes were implemented in the risk assessment model and the metrics according to the refinements identified during Activity 5. Four types of relationships among people (Organisational hierarchy, advice seeking, information exchange and friendship) were included in the model while attributes were added to entities in order to represent intrinsic risk characteristics. New metrics were developed incorporating the changes in the risk assessment model. Since the existing network analysis tools do not support these new metrics, software tools were developed to implement them using the Python Programming Language (Rossum 2013).

**Activity 7: Evaluate artefacts**

The enhanced artefacts were re-evaluated during this phase of the research. Details of the artefact evaluation are discussed under the next topic (Section 3.3).

**Activity 8: Finalise and report theoretical contributions**

This stage dealt with reporting the outcomes of the research in terms of the artefacts produced, theoretical contributions and opportunities for future research. These outcomes are discussed in detail in Chapter 7.

**3.4 Research Evaluation**

According to Hevner et al. (2004) evaluation is one of the most important requirements of design science research. Widely used design science research models such as ones proposed by Vaishnavi and Kuechler (2004), Peffers et al. (2008) and Venable (2006b) contain an evaluation phase. Pries-Heje et al. (2008) and Venable et al. (2012) provide some useful guidelines for evaluating artefacts created in design science research by using a two dimensional classification of evaluation strategies. According to one dimension, evaluation can be classified as either ex-ante (before the instantiation of the evaluated artefact) or ex-post (after the instantiation of the artefact). The other dimension classifies the evaluation as either naturalistic (carried out using real data by real users) or artificial (carried out using either unreal data or unreal users). The evaluation framework provided by Venable (2012) enable the researchers to select evaluation strategies and methods based on the nature and constraints of the research.

Among the research activities carried out in this project, listed in Table 3-3, activity 4 and 7 deal with evaluation of the artefacts created. The next two sub-topics discuss the evaluation carried out during each activity.

#### **3.4.1 Activity 4: Evaluate initial artefacts (first evaluation)**

The artefacts were evaluated at this stage by analysing an organisation, using real data collected. This was similar to a case study although the evaluation was carried out by the researcher himself. The objectives of the evaluation were to demonstrate the utility of the artefacts and to make improvements. Therefore, it can be called a formative evaluation. The artefacts instantiated during Activity 6 are the actual products of the research. Hence, evaluation at this stage can be considered ex-ante according to the framework proposed by Venable et al. (2012) since it is performed before the instantiation of the actual artefacts. Despite the use of real data collected from an organisation, this evaluation can be classified as artificial since researcher played the role of the security analyst (user).

#### **3.4.2 Activity 7: Evaluate artefacts (final evaluation)**

Two evaluation methods were used at this stage.

- Evaluation using case studies of three organisations.
- An evaluation workshop with the participation of security professionals.

It is important to evaluate how the artefacts would perform using real data collected from organisations since the problem addressed by them is socio-technical in nature. Numerous researchers (Benbasat et al. 1987; Darke et al.1998; Yin 2002) have suggested that case studies are a suitable approach for testing the behaviour of such technological artefacts in different organisational contexts. Evaluation using the case studies was similar to the one carried out during Activity 4. However, three case studies (three organisations including the one used in activity 4) were used instead of one. Detailed results of these three case studies are given in Chapter 6. This evaluation can be categorised as ex-post (since it was carried out after the instantiation of artefacts) and artificial (since the researcher himself played the role of analyst).

According to Venable (2006a), the utility of the artefacts can be best demonstrated using naturalistic evaluation. Therefore, the researcher conducted an evaluation workshop with

the participation of security professionals. During the one-day workshop researcher presented the artefacts to the participants, who then used anonymised data collected from three organisations to carry out a risk assessment (researcher provided the data). At the end of the workshop all the participants were presented with a questionnaire to evaluate the methodology they used during the day. Since this evaluation involved real users and they used real data (but anonymised due to privacy concerns), it can be called naturalistic. It is also ex-post since the evaluation occurred after the instantiation of artefacts. More details of the evaluation workshop are given in Section 4.3 in Chapter 4 while the evaluation questionnaire used is given in Appendix B. Results of this evaluation are presented in Chapter 7.

### **3.5 Chapter Summary**

The main objectives of Chapter 3 are to discuss the research methodology employed and to demonstrate the application of rigorous methods in obtaining the research outcomes. This chapter started with the specification of the research questions and objectives. Since the research objectives are concerned with producing useful artefacts that solve an important class of problems, it adopts a design science research paradigm. How this research adheres to the additional design science research requirements specified in the seminal paper by Hevner et al. (2004) was also discussed. Chapter 3 also presented three design science research process models and mapped the activities carried out in this research to the process model proposed by Venable (2006b). The next chapter continues the discussion of one aspect of the research methodology - data collection - in more detail.

## 4. Data Collection Methods

As outlined in the research methodology (Chapter 3), the first phase of the research (refer Activity 1 under section 3.3.2) involved collecting and analysing insider threat event data from public sources in order to identify socio-technical causes of access risks. At a later stage (refer Activity 7 under section 3.3.2), three case studies were carried out in order to evaluate the artefacts developed in this research using data collected from organisations. Additionally, data was collected from information security professionals during an evaluation workshop conducted by the researcher. This chapter describes the data gathered and methods employed to collect them during the three stages mentioned above. The progression of topics in the chapter is given in Figure 4-1.

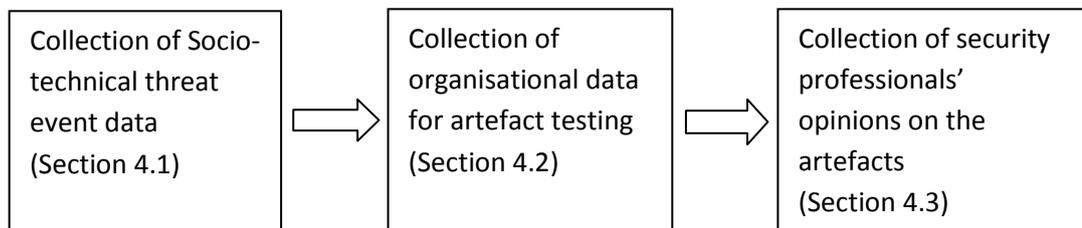


Figure 4-1: Arrangement of chapter sub-topics

### 4.1 Collection of Socio-Technical Threat Event Data

Before developing a risk assessment model and metrics, there is a need to find out what type of information system access risks occur and what socio-technical factors create these risks. Information access risks can be caused either by people who have been granted legitimate access or external agents who are attempting to obtain unauthorised access. Unauthorised access from external agents is outside the scope of this research since they can be mitigated with the help of technology focused risk assessment methodologies currently available for the security professionals. Information security threats occurring due to individuals whom organisations have placed a certain amount of trust, by granting them legitimate access to information systems, are called insider threats (Bishop and Gates 2008; Cappelli et al. 2009). Therefore, collecting past incident information on insider threat events is vital for understanding the types of access risks and socio-technical factors that contribute to these risks. *The CERT Guide to Insider Threats* (Cappelli et al. 2012) provides anonymised details of more than fifty insider threat cases. This is a valuable source of insider threat incident data since such information is very rarely published as a single

collection. Table 4-1 lists excerpts of the incident data obtained from *The CERT Guide to Insider Threats* (Cappelli et al. 2012). (Note: Since forty cases of insider threats are listed, the table spans multiple pages.

Table 4-1 : Insider threat incident descriptions extracted from Cappelli et al. (2012)

Case No.	Page Number in Cappelli et al. (2012)	Excerpts from Cappelli et al. (2012)
1	3	<i>"A network administrator who designed and created the network for a major U.S. city was not just the only person who fully understood the network, but also the only person who had the administrative passwords for the network devices. He also installed a rogue access point in the wiring closet."</i>
2	5	<i>"The company had outsourced its help desk operations to another company. One of the help desk operators needed money to care for his elderly parents, and therefore carried out a scheme to earn some extra money. He created fictitious email addresses, and used those email addresses to send requests for replacement parts, supposedly for government customers. He then had the replacement parts shipped to his home address, and to the home addresses of several relatives."</i>
3	5	<i>"A sales representative was approached by a competitor regarding employment with them. For the next two months, the sales rep emailed proprietary information from his current employer to his home, including customer lists, quotes, customer passwords, marketing and sales plans, material costs and profit margins, and a computer program used to configure quotes for customers. He then visited his potential employer and used a stolen password to access a secure area on his current employer's Web site. He deleted the contents of his hard drive at work, thinking that would destroy the evidence of his crime, and turned in his resignation. After starting his new job a few days later, he continued to access the secure customer area of his previous employer's Web site using the passwords he had stolen."</i>
4	244	<i>"A firm's network manager placed a malicious program—a timed logic bomb—on the network to disrupt and damage his employer as revenge for perceived wrongs. The malicious software deleted and modified more than 50,000 accounts and disrupted the firm's computer network. The investigation uncovered evidence that the insider had taken steps to conceal his activity: The malicious code actually deleted itself after execution, and the insider had deleted the system logs that had recorded his online activity related to planting the malicious code in the first place."</i>

*table continued on next page.....*

*table continued from previous page.....*

Case No.	Page Number in Cappelli et al. (2012)	Excerpts from Cappelli et al. (2012)
5	244	<p><i>“This prompted a system administrator to begin constructing a logic bomb at home, even working on it on Christmas day, and to use authorized remote access to move the logic bomb to the company’s network. He then propagated the malicious code to all of the company’s servers as part of the standard server upgrade procedure. He resigned when he found out the rumours about low bonuses were true; he had already laid the foundation for his revenge. The logic bomb, which he had set to go off two weeks later, deleted billions of files and disrupted service on thousands of servers throughout the United States.”</i></p>
6	245	<p><i>“Over a period of four days after receiving the bad news, the insider contacted management at the victim organization and threatened them. He stated that if he did not receive a significantly larger severance package and good employment recommendations, he would recruit his friends from an underground Internet hacking ring to attack the victim organization. He also claimed to have opened backdoors throughout the victim organization’s systems to facilitate such an attack.”</i></p>
7	245	<p><i>“Following his termination, he recruited members of an online hacking group to help him attack his former employer’s systems. He relayed passwords and other access control information to the underground group, and provided detailed instructions on how to use those credentials to break into his former employer’s network. Over a period of one week, the insider was able to organize the group and execute a coordinated denial-of-service attack against the retailer that lasted from the day before Thanksgiving until the Sunday after Thanksgiving—commonly recognized as the busiest shopping days of the year. Personnel at the organization detected problems in the network that were obstructing online sales and promptly responded to the incident.”</i></p>
8	246	<p><i>“When the victim organization rejected his proposal for follow-on work and decided to award the work to another firm, he became disgruntled and decided to take action to make the new system administrator “look bad.” He sabotaged the organization’s systems by planting logic bombs on five servers set to detonate after he left. Three of the five servers were subsequently damaged and went offline. Another system administrator searched for similar malicious code and uncovered additional logic bombs; the administrator’s actions prevented further damage.”</i></p>

*table continued on next page.....*

*table continued from previous page.....*

Case No.	Page Number in Cappelli et al. (2012)	Excerpts from Cappelli et al. (2012)
9	246	<p><i>“After receiving an anonymous tip that the insider was responsible for the leaks, the organization started an investigation. Working with law enforcement, the organization found evidence that the insider had been downloading its confidential information, which was outside his area of responsibility, for more than two years. The insider had downloaded massive numbers of proprietary documents using a USB removable storage drive and stored the data at his residence. The investigation also found evidence of the insider’s email correspondence with reporters discussing the proprietary documents, articles, and meetings. The entire incident took place over three years.”</i></p>
10	247	<p><i>“Over a ten-year period, the insider created the company’s network supporting the critical manufacturing processes and had sole authority for system administration of that network. During this time the insider centralized the only copy of the source code for all of the company’s critical production programs on a single server, and convinced management to institute policies mandating this practice. A logic bomb executed on the company’s network, deleting 1,000 critical manufacturing programs from the company’s server, the one on which the insider had centralized the company’s production programs earlier. No other current copy of the software was available to recover from the attack, since he had also requested and received, through intimidation, the only backup tape, violating company policy and amplifying the impact of his attack even further.”</i></p>
11	247	<p><i>“In response to an employee dispute, the contractor’s employer suspended his access to its systems, but failed to notify the energy management facility of its suspension, and his facility access was not disabled. A few days later he gained access to the energy production facility and, used a hammer to break the glass case enclosing the “emergency power off” button, and hit the button.”</i></p>
12	248	<p><i>“An information systems consultant at a large manufacturer ran several different password-cracking programs on the company’s network over a ten month period. Initially, he stored cracked passwords in a file on the company’s server. Later he installed a more sophisticated password cracking program. This program enabled him to automatically transfer all accounts and passwords that could be cracked to a remote computer on a regular basis.”</i></p>

*table continued on next page.....*

*table continued from previous page.....*

Case No.	Page Number in Cappelli et al. (2012)	Excerpts from Cappelli et al. (2012)
13	248	<i>"After finding out he was about to be terminated, the insider (system administrator) constructed and planted a logic bomb on the government organisations server to delete critical files."</i>
14	249	<i>"A database administrator and project manager at a government agency became disgruntled and resigned. She connected from her home computer to her previous organisation. Next she accessed a critical system using a DBA account password, which had not being changed since she resigned, and deleted critical data from the system."</i>
15	250	<i>"After the organisation told him his employment will be terminated in approximately one month an e-commerce developer logged in remotely from home, deleted the software he was developing, as well as software being developed by others, modified system logs to conceal his actions, and then changed the root password."</i>
16	250-251	<i>"A disgruntled consultant logged in remotely to a computer system, removed critical code from the system preventing employees and authorized users from accessing software he had created that was used to manage client data and business operations."</i>
17	251	<i>"A disgruntled insider working for an ISP left the organisation, used administrator accounts to take control of the ISP's network. He programmed 110 of ISP's customers' wireless access points to cut off Internet service."</i>
18	252	<i>"A disgruntled system administrator embedded a malicious code within scripts on his organisation's servers. Another system administrator detected the code and avoided an incident which would have wiped out critical data on more than 70 servers."</i>
19	252-253	<i>"An insider who was terminated by the employer gained access to a client's facility (a large manufacturer) posing as an authorised technical support provider. He used password information obtained from his previous employer to access manufacturer's computer kiosks and deleted files and passwords from wireless devices used by the manufacturer across the country."</i>
20	253	<i>"A disgruntled employee of a telecommunications company used the project leader's computer to modify code of a communications and routing software used by the company. He inserted malicious code as a logic bomb recorded in the configuration management system and attributed to the user. Clients were unable to use company's services when the logic bomb finally exploded. The lead developer suspected that the insider was responsible for the incident, and identified the insider as the perpetrator through audit logs."</i>

*table continued on next page.....*

*table continued from previous page.....*

Case No.	Page Number in Cappelli et al. (2012)	Excerpts from Cappelli et al. (2012)
21	253-254	<i>“One month after termination, a former application developer was able to log in using his previous credentials. He defaced the company website, changed the system passwords, and sent emails to customers saying that their accounts had been hacked and their passwords stolen.”</i>
22	254	<i>“An insider working for a telecommunications company deleted the entire database and software from three servers in the organisations network operations centre (NOC) by gaining physical access using a contractor’s badge. The NOC, which was left unattended, was solely protected by physical security; all the machines in the room were left logged in with system administrator access. The organisation’s recovery plan solely relied on backup tapes, which were also stored in the NOC. Insider took all the backup tapes with him when he left the facility.”</i>
23	255	<i>“A disgruntled employee of an organisation was a member of a hacker group. He recruited an outsider from a hacker group to obtain root access to organisations’ systems. They also successfully defaced the organisations’ web site.”</i>
24	256	<i>“When a programmer in a logistics company was terminated they followed the proper procedures by escorting him to his office to collect his belongings and then out of the building. The IT staff also disabled his remote access and changed passwords. However, they overlooked one account held by the insider that was only known by three people in the organisation. The insider used that account to delete the programs he had created while working there. The backups also failed since the insider had been responsible for the backups and he failed to test them properly. The insider had installed several backdoors and was one of only two people who knew the password to the account used in the attack.”</i>
25	257	<i>“Over a two-year period a disgruntled DBA of an organisation downloaded 60,000 employee records from the database to removable media. He solicited bids for the sale of information to criminal groups over the Internet.”</i>
26	257-258	<i>“The sole security administrator for a small telecommunications firm quit his job with no advance notice. He had a history of prior electronic crimes and pirating material online. Upon termination he refused to disclose administrative passwords until he received an additional payment. He locked organisation out of administrative functions. He also used a backdoor created earlier to remotely access organisation’s systems and delete the files he had created during the employment. He also changed the DNS records for the organisation to point to another server named to slander the organisation.”</i>

*table continued on next page.....*

*table continued from previous page.....*

Case No.	Page Number in Cappelli et al. (2012)	Excerpts from Cappelli et al. (2012)
27	258	<i>"A disgruntled insider copied a portion of a software product under development to removable media, deleted it from the company's server and removed the recent backup tapes. He then offered to restore the software in exchange for \$50,000. Unfortunately, most recent version of the software was never recovered."</i>
28	259	<i>"An insider abruptly resigned and joined a competitor of a paint manufacturing company. During his last days of employment he stole copies of 44GB of unauthorised data that included IP belonging to the organisation including formulas for the products he did not work on."</i>
29	260	<i>"An insider was involved with his former employer as a consultant after his resignation. Over the period he worked as a consultant he compiled and coerced others to compile proprietary source code in direct violation of the company security policy. He used the stolen source code to promote products for a new employer."</i>
30	261	<i>"A high-tech company shared some trade secrets with their legal counsel. The legal counsel had hired a document imaging company to copy their documents. An employee of the document imaging company bought his nephew to help him. The nephew, a university student, copied trade secret documents related to anti-piracy technology and released them online to be accessed by the hacker community."</i>
31	262	<i>"A senior engineer, his wife and another accomplice worked for an auto parts manufacturer. They colluded to steal proprietary information from the manufacturer, provide them to another manufacturer and receive commissions on sales made by the second manufacturer."</i>
32	264	<i>"An insider conspired with co-workers to enhance credit reports of consumers for money."</i>
33	265	<i>"A foreign currency trader executed a complex fraud scheme that involved convincing other employees not to track his trades or validate them, exploiting the fact that the organisation did not record trading calls. He also used remote access for his activities. When caught he claimed that trading through a group of employees is more secure than individual trades."</i>
34	265	<i>"A salesman for an information analysis provider was recruited by an outsider employed by a competing firm to relay his company's private communications. The outsider sent the insider an email message containing an attachment infected with a virus. The insider deliberately double-clicked on the infected attachment and as a result installed the malicious program, a keystroke logger, on several machines on his company's network."</i>

*table continued on next page.....*

*table continued from previous page.....*

<b>Case No.</b>	<b>Page Number in Cappelli et al. (2012)</b>	<b>Excerpts from Cappelli et al. (2012)</b>
35	266	<i>"An insider recruited to communicate drivers licence details to law enforcement officers in the field used her permissions to create fake entries for people who didn't possess valid licenses."</i>
36	266-267	<i>"Three employees of an organisation shared passwords to overcome separation of duty requirements. They also used the credentials of a privileged account they had access to create fraudulent payments."</i>
37	267	<i>"An insider supervised employees processing asylum applications for the U.S. government. He fraudulently altered asylum decisions either by himself or ordered his subordinates to do so. He used his subordinates' computers to conceal his activities."</i>
38	267-268	<i>"A supervisor in an organisation handling disability claims created fraudulent payments. The organisation failed to update her access rights when she changed positions, enabling her to modify data and also approve changes. Both positions used the same application but separate roles for entering, approving and authorising payments and she had access to all the roles enabling her to bypass Separation of duty controls."</i>
39	268	<i>"A requisition officer in a warehouse convinced the supervisor to obtain privileged access to the entire purchasing system. He used his excessive privileges to add a fake vendor, create purchase requisitions, and to modify the inventory system."</i>
40	270	<i>"The vice president of technology at a finance market information publisher was dismissed. However, he still had access to the email system after 3 years of the termination which he used to eavesdrop on top executive."</i>

The insider threat events described in Table 4-1 were analysed in order to identify socio-technical access vulnerabilities that contributed to the events. It can be observed that the same type of access vulnerabilities have contributed to many of the insider threat events descriptions in the table. The types of access vulnerabilities identified along with the corresponding insider threat case numbers are listed in Table 4-2. The identified vulnerability types are used to provide a classification of socio-technical access risks based on their causes (refer Figure 5-2 and Table 5-1) and to derive the entity and relationship types of the analysis model (refer Table 5-3 and Figure 5-3) given in Chapter 5.

Table 4-2: Access vulnerabilities that contributed to insider threat events given in Table 4-1

Case No.	Page Number in Cappelli et al. (2012)	Threat Type and description according to Cappelli et al. (2012)	Related Access Vulnerabilities
1	3	Insider IT sabotage (insider blocked administrative access to network devices upon being terminated)	<ul style="list-style-type: none"> <li>• A single employee having exclusive administrative access to information resources.</li> <li>• An employee has exclusive knowledge to perform a critical task</li> <li>• An employee has exclusive knowledge to use a resource.</li> </ul>
2	5	Insider Fraud (Insider used access to systems to commit fraud)	<ul style="list-style-type: none"> <li>• A Contractor performing a task exclusively</li> <li>• A contractor performing two dependent tasks that could lead to a conflict of interest</li> </ul>
3	5	Insider threat of Intellectual Property. (Insider stole confidential customer information and provided them to a competitor)	<ul style="list-style-type: none"> <li>• Employees having access privileges not required for their tasks (sales representative having access to customer passwords and software installers)</li> </ul>
4	244	Insider IT Sabotage. (Insider planted a logic bomb to delete files and disrupt the network)	<ul style="list-style-type: none"> <li>• An employee having exclusive administrative access to information resources.</li> <li>• An employee having exclusive knowledge to perform a critical task</li> <li>• An employee having exclusive knowledge to use a resource.</li> </ul>
5	244	Insider IT Sabotage. (Insider planted a logic bomb to delete files and disrupt the network)	<ul style="list-style-type: none"> <li>• Privileged users performing tasks exclusively.</li> </ul>
6	245	Insider IT Sabotage. (Insider threatened to cause harm using backdoors he created)	<ul style="list-style-type: none"> <li>• Privileged users having exclusive knowledge to perform a task</li> <li>• Privileged users having exclusive knowledge to use a resource</li> </ul>

*table continued on next page.....*

*table continued from previous page.....*

Case No.	Page Number in Cappelli et al. (2012)	Threat Type and description according to Cappelli et al. (2012)	Related Access Vulnerabilities
7	245	Insider IT Sabotage. (Insider used employer account details to organise a DoS attack against the company)	<ul style="list-style-type: none"> <li>• Attack was detected since user did not have exclusive administrative access to information resources</li> <li>• Organisations timely response is due to malicious employee not having exclusive knowledge with respect to a task or resource</li> </ul>
8	246	Insider IT Sabotage. (Authorized contractor planted a logic bombs to disrupt servers)	<ul style="list-style-type: none"> <li>• Further damage was prevented since the attacker did not have exclusive administrative access</li> <li>• Further damage was prevented since the attacker did not have exclusive knowledge with respect to a task or resource</li> </ul>
9	246	Insider IT Sabotage. (Insider leaked confidential information to external entities)	<ul style="list-style-type: none"> <li>• Insiders having access to confidential information which is not required for the job task. (non-enforcement of the need to know principal)</li> </ul>
10	247	Insider IT Sabotage (Disgruntled insider destroyed critical software resources)	<ul style="list-style-type: none"> <li>• Privileged users having exclusive access to a critical information resource.</li> <li>• Users performing tasks exclusively</li> <li>• Users having exclusive knowledge with respect to a task and resource</li> <li>• An employee having indirect access to an information resource (indirect access to backup)</li> <li>• An employee having transitive access to dependent resources (to the original copy of software and backup)</li> </ul>
11	247	Insider IT Sabotage (Insider caused a system failure)	<ul style="list-style-type: none"> <li>• Contractors having access to facility even after termination (access to resources not required for their tasks)</li> </ul>
12	248	Insider IT Sabotage (Insider cracked passwords to gain unauthorized access)	<ul style="list-style-type: none"> <li>• Users having access permissions not required for their tasks</li> </ul>

*table continued on next page....*

*table continued from previous page.....*

Case No.	Page Number in Cappelli et al. (2012)	Threat Type and description according to Cappelli et al. (2012)	Related Access Vulnerabilities
13	248	Insider IT Sabotage (Disgruntled insider installed scripts to delete critical files)	<ul style="list-style-type: none"> <li>• A contractor performing tasks exclusively</li> </ul>
14	249	Insider IT Sabotage (Insider deleted sensitive data after a transfer)	<ul style="list-style-type: none"> <li>• Employee having access to resources not required for the tasks (Failing to disable access for terminated employees)</li> </ul>
15	250	Insider IT Sabotage (Insider deleted software being developed)	<ul style="list-style-type: none"> <li>• Users having access to resource not required for their tasks (access to software being developed by others and system log)</li> </ul>
16	250-251	Insider IT Sabotage (A disgruntled consultant makes software unavailable)	<ul style="list-style-type: none"> <li>• Employee has exclusive privileged access to a resource.</li> <li>• Employee has exclusive knowledge with respect to a resource and a task</li> </ul>
17	251	Insider IT Sabotage (An insider disrupts Internet access of customers of an ISP)	<ul style="list-style-type: none"> <li>• Employee having access to resources not required for his tasks (not disabling access after termination of employment)</li> </ul>
18	252	Insider IT Sabotage (Insider attempted to embed a code to wipe out valuable data but was detected)	<ul style="list-style-type: none"> <li>• This incident was detected since the administrator did not have exclusive access to critical resources and did not perform tasks exclusively.</li> </ul>
19	252-253	Insider IT Sabotage (Insider deleted sensitive information disrupting IT services of a client)	<ul style="list-style-type: none"> <li>• People having access to resources not required for their tasks (Failing to disable the accounts of an employee after termination of employment.)</li> </ul>
20	253	Insider IT Sabotage (Insider inserted malicious code to disrupt services provided by the company)	<ul style="list-style-type: none"> <li>• The inside was caught since he did not possess exclusive knowledge with respect to a task or a resource.</li> </ul>
21	253-254	Insider IT Sabotage (Insider compromises company systems after termination of employment)	<ul style="list-style-type: none"> <li>• People having access to resources not required for their tasks (Failing to disable terminated employee's access credentials.)</li> </ul>

*table continued on next page....*

*table continued from previous page.....*

Case No.	Page Number in Cappelli et al. (2012)	Threat Type and description according to Cappelli et al. (2012)	Related Access Vulnerabilities
22	254	Insider IT Sabotage (Insider deleted data in the servers)	<ul style="list-style-type: none"> <li>• Reliance on only one form of access control (only restricting physical access)</li> <li>• Failing to separate access requirements to the system and the backups</li> </ul>
23	255	Insider IT Sabotage (Insider, with the help of an outsider, gained root access to systems and defaced the company Web site)	<ul style="list-style-type: none"> <li>• Failing to monitor and audit employee access to systems</li> <li>• Failing to carry out regular background checks of employees.</li> </ul>
24	256	Insider IT Sabotage (Insider deleted critical programs)	<ul style="list-style-type: none"> <li>• An employee has access to resources not required for his tasks</li> <li>• An employee has exclusive access to information resources</li> <li>• An employee performs tasks exclusively</li> <li>• A employee being assigned to two dependent tasks (Coding programs and creating backups of programs)</li> </ul>
25	257	Insider IT Sabotage/Fraud (insider downloaded sensitive information to removable drives and sold them to cybercriminals)	<ul style="list-style-type: none"> <li>• An employee has exclusive access to information resources</li> </ul>
26	257-258	Insider IT Sabotage/Fraud (Terminated security administrator commits multiple crimes against his former employer)	<ul style="list-style-type: none"> <li>• An employee performing tasks exclusively</li> <li>• An employee having exclusive access to critical information resources (e.g., administrator passwords)</li> </ul>
27	258	Insider IT Sabotage/Fraud (Insider deleted valuable software and demanded ransom to restore it)	<ul style="list-style-type: none"> <li>• An employee having access to two dependent information resources (software and its backup)</li> <li>• An employee performs two dependent tasks</li> </ul>
28	259	Theft of IP	<ul style="list-style-type: none"> <li>• Employees having access to information resources that are not required for the tasks they perform.</li> </ul>

*table continued on next page....*

*table continued from previous page.....*

Case No.	Page Number in Cappelli et al. (2012)	Threat Type and description according to Cappelli et al. (2012)	Related Access Vulnerabilities
29	260	Theft of IP	<ul style="list-style-type: none"> <li>• An employee having indirect access to information resource through the social networks</li> </ul>
30	261	Theft of IP	<ul style="list-style-type: none"> <li>• Contractors obtaining indirect access to information resources through social networks</li> </ul>
31	262	Theft of IP	<ul style="list-style-type: none"> <li>• A closely associated group of people controlling an information resource</li> </ul>
32	264	Fraud	<ul style="list-style-type: none"> <li>• A closely associated group of people performing a task</li> <li>• A closely associated group of people controlling a resource</li> </ul>
33	265	Fraud	<ul style="list-style-type: none"> <li>• An insider being exclusively assigned a critical task that was not supervised by another employee (Non-enforcement of separation of duty)</li> <li>• An insider having exclusive access to resources</li> </ul>
34	265	Fraud	<ul style="list-style-type: none"> <li>• An employee having access to the resources not required for his job tasks. (salesman having access to several computers with permissions to install software)</li> </ul>
35	266	Fraud	<ul style="list-style-type: none"> <li>• An employee having excessive privileges not required to perform her tasks.</li> </ul>
36	266-267	Fraud	<ul style="list-style-type: none"> <li>• Employees obtaining indirect access to information resources through the social networks.</li> <li>• Employees having excessive privileges not required for the tasks they perform</li> </ul>
37	267	Fraud	<ul style="list-style-type: none"> <li>• An employee having indirect access to resources through the social networks</li> <li>• An employee obtains transitive assignment to dependent tasks</li> <li>• An employee obtains transitive access to dependent information resources</li> </ul>

*table continued on next page....*

*table continued from previous page.....*

Case No.	Page Number in Cappelli et al. (2012)	Threat Type and description according to Cappelli et al. (2012)	Related Access Vulnerabilities
38	267-268	Fraud	<ul style="list-style-type: none"> <li>• An employee performing two dependent tasks</li> <li>• An employee performing a task exclusively</li> <li>• An employee has access to resources not required for her tasks</li> </ul>
39	268	Fraud	<ul style="list-style-type: none"> <li>• Employee performing tasks exclusively</li> <li>• Employee performing two dependent tasks</li> <li>• Employees having excessive privileges not required for his tasks</li> </ul>
40	270	Other	<ul style="list-style-type: none"> <li>• Employee having access to resources not required for her task (failing to disable access after termination)</li> </ul>

## 4.2 Collection of Organisational Data for Artefact Testing

The second data collection phase of the research dealt with collection of real socio-technical data from organisations in order to carry out three case-studies. The three case-studies formed part of the final evaluation of the artefacts as described in Chapter 3.

### 4.2.1 Selection of Organisations

One of the key challenges of undertaking research related to socio-technical aspects of information systems security is the collection of necessary data from organisations. Due to the difficulty in collecting data from Australian organisations as a result of privacy and legal concerns, researcher focused on organisations in Sri Lanka. The main reason for the choice of country was the support provided by *Sri Lanka Computer Emergency Readiness Team (Sri Lanka CERT/CC, website: <http://www.slcert.gov.lk>)* in gaining access to organisations. Sri Lanka CERT as the national CERT of the country is a trusted source of information security incident response and consultancy services and their endorsements played a crucial role in negotiating access to sensitive information.

Accordingly, invitations for organisations to participate in the research were sent through Sri Lanka CERT|CC. Two criteria were used to select organisations:

1. The organisation should belong to the banking and finance sector.
2. The organisation should comprise of 20-100 employees having access to organisational information systems.

The first criterion was used since the banking and finance sector organisations, typically categorised under critical infrastructure of a country (Lewis 2006), have demanding information security requirements. This fact is especially true with regards to information systems access and insider threat issues. The second criterion was used to select organisations that are both large enough to produce useful results and small enough to produce effective visualisations that demonstrate the utility of the methodology. Two organisations that consented to participate in the research had more than hundred employees. In such instances, one or more departments were selected for the study to avoid exceeding the organisational size specified in the second criterion. The selection strategy for these case-studies is similar to the “information oriented selection” prescribed by Flyvbjerg (2006). Carrying out multiple case-studies instead of one provides more scientific rigour for the evaluation as pointed out by Lee (1989).

Three organisations agreed to participate in the research and all data collected has been anonymised in order to safeguard confidentiality. Preservation of data anonymity was a requirement of the Ethics Approval provided for this research by the Curtin University Human Research Ethics Committee. The next sub-topic provides the details of the three organisations. They are referred to as Organisation 1, Organisation 2 and Organisation 3 throughout the thesis.

#### **4.2.2 Overview of Organisations**

##### **Organisation-1**

Organisation 1 is a leading company whose core business is providing life and property insurance solutions to its customers. They also have an affiliated company (under the same group) dealing with leasing and personal loan products. Since the organisation had more than hundred employees, the research only focused on the Finance Department (from this point onwards, all references to Organisation-1 only include the Finance Department). All

other departments and branches were excluded from the data collection. This department had twenty-four (24) employees who were using an Enterprise Resource Planning (ERP) system for core business functions. The ERP system consists of seven components – namely Accounts Receivable (AR), Accounts Payable (AP), Cash Management (CM), Fixed Assets (FA), Purchasing (Pur.), Inventory (Inv.) and General Ledger (GL). The front end software is coupled to the ERP system. In addition to the core business systems, they use their own email server; have access to the Internet and a separate information system for human resource matters. Organisation-1 has an IT Department who oversee the maintenance of all information systems. However, the organisation did not permit the IT Department to be included in this research. Also, the organisation did not identify any employee as having concerning behaviours to be flagged for intrinsic risk characteristics described in Chapter 5.

### **Organisation-2**

Organisation-2 is a company offering export credit and investment insurance services. It is an independent company operating under a larger umbrella organisation. The organisation had undergone significant downsizing just prior to the data collection effort. Twenty-two (22) employees were included in the study while a few others were excluded since they do not access core information systems of the organisation. The Organisation utilised custom (bespoke) software system for the core business functions. The software back-end uses a Microsoft SQL Server Database Management System. The core business system consists of three main modules - Claims, Guarantees and Policies. Additionally, there is a separate Financial Information System and an Administration Information System. The organisation also hosts its own email and web servers. These information systems are maintained by a single administrator with the help from external service providers who mainly perform administration and maintenance tasks related to the core business software. In contrast to Organisation-1, managers in this organisation identified people who have shown concerning behaviour. At the time of the data collection, they had requested the support of Sri Lanka CERT|CC to improve their information security posture in response to a suspected leak of confidential information by an insider.

### **Organisation-3**

Organisation-3 is a company offering personal and industrial leasing solutions to a diverse customer base that include transportation, construction, agriculture and healthcare industries. Since this organisation also had more than hundred employees, the data

collection effort focused on finance, operations, recoveries, insurance and IT departments. Moreover, all branches were excluded from the case study. A total of forty (40) employees have been included in the research. The organisation uses a loan and leasing management system which is integrated with a front office and operations module and a collections module. There is a separate system for the management of factoring solutions. At the time of the data collection, the organisation was performing a parallel run to introduce a new leasing system. The organisation has an IT Manager who has overall responsibility over the maintenance of information systems. However, the IT administrative tasks have been outsourced to contractor who has stationed one of their administrators on a full time basis at the Head Office of Organisation-3. This organisation did not identify any staff member as showing concerning behaviours to be flagged for intrinsic risk characteristics described in Chapter 5.

### **4.2.3 Data collection methods**

This sub-topic describes the types of data collected and the methods employed to collect them from the three organisations. Two data collection strategies were primarily used to collect data:

1. Review of documents (these include reports obtained from access control systems, network diagrams, standard operating procedures etc.)
2. Structured Interviews of staff members and contractors who access information systems of organisations.

First, as much information as possible was extracted from the review of documents provided by the organisations. These documents included network and software architecture diagrams, security policies, asset registers, reports obtained from access control systems and standard operating procedures. However, the required documents were not always available in the organisations.

As a second data collection strategy, structured interviews (also called interviewer-administered questionnaires) (Saunders et al. 2011) of staff members were carried out in order to fill the gaps in information required to instantiate the risk assessment model. Furthermore, structured interviews were essential to collect data on social interactions. The sample questionnaire utilised to collect data from individuals is given in Appendix A. All staff members in the three organisations were interviewed using this questionnaire. It was

administered by the interviewer to increase the response rate and to guide the participants by clarifying any doubts they might have regarding the questions. The questionnaire contained both open-ended and fixed choice questions. All individuals answered the base questionnaire while additional questions were asked from the managers, information owners and information custodians. Table 4-3 summarises the types of data collected from organisations in order to instantiate the model and the methods employed to collect them (Note: Table 4-3 spans multiple pages).

Table 4-3: Summary of types of data collected and methods used

<b>Type of Data</b>	<b>Related entity types in the meta-matrix illustrated in Table 5-3 (Chapter 5)</b>	<b>Whether it is relationship or attribute data</b>	<b>Data collection method</b>
Intrinsic risk properties of agents (types of concerning behaviour shown by agents)	People (agents)	Attributes of agents	Structured interviews (A question was asked from managers and information resource owners on past security incidents and whether any of the employees have been flagged for concerning behaviour.)
Information resource criticality /sensitivity	Resources	Attribute of information resources	Document review (any information classification in policy documents or asset registers) and; Structured interviews (A question was asked from the owners on the classification of information resources under their control.)
Task criticality	Tasks	Attribute of tasks	Document review (any indication of task criticality in standard operating procedures) and; Structured interviews (A question was asked from the managers regarding the criticalities of tasks supervised by them.)

*table continued on next page.....*

*table continued from previous page.....*

<b>Type of Data</b>	<b>Related entity types in the meta-matrix illustrated in Table 5-3 (Chapter 5)</b>	<b>Whether it is relationship or attribute data</b>	<b>Data collection method</b>
Formal reporting relationships	People (agents)	Relationships between people	Document review (extracted from the organisational chart)
Advice relationships	People (agents)	Relationships between people	Structured interviews (The participants were given a roster of all staff members and asked to select the level of advice seeking and advice giving behaviour.)
Information exchange relationships	People (agents)	Relationships between people	Structured interviews (The participants were given a roster of all staff members and asked to select the frequency of information exchange with each other staff member.)
Friendships between staff members	People (agents)	Relationships between people	Structured interviews (The participants were given a roster of all staff members and asked to select the level of friendship with each.)
Information resource access authorisations (who can access what resources?)	People (agents) and Resources	Relationships between people and resources	Document review (reports generated from access control systems detailing permissions) and; Structured interviews (The participants were given a list of information resources and asked to select the level of access they are allowed.)
Task assignments	People (agents) and Tasks	Relationships between people and tasks	Structured interviews (The participants were asked to select the tasks they perform.)
Knowledge possessed by people	People (agents) and Knowledge	Relationships between people and knowledge	Structured interviews (The participants were asked about their skills, knowledge and qualifications.)

*table continued on next page.....*

*table continued from previous page.....*

<b>Type of Data</b>	<b>Related entity types in the meta-matrix illustrated in Table 5-3 (Chapter 5)</b>	<b>Whether it is relationship or attribute data</b>	<b>Data collection method</b>
Dependencies among information resources	Resources	Relationships between resources	Document review (extracted from network and software architecture diagrams) and;  Structured interviews (Information owners and custodians were asked to describe the dependencies among information resources.)
Information resource requirements of tasks	Resources and Tasks	Relationships between resources and tasks	Document review (some resource requirements are detailed in the standard operating procedures)and;  Structured interviews (The managers were asked to list the resource requirements of tasks.)
Knowledge required to use information resources	Resources and Knowledge	Associations between resources and knowledge	Structured interviews (Information resource owners were asked to list the knowledge required to use the resources.)
Task dependencies	Tasks	Relationships between tasks	Document review (extracted from the standard operating procedures) and;  Structured interviews (The managers were asked to map the task dependencies.)
Knowledge requirements of tasks	Tasks and knowledge	Associations between tasks and knowledge	Structured interviews (The managers were asked to list the knowledge required to perform the tasks.)

### 4.3 Collecting Professional Opinions on the Artefacts

In addition to the case studies of the three organisations, the final evaluation of the artefacts were also carried out using a workshop attended by information security professionals as described in section 3.4 of Chapter 3. This one-day workshop was delivered as a part of the *Cyber Security Week 2013* activities organised by the *Sri Lanka CERT/CC*. Twenty-four (24) participants registered for this workshop out of which twenty-two (22) attended. Researcher was able to collect responses from twenty-one (21) of those participants. The workshop was structured as follows:

Session 1: Introduction to insider threats and socio-technical nature of access risks

Session 2: Introduction to network science modelling approaches

Session 3: Socio-technical access risk assessment methodology

Session 4: Exercises using anonymised data, discussion of the results and evaluation

The workshop started with an introduction to socio-technical access risks and insider threats that could result due them. Then the participants were given a brief overview of network modelling and analysis techniques since most of them did not have any prior exposure in that area. The third session introduced the risk assessment methodology – the model, method and metrics proposed in this research. Afterwards, they analysed the anonymised data using the software code supplied by the researcher. At the end of the workshop participants responded to the evaluation questionnaire given in Appendix B. The evaluation questionnaire obtained their viewpoints on various aspects of the risk assessment model, method and the metrics. Detailed results of the evaluation carried out at the end of the workshop are given in Chapter 7.

### 4.4 Chapter Summary

The main objective of Chapter 4 is to describe the data collection techniques employed in the research. First, threat event descriptions published by Cappelli et al. (2012) were analysed to identify common types of socio-technical access vulnerabilities. The second data collection phase involved collecting information from three organisations for the case studies that were used to evaluate the risk assessment methodology. A brief description of the three organisations and the criteria used to select them has been discussed in this chapter followed by a summary of methods used to collect each type of data. The second

data collection phase primarily utilised document review and structured interview techniques. The questionnaire used in the structured interviews is given in Appendix A. The third and final data collection phase involved a questionnaire given to security professionals who participated in an evaluation workshop. The evaluation questionnaire administered at the end of the workshop is given in Appendix B.

The insider threat event data collected during the first phase was used to produce a classification of socio-technical access risk types and to determine the entity and relationship types of the risk assessment model presented in the next chapter (Chapter 5). Chapter 6 presents the results of the three case studies that analysed the data collected from organisations (second data collection phase) using the risk assessment methodology. The results of the evaluation carried out using data collected in the workshop (third data collection phase) are presented in Chapter 7.

## 5. The Risk Assessment Model, Metrics and Method

This chapter describes the model used for the access risk assessment, the metrics defined based on the model and the risk assessment method to be followed. First, the chapter classifies access vulnerabilities identified in Table 4-2 in Chapter 4 into four different categories according to the type of risks they cause. Then a model that can be used to assess underlying socio-technical risks is presented. This risk assessment model encapsulates relevant entity types, relationships between them and attributes of entities. Next, this chapter describes metrics developed based on the model that can be used to assess each type of risk. Finally, a risk assessment method is presented for information security professionals to follow. The progression of topics in the chapter is shown in Figure 5-1.

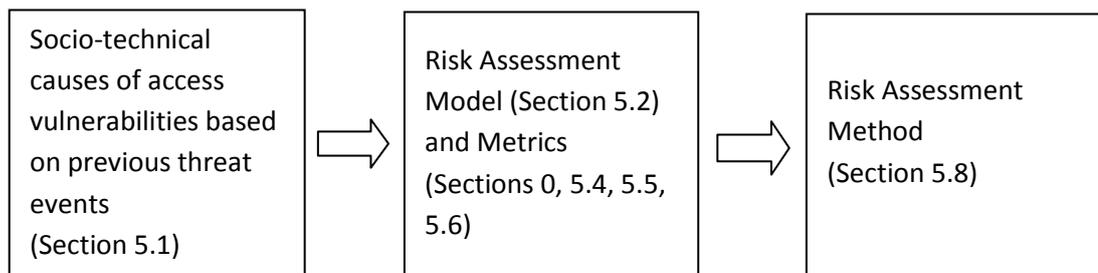


Figure 5-1: Arrangement of chapter sub-topics

### 5.1 Insider Threats and Related Socio-technical Access Risks

Employees obtain legitimate access to information resources depending on the requirements of the organisations and their job functions. In addition to internal employees, sometimes external consultants, contractors and even customers are granted access to various information resources. As defined in Chapter 1, all information security threats faced by an organisation arising due to threat agents with legitimate access can be categorised under insider threats. Analysing real insider threat events is an ideal way to identify socio-technical access vulnerabilities that contribute to such threats. Therefore, details of real insider threat events listed in Table 4-1 were analysed and the results are given in Table 4-2 of the previous chapter. From the cases in Table 4-1 it is clear that most access vulnerabilities are socio-technical in nature although there are few technical ones. Since all access vulnerabilities carry risks that could be exploited in threat events, they can be classified into several risk categories as shown in Figure 5-2 depending on their underlying cause.

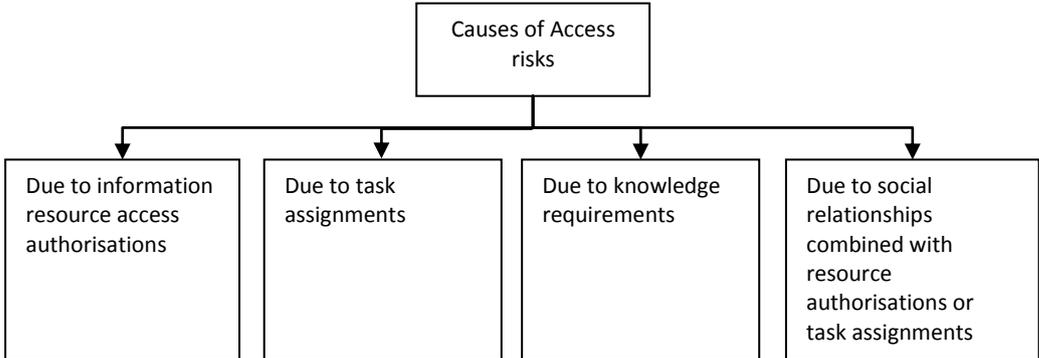


Figure 5-2: Causes of Socio-technical Access Risks

The first two categories of access risks in Figure 5-2 occur due to information resource access authorisations and task assignments of people in organisations. In general, these risks can be attributed to direct violations of access principles such as the need-to-know, separation of duty and dual control. The third category occurs due to specialised knowledge requirements of people needed to utilise resources and to complete tasks assigned to them. The final category occurs due to the combined effect of social relationships and one of the other factors such as resource access authorisations or task assignments. This final category accounts for risks created due to social aspects such as the power of employees owing to their position in the social networks, indirect access due to socio-technical information flows within an organisation and the possibility of collusion. Some of the risks due to social relationships would be intentional (e.g., collusion) while others such as indirect access due to socio-technical information flows could be unintentional. For instance, in the case number 37 listed in Table 4-1 a powerful employee convinces subordinates to violate the security policy of the organisation. The resource access risks of the powerful employee are greater in this case since he can obtain indirect access through his subordinates. Table 5-1 categorises the cases listed in Table 4-1 according to their underlying cause given in Table 4-2. Note that a given insider threat case might belong to more than one category since more than one socio-technical vulnerability can contribute to an insider threat event.

Table 5-1 : Cases listed in Table 4-1 categorised according to their underlying causes in Figure 5-2.

No	Risk	Example Case Number (from Table 4-1)
1	Risks due to information resource access authorisations	1, 3, 4, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 34, 35, 36, 38, 39, 40
2	Risks due to task assignments	2, 5, 10, 16, 18, 24, 26, 27, 33, 36, 38, 39
3	Risks due to knowledge requirements	1, 4, 6, 7, 8, 10, 16, 20
4	Risks due to social relationships combined with resource authorisations or task assignments	10, 29, 30, 31, 32, 36, 37

## 5.2 The Risk Assessment Model

### 5.2.1 Modelling important entity types and relationships between them

Four different types of entities that are important in the assessment of access risks can be identified from the cases listed in Table 4-1 and the socio-technical access risk classification in Figure 5-2 – people, information resources (called resources in the rest of this chapter), tasks performed by people (called tasks in the rest of this chapter) and knowledge possessed by people either required to perform a task or to utilize an information resource (called knowledge in the rest of this chapter). Carley (2002) has introduced a representation known as the “*meta-matrix*” to characterise the entities and their relationships in organisations. The meta-matrix representation of organisations proposed by Carley (2002; 2003) is presented in Table 5-2. A similar meta-matrix representation is used to model the associations between entity types important for the assessment of access risks as illustrated in Table 5-3.

Table 5-2: The meta-matrix representation of organisations introduced by Carley (2002; 2003)

	Agents	Knowledge	Tasks	Organisations
Agents	Interaction Network <i>Who knows who</i> “Structure”	Knowledge Network <i>Who knows what</i> “Culture”	Assignment Network <i>Who is assigned to what</i> “Jobs”	Employment Network <i>Who works where</i> “Demography”
Knowledge		Information Network <i>What informs what</i> “Data”	Requirements Network <i>What is needed to do what</i> “Needs”	Competency Network <i>What knowledge is where</i> “Culture”
Tasks			Precedence Network <i>What needs to be done before what</i> “Operations”	Industrial Network <i>What tasks are done where</i> “Niche”
Organisations				Inter-organizational Network <i>Which organizations work with which</i> “Alliances”

Table 5-3 lists four different types of relationships between people. Who reports to whom and who advises who are important in the assessment of socio-technical access risks since these relationships enable some employees to influence others in a manner that could create security risks. For example, a more powerful or a prestigious employee (owing to advice relationships, social capital of the person or organisational hierarchy) can

persuade another to commit actions that violate the security policy of an organisation. The relationship type who exchanges information with whom is important since this defines information flows within the organisation which can sometimes lead to indirect access to information resources. These information flows can use either technical tools (e.g., email, collaboration systems) or they can be other forms of interaction such as face-to-face communications. The relationship type who is a friend of whom includes friendship and kinship links among the people in an organisation. They are important since friendship and kinship can create risk of collusion and indirect access to information resources.

Table 5-3: Meta-matrix representation of entities and relationships that are important in the assessment of socio-technical access risks

	People	Resources	Tasks	Knowledge
People	1. Who reports to whom (formal hierarchy) 2. Who exchanges information with whom 3. Who advises whom 4. Who is a friend of whom	Who has access to what resources	Who is assigned to which tasks	Who possess what knowledge
Resources		What resource depends on what other resource	What resource is required for which task	What knowledge is required for what resource
Tasks			Which task is related to which other task	What knowledge is required for which task
Knowledge				What knowledge relates to what other knowledge (Not used in this research)

The relationship between people and resources indicated in the meta-matrix in Table 5-3 define the information resource access authorisations of the organisations. The strength of this relationship will reflect the type of access authorised (e.g., administrative access, read only, read/write) for an individual with reference to an information resource. The relationship between people and tasks in the meta-matrix define task assignments of individuals. Resource access and task assignment associations are the primary relationships required for the assessment of access risks. Resource dependencies are modelled as relationships between resources while the resource requirements of tasks are modelled as relationships between resources and tasks as indicated in the meta-matrix. Utilisation or configurations of resources require employees to hold relevant knowledge and such

knowledge requirements of resources are indicated as associations between resources and knowledge. Similarly, knowledge requirements of tasks are modelled as links between tasks and knowledge. Some types of associations between tasks are important in the assessment of socio-technical access risks. Examples include related tasks that can lead to conflicts of interest and dependencies between sensitive tasks. Such tasks are modelled as task to task links as indicated in the meta-matrix. McCulloh et al. (2013) demonstrate how this type of meta-matrix representations can be used to analyse risks in organisations with the help of metrics.

## 5.2.2 Modelling intrinsic risk characteristics of entities

### Intrinsic characteristics of people

If we take two equivalent employees in terms of their resource access authorisations, task assignments, knowledge and other social interactions, they (these two equivalent employees) can still pose different risks in terms of information access due to their different intrinsic characteristics. In a network model, such intrinsic characteristics can be included as node attributes. These node attributes can also be assigned values depending on the strength of the intrinsic property so that they are included in the risk metric calculations defined later in this chapter. The following is a list of such intrinsic characteristics of employees included in the network models as node attributes.

#### a) Official status of an agent (Attribute – $C_1(a_i)$ )

As evident from the insider threat cases in Table 4-1, one such characteristic could be based on the official status of an agent. An organisation can have people with different levels of official association to the organisation accessing information resources. Examples include permanent internal employees, contracted workers and external contractors. Security risk values can be assigned for all people accessing information resources of the organisation based on their official (corporate) status. Agent categories that the organisations can exercise greater control over and are likely to know more about (e.g., permanent employees working full-time) can be assigned lower risk values while the agent categories who are loosely associated with the organisations (e.g., external contractors) can be assigned higher risk values. This risk attribute can be assigned a standardised value (denoted by  $C_1(a_i)$ ) as defined in equation (1.1). However, the analysis carried out in this research uses a dichotomous classification of employees' official status for simplicity.

Therefore, a risk value of 0.5 is assigned to internal employees while a value of 1 is assigned for external contractors.

$$C_1(a_i) = \frac{\text{Risk value assigned for the official status of agent } a_i}{\text{highest risk value in the scale}} \quad (1.1)$$

*Risk value assigned* > 0 and  $0 < C_1(a_i) \leq 1$ .

#### **b) Personal history and behaviour based characteristics**

Furthermore, insider threat models by Cappelli et al. (2012) have identified some personal history or behaviour based characteristics exhibited by employees who are more likely to attempt unauthorised access with a malicious intent. These behavioural characteristics can be easily identified by either supervisors or co-workers although organisations often overlook their significance in information systems security due to the over reliance on technical security controls deployed. The five types of risk characteristics of employees identified by Cappelli et al. (2012, 28-39, 72-73, 108) and attributes that are used to model them in this research are given below. Some analysts would have information with sufficient granularity to quantify these characteristics identified in employees in a scale from a minimum (greater than 0) to a maximum risk value while others would only be able to provide a dichotomous classification. In order to accommodate both these scenarios, standardised risk attributes have been defined for each of the characteristics. The maximum possible value for standardised risk attributes would be one while the minimum should be greater than zero.

##### **I. Personal predispositions (Attribute – $C_2(a_i)$ )**

Cappelli et al. (2012, 28) define personal predispositions as “a characteristic historically linked to a propensity to exhibit malicious behaviour.” Band et al. (2006) describe the criteria for considering an employee under personal predispositions category which include mental health issues such as depression, panic attacks or drug addiction; personality issues such as lack of self esteem or empathy towards others (e.g., bullying, intimidation); poor social and decision making skills such as conflicts with colleagues, being unprofessional or non-adherence to rules; and or history of rule violations such as hacking offences. Organisations typically identify such predispositions through employee background checks or through long-term behavioural observations. The standardised personal predisposition risk attribute value of an agent  $a_i$  (denoted by  $C_2(a_i)$ ) is defined in equation (1.2).

$$C_2(a_i) = \frac{\text{personal predisposition risk value of an agent } a_i}{\text{highest personal predisposition risk in the scale}} \quad (1.2)$$

Note: *Personal predisposition risk assigned* > 0.

Therefore,  $0 < C_2(a_i) \leq 1$

## II. Disgruntlement or unmet expectations (Attribute – $C_3(a_i)$ )

Cappelli et al. (2006, 31) give examples for considering employees under the disgruntlement or unmet expectations category. For an employee to be considered under this category, he must have significant unfulfilled expectations from the organisation. Examples include not receiving anticipated promotions or salary increments, problems with supervisors and co-workers as well as changes in the working environment (e.g., restriction of freedoms). The standardised disgruntlement or unmet expectations risk attribute value of an agent  $a_i$  (denoted by  $C_3(a_i)$ ) is defined in equation (1.3).

$$C_3(a_i) = \frac{\text{disgruntlement risk value of an agent } a_i}{\text{highest disgruntlement risk in the scale}}$$

Note: (1.3)

*Disgruntlement risk assigned* > 0

Therefore,  $0 < C_3(a_i) \leq 1$

## III. Behavioural precursors (Attribute – $C_4(a_i)$ )

According to Cappelli et al. (2012, 35), these are concerning behaviours that can be observed in employees who carry a higher risk of committing insider threats. These behaviours include conflicts with supervisors and co-workers, poor performance, absenteeism etc. The difference between personal predispositions and behavioural precursors is that predispositions are typically historical or chronic behavioural issues while behavioural precursors correspond to a sudden emergence of a concerning behaviour. The standardised behavioural precursor risk attribute value of an agent  $a_i$  (denoted by  $C_4(a_i)$ ) is defined in equation (1.4).

$$C_4(a_i) = \frac{\text{behavioural precursor risk value of an agent } a_i}{\text{highest behavioral precursor risk in the scale}}$$

Note:

(1.4)

*Behavioural precursor risk assigned > 0*

*Therefore,  $0 < C_4(a_i) \leq 1$*

#### IV. Stressful events (Attribute – $C_5(a_i)$ )

According to Cappelli et al. (2012, 37), stressful events include negative workplace events affecting employees such as demotions, disciplinary inquiries and suspensions. Although not explicitly mentioned by Cappelli et al. (2012), personal events such as divorce or severe financial stress can also be included under this category. The standardised stressful event risk attribute value of an agent  $a_i$  (denoted by  $C_5(a_i)$ ) is defined in equation (1.5).

$$C_5(a_i) = \frac{\text{stressful event risk value of an agent } a_i}{\text{highest stressful event risk in the scale}}$$

Note:

(1.5)

*Stressful event risk assigned > 0*

*Therefore,  $0 < C_5(a_i) \leq 1$*

#### V. Technical Precursors (Attribute – $C_6(a_i)$ )

Technical precursors include the detection of malicious technical artefacts in possession of a user (e.g., hacking tools, packet sniffers, password crackers, malware samples, suspicious emails) or any alarms raised through security systems concerning the user access to resources (e.g., Security Information and Event Management (SIEM) systems, firewalls, intrusion prevention systems, network devices etc.) The standardised technical precursor risk attribute value of an agent  $a_i$  (denoted by  $C_6(a_i)$ ) is defined in equation (1.6).

$$C_6(a_i) = \frac{\text{technical precursor risk value of an agent } a_i}{\text{highest technical precursor risk in the scale}}$$

Note:

(1.6)

*Technical precursor risk assigned > 0*

*Therefore,  $0 < C_6(a_i) \leq 1$*

### **Composite risk attribute for agents ( $C_a(a_i)$ )**

It must be noted that agents may be classified for more than one type of intrinsic characteristic described above. Also, it is possible for an analyst to include an observation under more than one category. In order to represent the overall risk due to intrinsic characteristics of agent  $a_i$  in the metric calculations, a composite risk attribute  $C_a(a_i)$  can be defined per agent as presented in equation (1.7).

$$C_a(a_i) = \frac{1}{m} \sum_{j=1}^m w_j C_j(a_i) \quad (1.7)$$

Where;

$w_j$  = corresponding weight assigned to each attribute type  $j$ .  $\left( 0 \leq w_j \leq 1 \text{ and } \sum_{j=1}^m w_j = 1 \right)$ .

$m$  = number of attribute types included in the analysis.

$C_j(a_i)$  = value of the risk attribute type  $j$  of the agent  $a_i$ .

$j = 1, 2, 3, \dots, m$ .

If there is insufficient information, some types of intrinsic characteristics can be ignored all together (corresponding risk attribute weights –  $w_j$  can be set to 0). However, metric calculations described later in this chapter require a non-zero composite risk attribute ( $C_a(a_i)$ ) value and at least one characteristic should be included. Weights in the equation (1.7) enable the analyst to prioritize different agent risk characteristics according to the

organisational context and needs. The theoretical maximum value for the composite risk attribute of an agent ( $C_a(a_i)$ ) is one (1).

### **Standardised sensitivity/criticality of a resource ( $C_r(r_j)$ )**

Information resources of an organisation have various levels of sensitivity or criticality. A critical information resource having an access vulnerability poses a higher risk than a non-critical resource having the same vulnerability. Therefore, standardised criticality of a resource  $r_j$  (denoted by  $C_r(r_j)$ ) is defined as in the equation (1.8) and is included as an attribute of resource nodes.

$$C_r(r_j) = \frac{\textit{sensitivity / criticality of resource } r_j}{\textit{highest sensitivity / criticality of resources in the organisation}}$$

(1.8)

Note: sensitivity/criticality of resource  $r_j > 0$

Therefore,  $0 < C_r(r_j) \leq 1$

### **Standardised sensitivity/criticality of a task ( $C_t(t_p)$ )**

Similarly to the information resources, tasks carried out in an organisation can also be classified according to their criticality. An access vulnerability related to a critical task poses a higher risk than the same vulnerability related to a non-critical task. Therefore, standardised criticality of a task  $t_p$  (denoted by  $C_t(t_p)$ ) is defined as in equation (1.9) and included as an attribute of task nodes.

$$C_t(t_p) = \frac{\textit{sensitivity / criticality of task } t_p}{\textit{highest sensitivity / criticality of tasks in the organisation}}$$

(1.9)

sensitivity/criticality of task  $t_p > 0$

Therefore,  $0 < C_t(t_p) \leq 1$

### 5.2.3 Diagrammatic representation of the Risk Assessment Model

The entity and relationship types of the risk assessment model described in Section 5.2.1 and the intrinsic risk characteristics of the entities (attributes) described in Section 5.2.2 are illustrated in Figure 5-3.

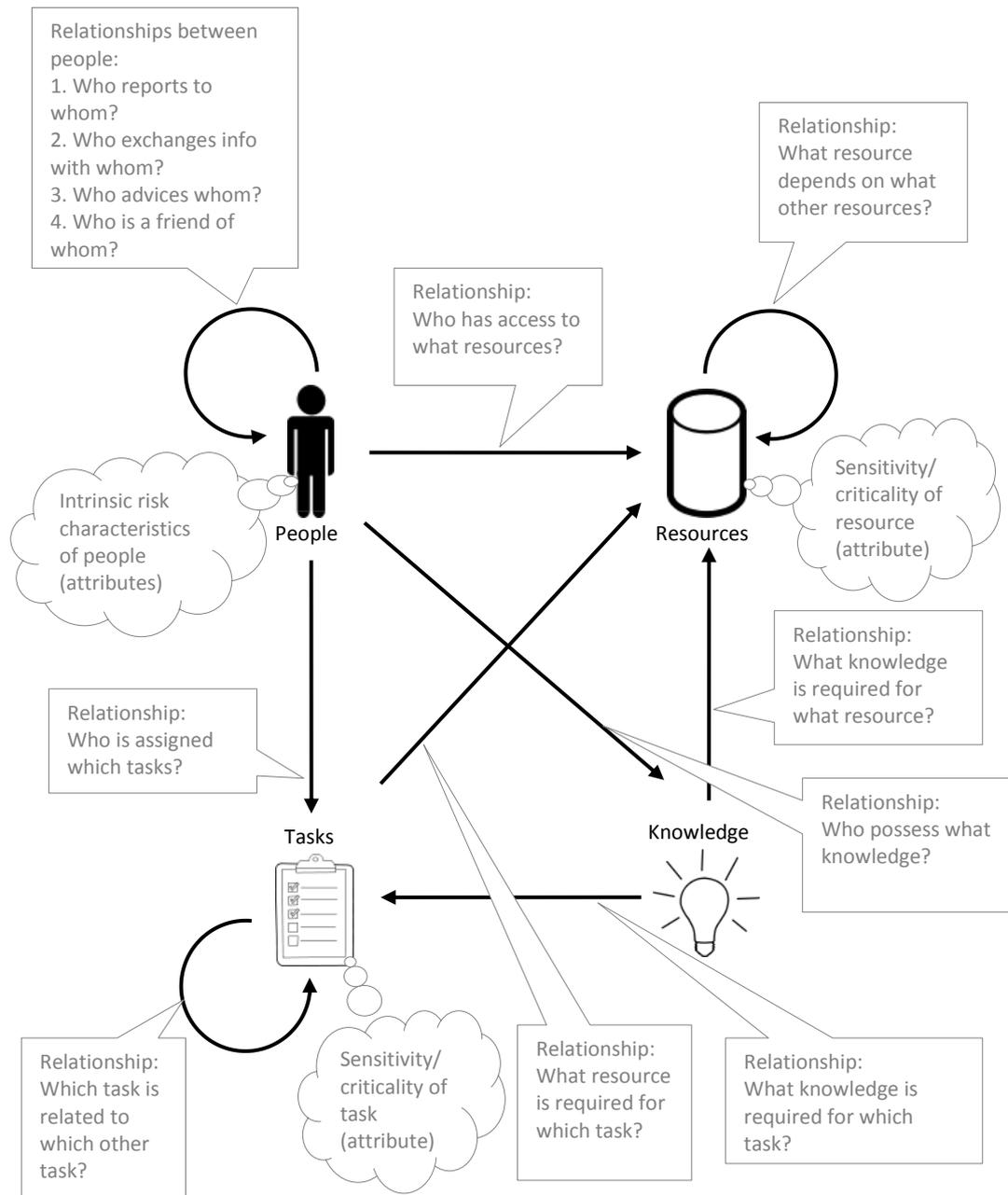


Figure 5-3: Diagram illustrating the entities, relationships and intrinsic risk properties of entities (attributes) of the risk assessment model.

### 5.3 Metrics for the assessment of risks occurring due to information resource access authorisations

Meta-network metrics can be used to assess access risks falling under each category in Figure 5-2. Under the first category – risks occurring due to information resource access authorisations, four types of risks were identified as summarized in Table 5-4.

Table 5-4: Risks occurring due to information resource authorisations

No	Risk	Example Case Number (from Table 4-1 )
1	Employee has exclusive access to resources (violation of the principle of dual control)	1, 4, 7, 8, 10, 16, 18, 24, 26
2	Employee has access to resources not required for his tasks (violation of the principle of least privilege)	3, 9, 11, 12, 15, 28, 34, 35, 36, 38, 39
3	Employee has exclusive administrative access to information resources	1, 4, 7, 8, 10, 16, 18, 26
4	Employee has access to two dependent information resources	2, 24, 27

The first two types of risks occur due to the violation of the principles of dual control (Saltzer and Schroeder 1975; Ward and Smith 2002) and least privilege (Sandhu et al. 2000; Ferraiolo and Kuhn 1992) respectively. The third type is a special case under exclusive access to resources. This third type is necessary because organisations often have more than one person accessing an information resource but still assign a single person exclusive administrative access. The fourth type of risk covers special cases where dual control is violated. Sometimes, due to varying levels of granularity of information available for the analyst, violation of dual control may appear as either risk type one or four.

Metrics for the assessment of risks occurring due to resource authorisations can be given up to three definitions – people or agent centric definitions, resource centric definitions and resource access relationship centric definitions. Agent centric metrics are useful to analyse key agents in terms of access risks and resource centric metrics are useful to identify and analyse resources facing greater risks. Resource access relationship centric metrics are used to identify resource authorisations that create greater risks to the organisation.

#### 5.3.1 Employee having exclusive access to information resources

An employee having exclusive access to information resources is a result of the non-enforcement of the principle of dual control (Ward and Smith 2002; Saltzer and Schroeder 1975). Ashworth and Carley (2006) have developed two metrics called the Task Exclusivity

Index (TEI) and Knowledge Exclusivity Index (KEI) that can be used to analyse agents performing exclusive tasks and having exclusive knowledge. A similar definition is used for the Resource Exclusivity Metric calculation in the network analysis software - ORA (Carley et al. 2012). However, these metrics have not been developed for the analysis of security risks and they do not incorporate attributes such as the sensitivity of the information resources and the risk characteristics of the agents. The Exclusive Resource Access Metrics (ERA) developed in this research are similar to the metrics developed by Ashworth and Carley (2006). However, the metrics presented here are customized for the assessment of access risks and incorporate some significant changes. First, the arbitrary weighting criteria used the metrics developed by Ashworth and Carley (2006) has been replaced by the agent composite risk attribute -  $C_a(a_i)$  and the resource sensitivity/criticality -  $C_r(r_j)$ . Second, metrics presented here allow the analysis to be carried out using either an agent centric, resource centric or agent-resource relationship centric manner where the metrics described in the previous research only produce agent centric results (metrics are calculated per agent). Figure 5-4 presents a simple example used to explain the notation and the calculation of ERA metric values. A short description of the metrics for assessing this risk is presented in Table 5-8 with the aid of a diagram. The table also compares the exiting metrics with the metrics developed in this research for the purpose of access risk assessment.

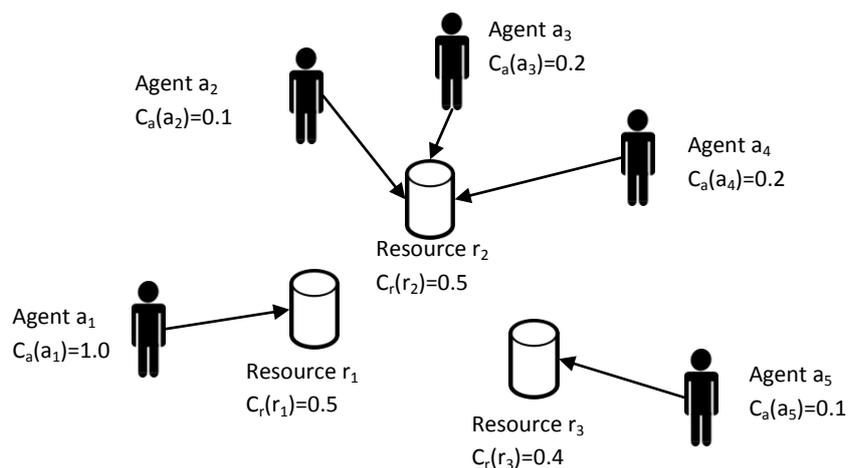


Figure 5-4: A simple example to demonstrate the ERA metric

**Exclusive Resource Access Metric for Resource  $r_j$  (ERA( $r_j$ ))**

The definition of the metric is:

$$ERA(r_j) = C_r(r_j) \cdot e^{1 - \sum_{i=0}^N \frac{1}{C_a(a_i)} \cdot AR(a_i, r_j)} \quad (1.10)$$

Where;

$AR(a_i, r_j)$  = Value at the row  $i$  and column  $j$  of the binarized Agent x Resource matrix.

$a_i \in \{a_0, a_1, a_2, \dots, a_N\}$  (set of agent nodes of the network).

$C_a(a_i)$  = Composite risk attribute for agent  $a_i$  as defined in equation (1.7).

$C_r(r_j)$  = Standardised sensitivity/criticality of information resource  $r_j$  as defined in equation (1.8).

The value of the ERA metric for resource  $r_j$  depends on three factors – the number of agents who have access to the resource, the composite risk attribute values of those agents and the sensitivity or criticality of the resource. Since  $ERA(r_j)$  metric is defined as an exponential function of the number of agents accessing a resource, the metric value exponentially decreases with the increase in number of agents accessing the resource. However, when counting the number of agents, they are weighted according to the inverse of their composite risk attribute values. The maximum value possible for the metric is 1, which occurs when the three conditions listed below are true:

1. There is only one agent accessing the resource.
2. That agent has a maximum composite risk attribute value of 1.
3. The resource is assigned the maximum standardised sensitivity/criticality score of 1.

In order to demonstrate the metric consider the three resources in Figure 5-4. The resource access matrix AR is shown below:

	$r_1$	$r_2$	$r_3$
$a_1$	1	0	0
$a_2$	0	1	0
$a_3$	0	1	0
$a_4$	0	1	0
$a_5$	0	0	1

According to equation (1.10) ERA( $r_1$ ) value can be calculated as:

$$ERA(r_1) = C_r(r_1)e^{1-\left(\frac{1}{C_a(a_1)}AR(a_1,r_1)+\frac{1}{C_a(a_2)}AR(a_2,r_1)+\frac{1}{C_a(a_3)}AR(a_3,r_1)+\frac{1}{C_a(a_4)}AR(a_4,r_1)+\frac{1}{C_a(a_5)}AR(a_5,r_1)\right)}$$

$$ERA(r_1) = 0.5e^{1-\left(\frac{1}{1}(1)+0+0+0+0\right)} = 0.5$$

Similarly ERA( $r_2$ ) and ERA( $r_3$ ) are calculated as shown below:

$$ERA(r_2) = 0.5e^{1-\left(0+\frac{1}{0.1}(1)+\frac{1}{0.2}(1)+\frac{1}{0.2}(1)+0\right)} = 2.80 \times 10^{-9}$$

$$ERA(r_3) = 0.4e^{1-\left(0+0+0+0+\frac{1}{0.1}(1)\right)} = 4.94 \times 10^{-5}$$

Resource  $r_1$  receives the highest ERA metric value since it is accessed by one agent while  $r_2$  receives the lowest value since it is accessed by three agents. Also note that agent  $a_1$  who has exclusive access to  $r_1$  has the maximum possible composite risk value of 1. Although resource  $r_3$  is exclusively accessed by a single agent as in the case of  $r_1$ ,  $r_3$  receives a significantly lower metric value than  $r_1$ . This is due to the lower composite agent risk value of  $a_5$  (agent who has exclusive access to  $r_3$ ) when compared with  $a_1$  (agent who has exclusive access to  $r_1$ ) and the lower resource criticality of  $r_3$ .

### Exclusive Resource Access Metric for Agent $a_i$ (ERA( $a_i$ ))

The definition of the metric is:

$$ERA(a_i) = C_a(a_i) \frac{\sum_{j=0}^M AR(a_i, r_j) \cdot ERA(r_j)}{\sum_{j=0}^M C_r(r_j)} \quad (1.11)$$

Where;

$AR(a_i, r_j)$  = Value at the row  $i$  and column  $j$  of the binarized Agent x Resource matrix.

$ERA(r_j)$  = ERA value of the resource  $r_j$  as defined in equation (1.10).

$a_i \in \{a_0, a_1, a_2, \dots, a_N\}$  (set of agent nodes of the network).

$r_j \in \{r_0, r_1, r_2, \dots, r_M\}$  (set of resource nodes).

$C_a(a_i)$  = Composite risk attribute for agent  $a_i$  as defined in equation (1.7).

$C_r(r_j)$  = Standardised sensitivity/criticality of information resource  $r_j$  as defined in equation (1.8).

$ERA(a_i)$  is a weighted proportion of information resources of an organisation that an agent  $a_i$  has exclusive access. The metric is weighted according to two criteria –  $ERA(r_j)$  values of the resources accessed by the agent and the composite risk attribute of the agent ( $C_a(a_i)$ ).  $ERA(r_j)$  in turn factors in the number of people accessing each resource, their composite risk attributes and the sensitivity/criticality of the resource. The theoretical maximum value for the metric is 1 which is obtained when two conditions listed below are true:

1. The agent has a maximum composite risk attribute value of 1.
2. The agent has exclusive access to all resources of the organisation.

The metric can be demonstrated using the example in Figure 5-4. ERA value for agent  $a_1$  can be calculated as:

$$ERA(a_1) = C_a(a_1) \frac{(AR(a_1, r_1)ERA(r_1) + AR(a_1, r_2)ERA(r_2) + AR(a_1, r_3)ERA(r_3))}{C_r(r_1) + C_r(r_2) + C_r(r_3)}$$

$$ERA(a_1) = 1 \cdot \frac{(1 \times 0.5 + 0 + 0)}{0.5 + 0.5 + 0.4} = 0.357$$

Similarly ERA values for agents  $a_2$  and  $a_5$  can be calculated:

$$ERA(a_2) = 0.1 \times \frac{(0 + 1 \times 2.80 \times 10^{-9} + 0)}{0.5 + 0.5 + 0.4} = 2 \times 10^{-10}$$

$$ERA(a_5) = 0.1 \times \frac{(0 + 0 + 1 \times 4.94 \times 10^{-5})}{0.5 + 0.5 + 0.4} = 3.53 \times 10^{-6}$$

Comparatively, agent  $a_2$  receives the lowest metric score since  $a_2$  does not have exclusive access to the resource  $r_2$  ( $ERA(r_2)$  is the lowest out of the metric scores of three resources). Although agents  $a_1$  and  $a_5$  have exclusive access to a resource, this risk for the resource  $r_1$  ( $ERA(r_1)$ ) accessed by  $a_1$  is much greater than the same for resource  $r_3$  ( $ERA(r_3)$ ) accessed by  $a_5$ . Also,  $a_1$  has a higher composite agent risk ( $C_a(a_1) = 1$ ) than  $a_5$  ( $C_a(a_5) = 0.1$ ). As a result,  $a_1$  receives a much higher metric score than  $a_5$ .

### Exclusive Resource Access Metric for Agent-Resource Pairs ( $ERA(a_i, r_j)$ )

The definition of the metric is:

$$ERA(a_i, r_j) = AR(a_i, r_j) \cdot C_a(a_i) \cdot ERA(r_j) \quad (1.12)$$

Where;

$AR(a_i, r_j)$  = Value at the row  $i$  and column  $j$  of the binarized Agent x Resource matrix.

$ERA(r_j)$  = ERA value of the resource  $r_j$  as defined in equation (1.10).

$C_a(a_i)$  = Composite risk attribute for agent  $a_i$  as defined in equation (1.7).

$ERA(a_i, r_j)$  metric for a agent, resource pair is the product of the composite risk attribute of the agent  $a_i$  (denoted by  $C_a(a_i)$ ) and the  $ERA(r_j)$  value of the resource  $r_j$ . The  $AR(a_i, r_j)$  term ensures that the metric value will be zero for all node pairs which do not have a resource access relationship between them. The maximum possible value for the metric is 1 which occurs when two conditions are fulfilled:

1. The agent concerned has a maximum composite risk attribute value of 1.
2. The resource accessed by the agent has an  $ERA(r_j)$  value of 1.

This metric can be demonstrated using the example in Figure 5-4. ERA value for resource access authorisation for agent  $a_1$  to access resource  $r_1$  can be calculated as:

$$ERA(a_1, r_1) = AR(a_1, r_1) \cdot C_a(a_1) \cdot ERA(r_1)$$

$$ERA(a_1, r_1) = 1 \times 1 \times 0.5 = 0.5$$

Similarly  $ERA(a_2, r_2)$  and  $ERA(a_3, r_3)$  values can be calculated as:

$$ERA(a_2, r_2) = 1 \times 0.1 \times 2.80 \times 10^{-9} = 2.80 \times 10^{-10}$$

$$ERA(a_3, r_3) = 1 \times 0.1 \times 4.94 \times 10^{-5} = 4.94 \times 10^{-6}$$

It is clear that resource access authorisation  $(a_1, r_1)$  receives a high score due to the high agent composite risk ( $C_a(a_1) = 1$ ) and high  $ERA(r_1)$  value. The other two agent, resource pairs receive lower values due to lower agent risk and lower  $ERA(r_j)$  values of the resources involved.

### 5.3.2 Employee having exclusive administrative access to information resources

An employee having exclusive administrative access to information resources is a special case under the exclusive resource access. Often organisations have more than one person accessing a given information resource, but sometimes only one of them will have administrative access. It is clear from the cases in Table 4-1 that majority of the security breaches occurred due to users with administrative or privileged access to information resources. *The Common Sense Guide to Prevention and Detection of Insider Threats* (Cappelli et al. 2009), published by CERT|CC, USA, recommend implementing dual-control and separation of duty for all administrative access requirements. If the three ERA metrics, defined earlier in section 5.3.1, are used only considering the privileged (administrative) access authorisations agents have for resources, exclusive administrative access risks of an organisation can be quantified. Therefore, a metric termed the administrative access to information resources (EAA) is given three definitions which are agent centric -  $EAA(a_i)$ , resource centric -  $EAA(r_i)$  and resource access relationship centric -  $EAA(a_i, r_i)$ . These three are identical to their corresponding metrics in section 5.3.1, except for the fact these only consider resource access relationships corresponding to privileged access. A short description of the EAA metrics for assessing this risk is presented in Table 5-8 with the aid of a diagram. The table also compares the existing metrics with the metrics developed in this research for the purpose of access risk assessment.

**Exclusive Administrative Access Metric for Resource  $r_j$  (EAA( $r_j$ ))**

The definition of the metric is:

Let any given element of the  $AR_x$  matrix defined as:

$$\forall i \forall j: AR_x(a_i, r_j) = [AR(a_i, r_j) = x]$$

Therefore, each element of the  $AR_x$  matrix equals one (1) if the corresponding element in  $AR$  matrix is equal to  $x$  and otherwise it is zero (0) where  $x$  = link weight of administrative links. Then, EAA( $r_j$ ) is defined as:

$$EAA(r_j) = C_r(r_j) \cdot e^{1 - \sum_{i=0}^N \frac{1}{C_a(a_i)} \cdot AR_x(a_i, r_j)} \quad (1.13)$$

Where;

$AR(a_i, r_j)$  = Value at the row  $i$  and column  $j$  of the Agent x Resource matrix.

$a_i \in \{a_0, a_1, a_2, \dots, a_N\}$  (set of agent nodes of the network).

$C_a(a_i)$  = Composite risk attribute for agent  $a_i$  as defined in equation (1.7).

$C_r(r_j)$  = Standardised sensitivity/criticality of information resource  $r_j$  as defined in equation (1.8).

The EAA( $r_j$ ) metric definition is based on the ERA( $r_j$ ) metric equation (1.10). The only difference is that EAA( $r_j$ ) ignores all other resource access links except for administrative access links. The value of the metric exponentially decreases with the increase in number of agents having administrative access to the resource. However, when counting the number of agents, they are weighted according to the inverse of their composite risk attribute values. The theoretical maximum and minimum values of the metric are same as for the ERA( $r_j$ ) metric.

**Exclusive Administrative Access Metric for Agent  $a_i$  (EAA( $a_i$ ))**

EAA( $a_i$ ) is a weighted proportion of information resources to which an agent has exclusive administrative access. The metric is weighted according to two criteria – EAA( $r_j$ ) values of the resources accessed by the agent and the composite risk attribute of the agent

( $C_a(a_i)$ ). The theoretical maximum and minimum values for this metric is same as for ERA( $a_i$ ) metric defined in equation (1.11).

The definition of the metric based on the ERA( $a_i$ ) metric defined in equation (1.11) is:

Let any given element of the  $AR_x$  matrix defined as:

$$AR_x(a_i, r_j) = [AR(a_i, r_j) = x]$$

Therefore, each element of the  $AR_x$  matrix equals one (1) if the corresponding element in  $AR$  matrix is equal to  $x$  and otherwise it is zero (0) where  $x$  = link weight of administrative links. Then:

$$EAA(a_i) = C_a(a_i) \cdot \frac{\sum_{j=0}^M AR_x(a_i, r_j) \cdot EAA(r_j)}{\sum_{j=0}^M C_r(r_j)} \quad (1.14)$$

Where;

$AR(a_i, r_j)$  = Value at the row  $i$  and column  $j$  of the Agent x Resource matrix.

$AR_x(a_i, r_j)$  = Value at the row  $i$  and column  $j$  of the derived  $AR_x$  matrix.

$EAA(r_j)$  = EAA value of the resource  $r_j$ .

$a_i \in \{a_0, a_1, a_2, \dots, a_N\}$  (set of agent nodes of the network).

$r_i \in \{r_0, r_1, r_2, \dots, r_M\}$  (set of resource nodes).

$C_a(a_i)$  = Composite risk attribute for agent  $a_i$  as defined in equation (1.7).

$C_r(r_j)$  = Standardised sensitivity/criticality of information resource  $r_j$  as defined in equation (1.8).

### **Exclusive Administrative Access Metric for Agent-Resource Pairs (EAA( $a_i, r_j$ ))**

The definition of the metric based on the ERA( $a_i, b_j$ ) metric defined in equation (1.12) is:

Let any given element of the  $AR_x$  matrix defined as:

$$AR_x(a_i, r_j) = [AR(a_i, r_j) = x]$$

Therefore, each element of the  $AR_x$  matrix equals one (1) if the corresponding element in  $AR$  matrix is equal to  $x$  and otherwise it is zero (0) where  $x$  = link weight of administrative links. Then;

$$EAA(a_i, r_j) = AR_x(a_i, r_j) \cdot C_a(a_i) \cdot EAA(r_j) \quad (1.15)$$

Where;

$AR(a_i, r_j)$  = Value at the row  $i$  and column  $j$  of the Agent x Resource matrix.

$AR_x(a_i, r_j)$  = Value at the row  $i$  and column  $j$  of the derived  $AR_x$  matrix.

$EAA(r_j)$  = EAA value of the resource  $r_j$ .

$C_a(a_i)$  = Composite risk attribute for agent  $a_i$  as defined in equation (1.7).

$EAA(a_i, r_j)$  metric for an agent resource pair is the product of the composite risk attribute of the agent ( $C_a(a_i)$ ) and the  $EAA(r_j)$  value of the resource. The  $AR_x(a_i, r_j)$  term ensures that the metric value will be zero for all node pairs that do not have an administrative access relationship between them. The maximum possible value for the metric is one which occurs when two conditions are fulfilled:

1. The agent concerned has a composite risk attribute value of 1.
2. The agent has administrative access to a resource with an  $EAA(r_j)$  value of 1.

### 5.3.3 Employee having access to resources not required for their tasks

Employees having access to resources not essential for their tasks occur due to the non-enforcement of the principle of least privilege (Sandhu et al. 1996; Ferraiolo and Kuhn 1992). Lee and Carley (2004) and Carley et al. (2012) have defined a metric known as the Agent Resource Waste Congruence (ARWC) that can be used to identify agents having access to resources that are not required for the tasks they perform. However, ARWC metric has not been defined in an information security perspective and it does not incorporate factors such as sensitivity/criticality of resources or risk characteristics of agents. Therefore, a new metric called the Violation of Need to Access Metric (VNA) have been defined based on the ARWC metric. The VNA metric calculation considers both sensitivity/criticality of the resources and the composite risk attribute of the agents. The

metric can be given two definitions, which are agent centric -  $VNA(a_i)$  and agent-resource authorisation centric -  $VNA(a_i, r_j)$ . Figure 5-5 is a simple illustration used to explain the notation and calculation of the VNA metric. A short description of the metrics for assessing this risk is presented in Table 5-8 with the aid of a diagram. The table also compares the exiting metrics with the metrics developed in this research for the purpose of access risk assessment.

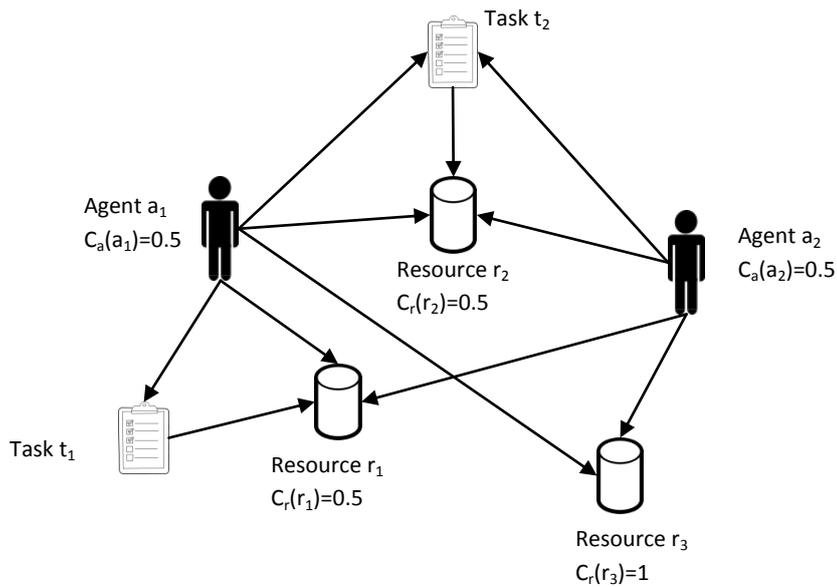


Figure 5-5: A simple example to demonstrate the VNA metric

**Violation of Need to Access Metric for Agents ( $VNA(a_i)$ )**

The definition of the metric is:

Let  $AR_T$  matrix be

$AR_T = AT \times TR$  then;

$$VNA(a_i) = C_a(a_i) \frac{\sum_{j=0}^M C_r(r_j) \cdot AR(a_i, r_j) [AR_T(a_i, r_j) = 0]}{\sum_{j=0}^M C_r(r_j) \cdot AR(a_i, r_j)} \tag{1.16}$$

Where,

$AT$  = Agent x Task matrix (binarized).

$TR$  = Task x Resource matrix (binarized).

$AR(a_i, r_j)$  = Value at the row  $i$  and column  $j$  of the binarized Agent x Resource matrix.

$AR_T(a_i, r_j)$  = Value at the row  $i$  and column  $j$  of the derived  $AR_T$  matrix.

$C_a(a_i)$  = Composite risk attribute for agent  $a_i$  as defined in equation (1.7).

$C_r(r_j)$  = Standardised sensitivity/criticality of information resource  $r_j$  as defined in equation (1.8).

$r_j \in \{r_0, r_1, r_2, \dots, r_M\}$  (set of resource nodes).

The metric calculates the weighted proportion of resources that are not required for the agents tasks out of the resources accessed by the agent. The two weighting criteria are the composite risk attribute of the agent -  $C_a(a_i)$  and the standardised sensitivity/criticality of the resources accessed. The maximum possible value of the metric is 1, which occurs when two conditions are fulfilled:

1. All the resources accessed by the agent are non-essential for the tasks performed by him.
2. The agent has the maximum composite risk attribute value of 1.

Any non-zero value obtained for the metric indicates an agent having access to at least one resource not required for the tasks performed by him. This metric can be demonstrated using the example given in Figure 5-5. First, in order to calculate the VNA value of agent  $a_1$ , note that this agent has access to three resources ( $r_1, r_2, r_3$ ) out of which  $r_3$  is not required for any tasks performed by the agent. Therefore, the metric calculation for  $a_1$  would be:

$$VNA(a_1) = C_a(a_1) \frac{(0 + 0 + C_r(r_3))}{(C_r(r_1) + C_r(r_2) + C_r(r_3))}$$

Note that first two terms within the brackets in the numerator are zero since the first two resources are required for the tasks performed by  $a_1$ . Therefore the condition within the square bracket of the equation is false for the first two terms.

$$VNA(a_1) = 0.5 \frac{(0 + 0 + 1)}{(0.5 + 0.5 + 1)} = 0.25$$

Similarly,  $VNA(a_2)$  can be calculated as:

$$VNA(a_2) = 0.5 \frac{(0 + 0.5 + 1)}{(0.5 + 0.5 + 1)} = 0.375$$

Agent  $a_2$  receives a higher metric score than agent  $a_1$  since  $a_2$  has access to two resources not required for his tasks while  $a_1$  has access to only one resource not required for his tasks.

### Violation of Need to Access Metric for Agent-Resource Pair ( $VNA(a_i, r_j)$ )

The definition of the metric is:

*Let  $AR_T$  matrix be :*

$$AR_T = AT \times TR$$

*then;*

$$VNA(a_i, r_j) = C_a(a_i) \cdot C_r(r_j) \cdot AR(a_i, r_j) [AR_T(a_i, r_j) = 0] \quad (1.17)$$

Where,

$AT$  = Agent x Task matrix (binarized).

$TR$  = Task x Resource matrix (binarized).

$AR(a_i, r_j)$  = Value at the row  $i$  and column  $j$  of the binarized Agent x Resource matrix.

$AR_T(a_i, r_j)$  = Value at the row  $i$  and column  $j$  of the derived  $AR_T$  matrix.

$C_a(a_i)$  = Composite risk attribute for agent  $a_i$  as defined in equation (1.7).

$C_r(r_j)$  = Standardised sensitivity/criticality of information resource  $r_j$  as defined in equation (1.8).

This metric simply weighs the resource access links of agent  $a_i$  that are not required for the tasks performed by the agent according to the composite risk attribute value of the agent and the sensitivity/criticality of the information resource  $r_j$ . The maximum possible value for the metric is 1 which occurs when three conditions are satisfied:

1. Resource  $r$  is not required for any of the tasks performed by the agent  $a$ .

2. Agent has the maximum risk attribute ( $C_a(a_i) = 1$ ).
3. The resource  $r$  has maximum criticality/sensitivity ( $C_r(r_j) = 1$ ).

VNA metric can be demonstrated using the example in Figure 5-5. The metric calculation for the resource access authorisation for agent  $a_1$  to access resource  $r_1$  would be:

$$VNA(a_1, r_1) = C_a(a_1) \cdot C_r(r_1) \cdot AR(a_1, r_1) [AR_T(a_1, r_1) = 0]$$

Since  $r_1$  is required for the task  $t_1$  performed by  $a_1$ , the condition within the square bracket becomes false.

$$VNA(a_1, r_1) = 0.5 \times 0.5 \times 0 = 0$$

Therefore, if a resource is required for at least one task performed by an agent the VNA metric for the corresponding agent, resource pair will be zero. Similarly, the metric calculation for the resource access authorisation for agent  $a_2$  to access resource  $r_2$  would be:

$$VNA(a_2, r_2) = 0.5 \times 0.5 \times 1 = 0.25$$

In this case, condition within square bracket is true since  $r_2$  is not required for any of the tasks performed by  $a_2$ . The metric calculation for the resource access authorisation for agent  $a_2$  to access resource  $r_3$  would be:

$$VNA(a_2, r_3) = 0.5 \times 1 \times 1 = 0.5$$

$VNA(a_2, r_3)$  value is greater than  $VNA(a_2, r_2)$  value since resource  $r_3$  has a higher sensitivity/criticality than  $r_2$ .

### 5.3.4 Employee has access to two dependent information resources

An employee having access to two dependent information resources can lead to access risks. For example, in cases 24 and 27 listed in Table 4-1, a malicious employee had access to original information and its backup, which enabled him to compromise both resources. The metric for calculating risks due to agents having access to dependent information resources, termed Access to Dependent Resources Metric (ADR), is given two definitions which are agent centric -  $ADR(a_i)$  and agent-resource access centric -  $ADR(a_i, r_j)$ . Figure 5-6 is

an illustration of a simple example used to clarify the notation used and the calculation of the ADR metrics. A short description of the ADR metrics for assessing this risk is also presented in Table 5-8.

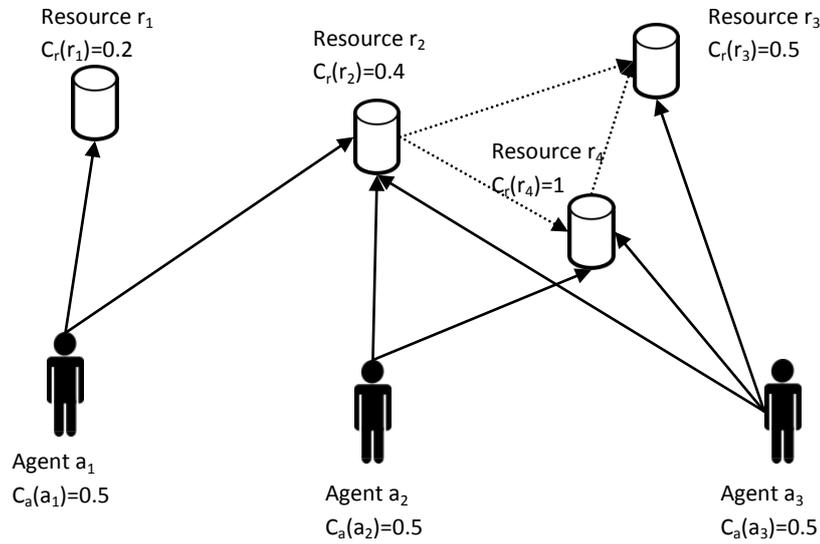


Figure 5-6: A simple example to demonstrate the ADR metric

**Access to Dependent Resources Metric for Agent  $a_i$  ( $ADR(a_i)$ )**

The metric is defined as follows:

Let Agent x Resource (resource access) matrix weighted according to resource sensitivities ( $C_r(r_j)$ ), denoted by  $AR_w$ , be defined as:

$$\forall i \forall j : AR_w(a_i, r_j) = C_r(r_j) \cdot AR(a_i, r_j) \tag{1.18}$$

Therefore, each element in  $AR_w$  matrix is equal to the corresponding element in  $AR$  matrix multiplied by the sensitivity/criticality of the relevant resource. Then let,

$$AR_R = AR_w \times RR \tag{1.19}$$

Then the Access to Dependent Resource Metric for agents ( $ADR(a_i)$ ) can be defined as:

$$ADR(a_i) = C_a(a_i) \cdot \frac{\sum_{j=0}^M C_r(r_j) \cdot AR_R(a_i, r_j) [AR(a_i, r_j) > 0]}{\sum_{j=0}^M \sum_{k=0}^M C_r(r_j) \cdot C_r(r_k) \cdot RR(r_j, r_k)} \quad (1.20)$$

Where,

$AR(a_i, r_j)$  = Value at the row  $i$  and column  $j$  of the binarized Agent x Resource matrix.

$AR_R(a_i, r_j)$  = Value at the row  $i$  and column  $j$  of the derived  $AR_R$  matrix.

$AR_w$  = Agent x Resource matrix weighted according to resource sensitivities/criticalities.

RR = Resource x Resource matrix (binarized).

$C_a(a_i)$  = Composite risk attribute for agent  $a_i$  as defined in equation (1.7).

$C_r(r_j)$  and  $C_r(r_k)$  = Standardised sensitivity/criticality of information resource  $r_j$  and  $r_k$  as defined in equation (1.8).

$r_j, r_k \in \{r_0, r_1, r_2, \dots, r_M\}$  (set of resource nodes of the network).

$a_i \in \{a_0, a_1, a_2, \dots, a_N\}$  (set of agent nodes of the network).

In this metric formula, the numerator calculates the number of dependent resources that the agent can access, weighted according to the sensitivity of the two resources involved. The denominator calculates the weighted value for all resource dependencies in the organisation. The maximum value of the metric is 1, which occurs when two conditions are satisfied:

1. Agent has access to all dependent resources of the organisation.
2. Agent has a composite risk attribute value of 1.

The  $ADR(a_i)$  matrix calculation can be demonstrated using the example in Figure 5-6. The resource access matrix (AR) and the resource access matrix weighted according to resource criticality ( $AR_w$ ) are:

*AR matrix*

	$r_1$	$r_2$	$r_3$	$r_4$
$a_1$	1	1	0	0
$a_2$	0	1	0	1
$a_3$	0	1	1	1

$$\forall i \forall j : AR_w(a_i, r_j) = C_r(r_j).AR(a_i, r_j)$$

	$r_1$	$r_2$	$r_3$	$r_4$
$a_1$	0.2	0.4	0	0
$a_2$	0	0.4	0	1
$a_3$	0	0.4	0.5	1

Then the resource dependency matrix (RR) and the  $AR_R$  matrix are:

*RR matrix*

	$r_1$	$r_2$	$r_3$	$r_4$
$r_1$	0	0	0	0
$r_2$	0	0	1	1
$r_3$	0	0	0	0
$r_4$	0	0	1	0

$$AR_R = AR_w \times RR$$

	$r_1$	$r_2$	$r_3$	$r_4$
$a_1$	0	0	0.4	0.4
$a_2$	0	0	1.4	0.4
$a_3$	0	0	1.4	0.4

Also, the RR matrix weighted according to resource sensitivity

$\forall j \forall k : C_r(r_j).C_r(r_k).RR(r_j, r_k)$  can be expressed as:

	$r_1$	$r_2$	$r_3$	$r_4$
$r_1$	0	0	0	0
$r_2$	0	0	0.4	0.2
$r_3$	0	0	0	0
$r_4$	0	0	0.5	0

Then the ADR metric for agent  $a_1$  would be:

$$ADR(a_1) = C_a(a_1) \times \frac{(C_r(r_1).AR_R(a_1, r_1)[AR(a_1, r_1) > 0] + \dots + C_r(r_4).AR_R(a_1, r_4)[AR(a_1, r_4) > 0])}{C_r(r_2).C_r(r_3).RR(r_2, r_3) + C_r(r_2).C_r(r_4).RR(r_2, r_4) + C_r(r_4).C_r(r_3).RR(r_4, r_3)}$$

$$ADR(a_1) = 0.5 \times \frac{(0+0+0+0)}{1.1} = 0$$

Although agent  $a_1$  has access to two resources  $r_1$  and  $r_2$ , there are no dependencies between them. Therefore, the numerator of the equation is zero. The denominator

represents the total number of resource dependencies in the organisation, weighted according to the sensitivity/criticality of the two resources.

Similarly ADR metric for agents  $a_1$  and  $a_2$  can be calculated as:

$$ADR(a_2) = 0.5 \times \frac{(0 + 0 + 0 + 1 \times 0.4)}{1.1} = 0.182$$

$$ADR(a_3) = 0.5 \times \frac{(0 + 0 + 0.5 \times 1.4 + 1 \times 0.4)}{1.1} = 0.5$$

Agent  $a_1$  receives a metric score of zero (0) since he does not have access to dependent information resources. Inspection of Figure 5-6 confirms that agent  $a_2$  can access resource  $r_2$  that depends on the resource  $r_4$ , which is also accessible by the same agent. Therefore, the fourth term in the numerator becomes non-zero and  $a_2$  receives a metric score of 0.182. Agent  $a_3$  has access to all instances of dependent resources in the example – resource  $r_4$ , which depends on  $r_3$  and resource  $r_2$ , which depends on both  $r_3$  and  $r_4$ . Therefore,  $a_3$  receives the highest metric score reflecting a greater risk of access to dependent information resources. Also the results are weighted according to criticalities of the resources involved and the composite agent risk.

#### **Access to Dependent Resources Metric for Agent, Resource Pairs ( $ADR(a_i, r_j)$ )**

Let Agent x Resource (resource access) matrix weighted according to resource sensitivities -  $C_r(r_j)$ , denoted by  $AR_w$ , be defined as in equation (1.18):

$$\forall i \forall j : AR_w(a_i, r_j) = C_r(r_j) \cdot AR(a_i, r_j)$$

Therefore, each element in  $AR_w$  matrix is equal to the corresponding element in  $AR$  matrix multiplied by the sensitivity/criticality of the relevant resource. Then, according to equation (1.19):

$$AR_R = AR_w \times RR$$

Then, the Access to Dependent Resource Metric for agent resource pairs ( $ADR(a_i, r_j)$ ) can be defined as:

$$ADR(a_i, r_j) = C_a(a_i) \cdot C_r(r_j) \cdot \frac{AR_R(a_i, r_j) [AR(a_i, r_j) > 0]}{\sum_{k=0}^M C_r(r_k) \cdot AR(a_i, r_k) [k \neq r]} \quad (1.21)$$

Where,

$AR(a_i, r_j)$  = Value at the row  $i$  and column  $j$  of the binarized Agent x Resource matrix.

$AR_R(a_i, r_j)$  = Value at the row  $i$  and column  $j$  of the derived  $AR_R$  matrix.

$AR_w$  = Agent x Resource matrix weighted according to resource sensitivities/criticalities.

RR = Resource x Resource matrix (binarized).

$C_a(a_i)$  = Composite risk attribute for agent  $a_i$  as defined in equation (1.7).

$C_r(r_j)$  and  $C_r(r_k)$  = Standardised sensitivity/criticality of information resource  $r_j$  and  $r_k$  as defined in equation (1.8).

$r_j, r_k \in \{r_0, r_1, r_2, \dots, r_M\}$  (set of resource nodes of the network).

The numerator of the metric calculates the weighted number of other resources that depend on the resource  $r_j$  provided that agent  $a_i$  can also access  $r_j$  directly. The denominator calculates the weighted number of resources accessed by the agent  $a_i$  excluding  $r_j$ . The value is also weighted according to the sensitivity of the resource  $r_j$  ( $C_r(r_j)$ ) and the composite risk attribute value of the agent  $a_i$  ( $C_a(a_i)$ ). The theoretical maximum of the metric is 1, which occurs under three conditions:

1. All other resources accessed by the agent  $a_i$  depend on the resource  $r_j$ .
2. Agent has the maximum composite risk attribute value of 1.
3. Resource  $r_j$  has the maximum standardised sensitivity/criticality of 1.

The  $ADR(a_i, r_j)$  metric can also be demonstrated using the example in Figure 5-6. The resource access matrix (AR) and the resource access matrix, weighted according to resource criticality ( $AR_w$ ) are:

*AR matrix*

	$r_1$	$r_2$	$r_3$	$r_4$
$a_1$	1	1	0	0
$a_2$	0	1	0	1
$a_3$	0	1	1	1

$$\forall i \forall j : AR_w(a_i, r_j) = C_r(r_j) \cdot AR(a_i, r_j)$$

	$r_1$	$r_2$	$r_3$	$r_4$
$a_1$	0.2	0.4	0	0
$a_2$	0	0.4	0	1
$a_3$	0	0.4	0.5	1

Then the resource dependency matrix (RR) and the  $AR_R$  matrix are:

*RR matrix*

	$r_1$	$r_2$	$r_3$	$r_4$
$r_1$	0	0	0	0
$r_2$	0	0	1	1
$r_3$	0	0	0	0
$r_4$	0	0	1	0

$$AR_R = AR_w \times RR$$

	$r_1$	$r_2$	$r_3$	$r_4$
$a_1$	0	0	0.4	0.4
$a_2$	0	0	1.4	0.4
$a_3$	0	0	1.4	0.4

The metric for resource authorisation that agent  $a_1$  has for  $r_1$ , denoted by  $ADR(a_1, r_1)$  is:

$$ADR(a_1, r_1) = C_a(a_1) \cdot C_r(r_1) \cdot \frac{AR_R(a_1, r_1) [AR(a_1, r_1) > 0]}{C_r(r_2)AR(a_1, r_2) + C_r(r_3)AR(a_1, r_3) + C_r(r_4)AR(a_1, r_4)}$$

$$ADR(a_1, r_1) = 0.5 \times 0.2 \times \frac{0}{0.4 + 0 + 0} = 0$$

Similarly,  $ADR(a_3, r_3)$  and  $ADR(a_3, r_4)$  can be calculated as:

$$ADR(a_3, r_3) = 0.5 \times 0.5 \times \frac{1.4}{0.4 + 0 + 1} = 0.25$$

$$ADR(a_3, r_4) = 0.5 \times 1 \times \frac{0.4}{0.4 + 0.5 + 0} = 0.222$$

$ADR(a_1, r_1)$  is zero since no other resource accessed by  $a_1$  depends on  $r_1$ .  $ADR(a_3, r_3)$  takes a higher value than  $ADR(a_3, r_4)$  since two other resources accessed by agent  $a_3$  depends on  $r_3$  while only one other resource accessed by the same agent depends on  $r_4$ .

### 5.4 Metrics for the assessment of risks occurring due to task assignments

Under the second category in Figure 5-2 – risks occurring due to task assignments, two types of risks have been identified as summarized in Table 5-5.

Table 5-5: Risks occurring due to task assignments

No	risk	Example Case Number (from Table 4-1)
1	Employee performs a task exclusively	2, 5, 10, 16, 18, 24, 26, 33, 38, 39
2	Employee performs two dependent tasks	2, 24, 27, 38, 39

Sometimes, an employee performing a task exclusively can lead to fraud, sabotage or information leakage, particularly in the absence of any supervision of the task. In such instances, Separation of Duty Principle (Clark and Wilson 1987; Ferraiolo and Kuhn 1992) must be enforced by creating a related supervisory or approval task and assigning the core and the supervisory tasks to two different individuals. The second type of risk in Table 5-5 corresponds to instances where two dependent tasks are performed by the same employee, leading to a conflict of interest. Again, the two tasks should be assigned to two separate employees by enforcing separation of duty requirements.

#### 5.4.1 Employee exclusively assigned to tasks

An employee performing a task exclusively can lead to fraud, sabotage or information leakage, particularly in the absence of any supervision of the task as mentioned in the previous paragraph. Ashworth and Carley (2006) has developed a metric termed Task Exclusivity Index (TEI) that can be used to analyse agents performing exclusive tasks. However, TEI has not been developed for the assessment of security risks and it does not consider intrinsic factors such as the agent risk characteristics or the sensitivity/criticality of the task. Therefore, a new metric, termed the Exclusive Task Assignment Metric (ETA), was developed from the original concepts to assess exclusive task assignment risks. Similarly to the ERA metric described under section 5.3.1, the ETA metric presented here allows deeper analysis to be carried out using either an agent centric -  $ETA(a_i)$ , task centric -  $ETA(t_p)$  or agent-task relationship centric -  $ETA(a_i, t_p)$  focus. Figure 5-7 is a simple example used to illustrate the notation and calculation of ETA metrics. A short description of the three ETA metrics for assessing this risk is also presented in Table 5-8 with the aid of a diagram. The

table compares the exiting metrics with the ETA metrics developed in this research for the purpose of access risk assessment.

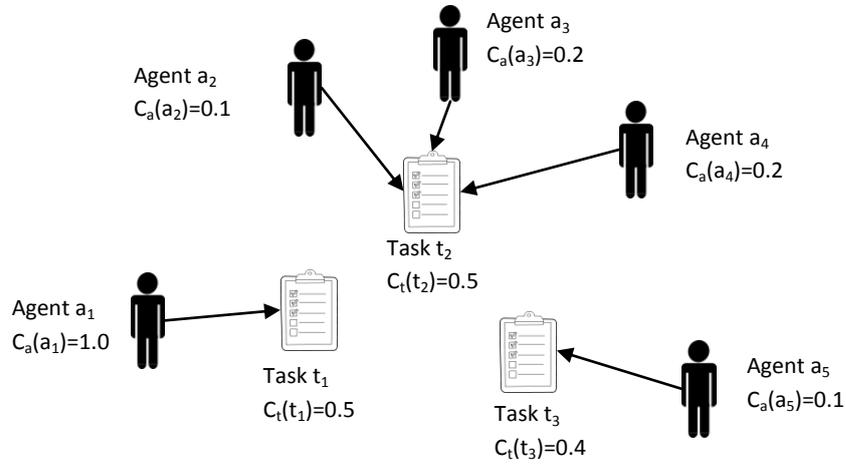


Figure 5-7: A simple example used to illustrate ETA metrics

**Exclusive Task Assignment Metric for task t<sub>p</sub> (ETA(t<sub>p</sub>))**

The definition of the metric is:

$$ETA(t_p) = C_t(t_p) \cdot e^{1 - \sum_{i=0}^N \frac{1}{C_a(a_i)} \cdot AT(a_i, t_p)} \tag{1.22}$$

Where;

AT(a<sub>i</sub>, t<sub>p</sub>) = Element in the i<sup>th</sup> row and p<sup>th</sup> column of the Agent x Task Matrix (binarized).

a ∈ {a<sub>0</sub>, a<sub>1</sub>, a<sub>2</sub>, ..., a<sub>N</sub>} (set of agent nodes of the network).

C<sub>a</sub>(a<sub>i</sub>) = Composite risk attribute for agent a<sub>i</sub> as defined in equation (1.7).

C<sub>t</sub>(t<sub>p</sub>) = Standardised sensitivity/criticality of task t<sub>p</sub> as defined in equation (1.9).

The value of the ETA(t<sub>p</sub>) metric depends on three factors – the number of agents assigned for the task, the composite risk attribute values of those agents, and the sensitivity or criticality of the task. The ETA(t<sub>p</sub>) metric exponentially decreases with the increase in number of agents assigned for the task. However, when counting the number of agents,

each one is weighted according to the inverse of their composite risk attribute values. The maximum value possible for the metric is 1, which occurs when three conditions are true:

1. There is only one agent assigned for the task.
2. The agent has a maximum composite risk attribute value of 1.
3. The task is assigned the maximum standardised sensitivity/criticality score of 1.

The  $ETA(t_p)$  metric is calculated in the same way as the  $ERA(r_j)$  metric defined in equation (1.10) in section 5.3.1. The only difference is that instead of resources  $ETA(t_p)$  metric focuses on tasks.

### Exclusive Task Assignment Metric for Agent $a_i$ ( $ETA(a_i)$ )

The definition of the metric is:

$$ETA(a_i) = C_a(a_i) \cdot \frac{\sum_{p=0}^U AT(a_i, t_p) \cdot ETA(t_p)}{\sum_{p=0}^U C_t(t_p)} \quad (1.23)$$

Where;

$AT(a_i, t_p)$  = Element in the  $i$ th row and  $p$ th column of the Agent x Task Matrix (binarized).

$a \in \{a_0, a_1, a_2, \dots, a_N\}$  (set of agent nodes of the network).

$t \in \{t_0, t_1, t_2, \dots, t_U\}$  (set of task nodes).

$C_a(a_i)$  = Composite risk attribute for agent  $a_i$  as defined in equation (1.7).

$C_t(t_p)$  = Standardised sensitivity/criticality of task  $t_p$  as defined in equation (1.9).

$ETA(a_i)$  is a weighted proportion of tasks that an agent performs. The metric is weighted according to two criteria –  $ETA(t_p)$  values of the tasks performed by the agent, and the composite risk attribute of the agent ( $C_a(a_i)$ ).  $ETA(t_p)$  in turn factors in the number of people performing each task and their risk attributes as well as the sensitivity/criticality of the task. The theoretical maximum value for the metric is 1, which is obtained when three conditions are fulfilled:

1. The agent has a maximum composite risk attribute value of 1.
2. The agent is assigned all the tasks of the organisation.
3. All tasks in the organisation have an  $ETA(t_p)$  value of 1.

The  $ETA(a_i)$  metric is calculated in the same way as the  $ERA(a_i)$  metric defined in equation (1.11) in section 5.3.1. The only difference is that instead of resources  $ETA(a_i)$  metric focuses on tasks.

### **Exclusive Task Assignment Metric for Agent-Task Pairs ( $ETA(a_i, t_p)$ )**

The definition of the metric is:

$$ETA(a_i, t_p) = AT(a_i, t_p) \cdot C_a(a_i) \cdot ETA(t_p) \quad (1.24)$$

Where;

$AT(a_i, t_p)$  = Element in the  $i$ th row and  $p$ th column of the Agent x Task Matrix (binarized).

$C_a(a_i)$  = Composite risk attribute for agent  $a_i$  as defined in equation (1.7).

$ETA(t_p)$  = Exclusive task assignment risk value of task  $t_p$ .

$ETA(a_i, t_p)$  metric for an agent task pair is the product of the composite risk attribute of the agent ( $C_a(a_i)$ ) and the  $ETA(t_p)$  value of the task. The  $AT(a_i, t_p)$  term ensures that the metric value will be zero for all node pairs that do not have an agent-task relationship between them. The maximum possible value for the metric is one, which occurs when the following conditions are satisfied:

1. Agent has a composite risk attribute value of 1.
2. The task concerned has an  $ETA(t_p)$  value of 1.

The  $ETA(a_i, t_p)$  metric is calculated the same way as the  $ERA(a_i, r_j)$  metric defined in equation (1.12) in section 5.3.1. The only difference is that instead of resources  $ETA(a_i, t_p)$  metric focuses on tasks.

### 5.4.2 Employee performs two dependent tasks

An employee performing dependent tasks is a special case of the non-enforcement of separation of duty principle. The metric for calculating risks due to agents performing dependent tasks, termed Assignment of Dependent Tasks Metric (ADT), is given two definitions that are agent centric -  $ADT(a_i)$  and agent-task assignment centric -  $ADT(a_i, t_p)$ . Figure 5-8 illustrates a simple example used to demonstrate the ADT metrics developed in this research. A short description of the ADT metrics is also presented in Table 5-8 with the aid of a diagram.

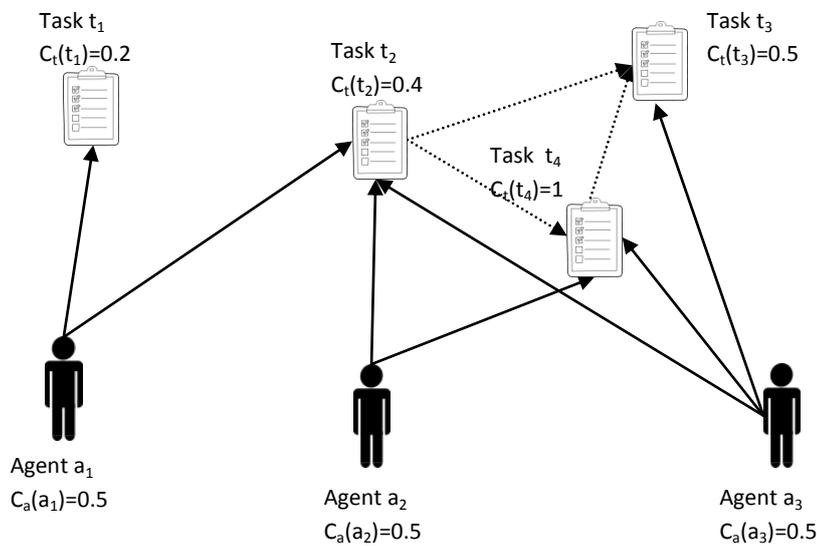


Figure 5-8: A simple example used to illustrate the ADT metrics

#### Assignment of Dependent Tasks Metric for Agent $a_i$ ( $ADT(a_i)$ )

The metric is defined as follows:

Let Agent x Task matrix weighted according to task sensitivities/criticalities -  $C_t(t_p)$ , denoted by  $AT_w$ , be defined as:

$$\forall i \forall p : AT_w(a_i, t_p) = C_t(t_p) \cdot AT(a_i, t_p) \tag{1.25}$$

Then let,

$$AT_T = AT_w \times TT \quad (1.26)$$

Then the Assignment of Dependent Tasks Metric for agents -  $ADT(a_i, t_p)$  can be defined as:

$$ADT(a_i) = C_a(a_i) \cdot \frac{\sum_{p=0}^U C_t(t_p) \cdot AT_T(a_i, t_p) [AT(a_i, t_p) > 0]}{\sum_{p=0}^U \sum_{k=0}^U C_t(t_p) \cdot C_t(t_k) \cdot TT(t_p, t_k)} \quad (1.27)$$

Where,

$AT(a_i, t_p)$  = Value at the row  $i$  and column  $p$  of the binarized Agent x task matrix.

$AT_T(a_i, t_p)$  = Value at the row  $i$  and column  $p$  of the derived  $AT_T$  matrix.

$AT_w$  = Agent x Task matrix weighted according to task sensitivities/criticalities.

$TT$  = Task x Task matrix (binarized).

$C_a(a_i)$  = Composite risk attribute for agent  $a_i$  as defined in equation (1.7).

$C_t(t_p), C_t(t_k)$  = Standardised sensitivity/criticality of task  $t_p$  and  $t_k$  as defined in equation (1.9).

$t_p, t_k \in \{t_0, t_1, t_2, \dots, t_N\}$  (set of task nodes of the network).

$a_i \in \{a_0, a_1, a_2, \dots, a_N\}$  (set of agent nodes of the network).

In this metric formula, the numerator calculates the number of dependent tasks that the agent performs, weighted according to the sensitivity of the two tasks involved. The denominator calculates the weighted value for all task dependencies in the organisation. The maximum value of the metric is 1, which occurs when the following conditions are fulfilled:

1. The agent is assigned all dependent tasks of the organisation.
2. The agent has a composite risk attribute value of 1.

The ADT( $a_i$ ) metric is calculated the same way as the ADR( $a_i$ ) metric defined in equation (1.20) in section 5.3.4. The only difference is that ADT( $a_i$ ) metric focus on the task assignments instead of resource authorisations.

### Assignment of Dependent Tasks Metric for Agent, Task Pairs (ADT( $a_i, t_p$ ))

Agent x Task matrix weighted according to task sensitivities/criticalities -  $C_t(t_p)$ , denoted by  $AT_w$ , is defined in equation (1.25):

$$\forall i \forall p : AT_w(a_i, t_p) = C_t(t_p) \cdot AT(a_i, t_p)$$

Also, equation (1.26) defines  $AT_T$  as:

$$AT_T = AT_w \times TT$$

Then, the Assignment of Dependent Tasks Metric for agent task pairs - ADT( $a_i$ ) can be defined as:

$$ADT(a_i, t_p) = C_a(a_i) \cdot C_t(t_p) \cdot \frac{AT_T(a_i, t_p) [AT(a_i, t_p) > 0]}{\sum_{k=0}^U C_t(t_k) \cdot AT(a_i, t_k) [k \neq p]} \quad (1.28)$$

Where,

$AT(a_i, t_p)$  = Value at the row  $i$  and column  $p$  of the binarized Agent x task matrix.

$AT_T(a_i, t_p)$  = Value at the row  $i$  and column  $p$  of the derived  $AT_T$  matrix.

$AT_w$  = Agent x Task matrix weighted according to task sensitivities/criticalities.

$TT$  = Task x Task matrix (binarized).

$C_a(a_i)$  = Composite risk attribute for agent  $a_i$  as defined in equation (1.7).

$C_t(t_p), C_t(t_k)$  = Standardised sensitivity/criticality of task  $t_p$  and  $t_k$  as defined in equation (1.9).

$t_p, t_k \in \{t_0, t_1, t_2, \dots, t_N\}$  (set of task nodes of the network).

$a_i \in \{a_0, a_1, a_2, \dots, a_N\}$  (set of agent nodes of the network).

The numerator of the metric calculates the weighted number of other tasks that depend on  $t_p$ , which agent  $a_i$  performs. The denominator calculates the weighted number of tasks performed by the agent  $a_i$  excluding  $t_p$ . The value is also weighted according to the sensitivity/criticality of the task  $t_p$  ( $C_t(t_p)$ ) and the composite risk attribute value of the agent  $a_i$  ( $C_a(a_i)$ ). The theoretical maximum of the metric is 1, which occurs when three conditions are true:

1. All other tasks performed by the agent  $a_i$  depend on task  $t_p$ .
2. Agent has the maximum composite risk attribute value of 1.
3. Task  $t_p$  has the maximum standardised sensitivity/criticality of 1.

The  $ADT(a_i, t_p)$  metric is calculated the same way as the  $ADR(a_i, r_j)$  metric defined in the equation (1.21) in section 5.3.4. The only difference is that  $ADT(a_i, t_p)$  metric focuses on task assignments instead of resource authorisations.

## 5.5 Metrics for the assessment of risks occurring due to knowledge requirements

From the examples in Table 4-1, it is clear that most access violations categorised as insider IT sabotage were carried out by threat agents who had exclusive knowledge about the administration of information resources. Therefore, under the third category in Figure 5-2– risks occurring due to knowledge requirements, two types of risks have been identified as summarized in Table 5-6.

Table 5-6: Risks occurring due to knowledge requirements

No	Risk	Example Case Number (from Table 4-1)
1	Employee has exclusive knowledge to operate an information resource	1, 4, 6, 7, 8, 10, 16, 20
2	Employee has exclusive knowledge to perform a task	1, 4, 6, 7, 8, 10, 16, 20

### 5.5.1 Employee having exclusive knowledge to operate an information resource

There is an increased risk to the availability, integrity and confidentiality of the information resources from the employees having exclusive knowledge to operate them since others in the organisation lack the skills to detect, prevent or recover resources from such breaches of security. The metric for calculating the risk due to agents exclusively

possessing knowledge for a resource is given two definitions: agent centric -  $EKR(a_i)$  and resource access centric -  $EKR(a_i, r_j)$ . A simple example used to explain the notation and the calculation of the ERA metrics is illustrated in Figure 5-9. Furthermore, a short description of the two EKR metrics is presented in Table 5-8.

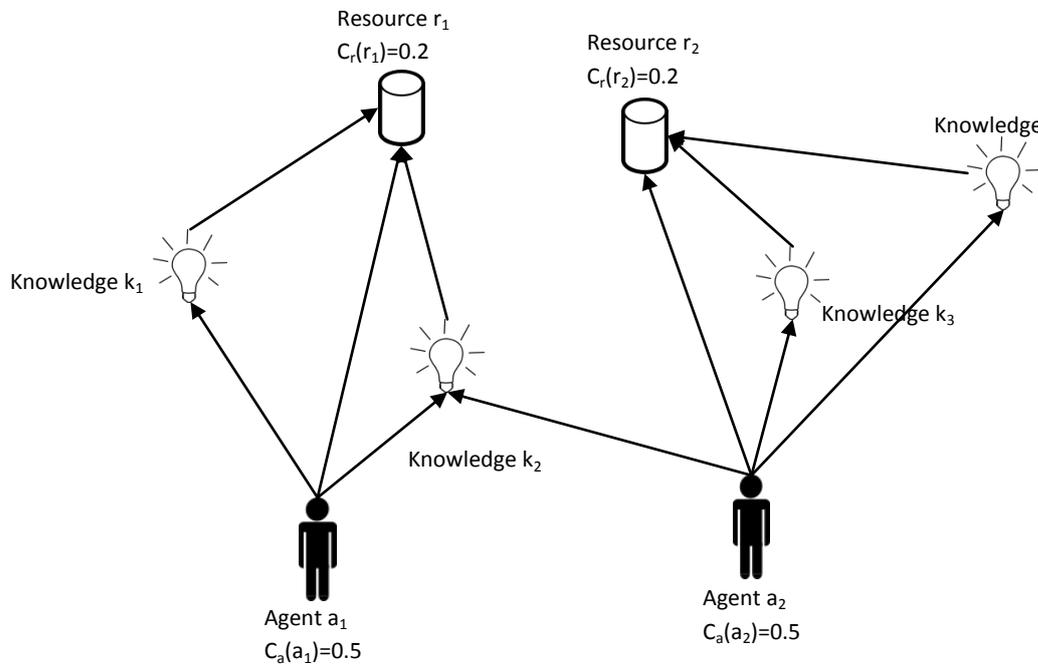


Figure 5-9: Simple example used to demonstrate EKR metrics

**Exclusive Knowledge for Resource Metric for Agent  $a_i$  ( $EKR(a_i)$ )**

The metric is defined as follows:

Let the matrix depicting agents possessing knowledge to use a resource, denoted by  $AR_k$  defined as:

$$AR_K = AK \times KR$$

The total number of  $a_s, k_q$  pairs, where agent  $a_s$  has knowledge  $k_q$  required to use resource  $r_j$  is given by:

$$\sum_{s=0}^N AR_K(a_s, r_j) \tag{1.29}$$

Therefore, the proportion of knowledge possessed by agent  $a_i$  required for resource  $r_j$  out of all  $a_s, k_q$  pairs, where agent  $a_s$  has knowledge  $k_q$  required to use resource  $r_j$ , denoted by  $X(a_i, r_j)$  is given by:

$$X(a_i, r_j) = \frac{AR_K(a_i, r_j)}{\sum_{s=0}^N AR_K(a_s, r_j)} \left[ \sum_{s=0}^N AR_K(a_s, r_j) \neq 0 \right] \quad (1.30)$$

Then,  $EKR(a_i)$  can be defined as:

$$EKR(a_i) = C_a(a_i) \cdot \frac{\sum_{j=0}^M AR(a_i, r_j) \cdot X(a_i, r_j) \cdot C_r(r_j)}{\sum_{j=0}^M C_r(r_j)} \quad (1.31)$$

Where,

AK = Agent x Knowledge matrix.

KR = Knowledge x Resource matrix.

$AR(a_i, r_j)$  = Value at the row  $i$  and column  $j$  of the binarized Agent x Resource matrix.

$AR_K(a_i, r_j)$  = Value at the row  $i$  and column  $j$  of the derived  $AR_K$  matrix.

$a_i, a_s \in \{a_0, a_1, a_2, \dots, a_N\}$  (set of agent nodes of the network).

$r_j \in \{r_0, r_1, r_2, \dots, r_M\}$  (set of resource nodes).

$C_a(a_i)$  = Composite risk attribute for agent  $a_i$  as defined in equation (1.7).

$C_r(r_j)$  = Standardised sensitivity/criticality of information resource  $r_j$  as defined in equation (1.8).

$EKR(a_i)$  is the weighted proportion of resources, where an agent has exclusive knowledge for the resource. The weighting criteria include  $X(a_i, r_j)$ , which measures the extent to which an agent exclusively possesses the knowledge required for a resource. The other weighting criteria are sensitivity/criticality of the resource ( $C_r(r_j)$ ) and the composite risk attribute for

the agent ( $C_a(a_i)$ ). The maximum possible value for the metric is 1, which occurs when two conditions are fulfilled:

1. The agent exclusively holds all the knowledge required to use all information resources of the organisation.
2. The agent has a composite risk attribute value of 1.

The  $EKR(a_i)$  metric calculation can be demonstrated using the simple example illustrated in Figure 5-9. The Agent x Knowledge and Agent x Resource matrices for the example would be:

<i>AK matrix</i>	<i>KR matrix</i>
$  \begin{array}{ccccc}  & k_1 & k_2 & k_3 & k_4 \\  a_1 & 1 & 1 & 0 & 0 \\  a_2 & 0 & 1 & 1 & 1  \end{array}  $	$  \begin{array}{ccc}  & r_1 & r_2 \\  k_1 & 1 & 0 \\  k_2 & 1 & 0 \\  k_3 & 0 & 1 \\  k_4 & 0 & 1  \end{array}  $

The  $AR_k$  matrix, defined as  $AR_k = AK \times KR$  shows the agents possessing knowledge to operate a function:

$$\begin{array}{cc}
 AR_k = AK \times KR & \\
 \begin{array}{cc}
 r_1 & r_2 \\
 a_1 & 2 & 0 \\
 a_2 & 1 & 2
 \end{array}
 \end{array}$$

Therefore,  $X(a_1, r_1)$  according to equation (1.30) would be:

$$X(a_1, r_1) = \frac{AR_k(a_1, r_1)}{(AR_k(a_1, r_1) + AR_k(a_2, r_1))}$$

Note that the denominator is the total number of  $a_i, k_q$  pairs where  $a_i$  has knowledge  $k_q$  required to use resource  $r_1$  which is given by the sum of the column  $r_1$  of the  $AR_k$  matrix. Therefore,  $X(a_1, r_1)$  is the proportion of knowledge possessed by  $a_1$  with respect to resource  $r_1$ .

$$X(a_1, r_1) = \frac{2}{(2+1)} = 0.667$$

Similarly,  $X(a_1, r_2)$  would be:

$$X(a_1, r_2) = \frac{0}{(0+2)} = 0$$

Therefore,  $EKR(a_1)$  according to the equation (1.31) would be:

$$EKR(a_1) = C_a(a_1) \cdot \frac{(AR(a_1, r_1) \cdot X(a_1, r_1) \cdot C_r(r_1) + AR(a_1, r_2) \cdot X(a_1, r_2) \cdot C_r(r_2))}{(C_r(r_1) + C_r(r_2))}$$

$$EKR(a_1) = 0.5 \times \frac{(1 \times 0.667 \times 0.2 + 0 \times 0 \times 0.2)}{(0.2 + 0.2)} = 0.1667$$

Similarly,  $EKR(a_2)$  can be calculated:

$$X(a_2, r_1) = \frac{1}{(2+1)} = 0.333$$

$$X(a_2, r_2) = \frac{2}{(0+2)} = 1$$

Note that agent  $a_2$  exclusively possess all knowledge required to use resource  $r_2$  (refer Figure 5-9). Therefore,  $X(a_2, r_2)$  takes maximum value of 1. Then:

$$EKR(a_2) = C_a(a_2) \cdot \frac{(AR(a_2, r_1) \cdot X(a_2, r_1) \cdot C_r(r_1) + AR(a_2, r_2) \cdot X(a_2, r_2) \cdot C_r(r_2))}{(C_r(r_1) + C_r(r_2))}$$

$$EKR(a_2) = 0.5 \times \frac{(0 \times 0.333 \times 0.2 + 1 \times 1 \times 0.2)}{(0.2 + 0.2)} = 0.25$$

Although both agents  $a_1$  and  $a_2$  have the same agent risk values and have access to exactly one resource each,  $a_2$  exclusively possess all knowledge required for resource  $r_2$ . Hence,  $a_2$  receives a higher metric score.

#### **Exclusive Knowledge for Resource Metric for Agent-Resource Pairs ( $EKR(a_i, r_j)$ )**

The proportion of knowledge possessed by agent  $a_i$  required for resource  $r_j$  out of all  $a_s, k_q$  pairs, where agent  $a_s$  has knowledge  $k_q$  required to use resource  $r_j$ , denoted by  $X(a_i, r_j)$  is given by equation (1.30) described earlier. Therefore,  $EKR(a_i, r_j)$  can be defined as:

$$EKR(a_i, r_j) = AR(a_i, r_j) \cdot C_a(a_i) \cdot C_r(r_j) \cdot X(a_i, r_j) \quad (1.32)$$

Where,

$X(a_i, r_j)$  = The extent to which an agent  $a_i$  exclusively possesses the knowledge required for resource  $r_j$  as defined in equation (1.30).

$AR(a_i, r_j)$  = Value at the row  $i$  and column  $j$  of the binarized Agent x Resource matrix.

$a_i, a_s \in \{a_0, a_1, a_2, \dots, a_N\}$  (set of agent nodes of the network).

$r_j \in \{r_0, r_1, r_2, \dots, r_N\}$  (set of resource nodes).

$C_a(a_i)$  = Composite risk attribute for agent  $a_i$  as defined in equation (1.7).

$C_r(r_j)$  = Standardised sensitivity/criticality of information resource  $r_j$  as defined in equation (1.8).

This metric is the product of the extent to which an agent  $a_i$  exclusively possesses the knowledge required for resource  $r_j$  denoted by  $X(a_i, r_j)$ , the criticality of the resource -  $C_r(r_j)$  and the composite risk attribute of the agent -  $C_a(a_i)$ . The  $AR(a_i, r_j)$  formula ensures that the metric value will be zero if there is no resource access authorisation for  $a_i$  to access the resource  $r_j$ . The maximum possible value for the metric is one, which occurs when three conditions are satisfied:

- 1 Agent  $a_i$  exclusively holds all knowledge required for resource  $r_j$ .
- 2 Agent  $a_i$  has a maximum risk attribute value (equal to 1).
- 3 Resource  $r_j$  has maximum standardised sensitivity/criticality (equal to 1).

The  $EKR(a_i, r_j)$  metric calculation can be demonstrated using the example illustrated in Figure 5-9.  $EKR(a_1, r_1)$  can be calculated as:

$$EKR(a_1, r_1) = AR(a_1, r_1) \cdot C_a(a_1) \cdot C_r(r_1) \cdot X(a_1, r_1)$$

$$EKR(a_1, r_1) = 1 \times 0.5 \times 0.2 \times 0.667 = 0.0667$$

Similarly,  $EKR(a_2, r_2)$  can be calculated:

$$EKR(a_1, r_1) = AR(a_1, r_1) \cdot C_a(a_1) \cdot C_r(r_1) \cdot X(a_1, r_1)$$

$$EKR(a_2, r_2) = 1 \times 0.5 \times 0.2 \times 1 = 0.1$$

$EKR(a_2, r_2)$  is greater than  $EKR(a_1, r_1)$  since  $a_2$  exclusively holds all knowledge required to use  $r_2$  while  $a_1$  does not exclusively hold all knowledge required to use  $r_1$ .

### 5.5.2 Employee having exclusive knowledge to perform a task

Employees possessing exclusive knowledge to perform a task create opportunities for them to obtain unauthorised access to information systems, commit fraud and sabotage without being detected since others in the organisation do not have the skills to monitor and audit their activities. The metric for calculating the risks due to agents exclusively possessing knowledge to perform a task is given two definitions: agent centric -  $EKT(a_i)$  and task assignment centric -  $EKT(a_i, t_p)$ . A simple example used to demonstrate the notations used and EKT metrics is illustrated in Figure 5-10. Furthermore, a short description of the two EKT metrics is presented in Table 5-8 with the aid of a diagram.

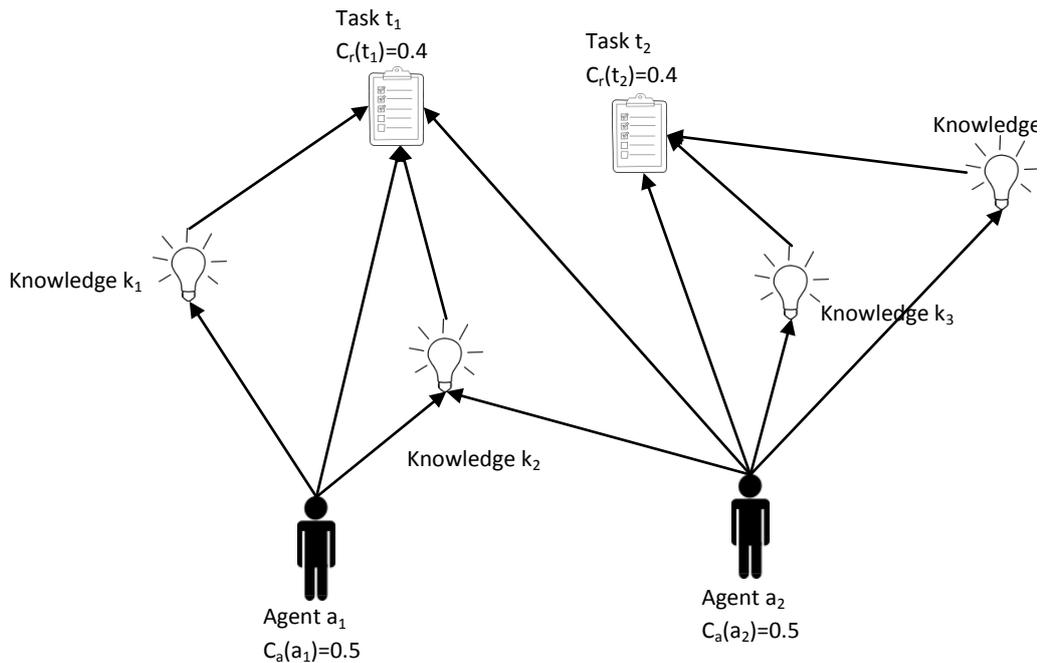


Figure 5-10: A simple example used to demonstrate EKT metrics

#### Exclusive Knowledge for Task Metric for Agent $a_i$ ( $EKT(a_i)$ )

Let the metric depicting agents possessing knowledge to perform a task, denoted by  $AT_k$  be defined as:

$$Let AT_k = AK \times KT$$

The number of  $a_s, k_q$  pairs where agent  $a_s$  has knowledge  $k_q$  required to perform task  $t_p$  is given by:

$$\sum_{s=0}^N AT_K(a_s, t_p) \quad (1.33)$$

Therefore, the proportion of knowledge possessed by agent  $a_i$  required to perform task  $t_p$  out of all  $a_s, k_q$  pairs, where agent  $a_s$  has knowledge  $k_q$  required to perform task  $t_p$ , denoted by  $Y(a_i, t_p)$  is given by:

$$Y(a_i, t_p) = \frac{AT_K(a_i, t_p)}{\sum_{s=0}^N AT_K(a_s, t_p)} \left[ \sum_{s=0}^N AT_K(a_s, t_p) \neq 0 \right] \quad (1.34)$$

Then  $EKT(a_i)$  can be defined as:

$$EKT(a_i) = C_a(a_i) \cdot \frac{\sum_{p=0}^U AT(a_i, t_p) \cdot Y(a_i, t_p) \cdot C_t(t_p)}{\sum_{p=0}^U C_t(t_p)} \quad (1.35)$$

Where,

AK = Agent x Knowledge matrix.

KT = Knowledge x Task matrix.

$AT(a_i, t_p)$  = Value at the row  $i$  and column  $p$  of the binarized Agent x Task matrix.

$AT_K(a_i, t_p)$  = Value at the row  $i$  and column  $p$  of the derived  $AT_K$  matrix.

$a_i, a_s \in \{a_0, a_1, a_2, \dots, a_N\}$  (set of agent nodes of the network).

$t_p \in \{t_0, t_1, t_2, \dots, t_U\}$  (set of resource nodes).

$C_a(a_i)$  = Composite risk attribute for agent  $a_i$  as defined in equation (1.7).

$C_t(t_p)$  = Standardised sensitivity/criticality of task  $t_p$  as defined in equation (1.9).

$EKT(a_i)$  is the weighted proportion of tasks where an agent has exclusive knowledge for the task. The weighting criteria include  $Y(a_i, t_p)$  which measures the extent to which an agent exclusively possesses the knowledge required for a task. The other weighting criteria are sensitivity/criticality of the task ( $C_t(t_p)$ ) and the composite risk attribute for the agent ( $C_a(a_i)$ ). The maximum possible value for the metric is 1, which occurs when two conditions are fulfilled:

1. The agent exclusively holds all knowledge required to perform all tasks in the organisation.
2. The agent has a composite risk attribute value of 1.

The  $EKT(a_i)$  metric is calculated in the same way as the  $EKR(a_i)$  metric demonstrated in the previously. The only difference is instead of resource authorisations of agents,  $EKT(a_i)$  focuses on task assignments.

#### **Exclusive Knowledge for Task Metric for Agent-Task Pairs ( $EKT(a_i, t_p)$ )**

The proportion of knowledge possessed by agent  $a_i$  required for task  $t_p$  out of all  $a_s, k_q$  pairs, where agent  $a_s$  has knowledge  $k_q$  required to perform task  $t_p$ , denoted by  $Y(a_i, t_p)$  is given by equation (1.34). Therefore,  $EKT(a_i, t_p)$  can be defined as:

$$EKT(a_i, t_p) = AT(a_i, t_p) \cdot C_a(a_i) \cdot C_t(t_p) \cdot Y(a_i, t_p) \quad (1.36)$$

Where,

$Y(a_i, t_p)$  = The extent to which an agent  $a_i$  exclusively possesses the knowledge required for task  $t_p$  as defined in equation (1.34).

$AT(a_i, t_p)$  = Value at the row  $i$  and column  $p$  of the binarized Agent x Task matrix.

$a_i, a_s \in \{a_0, a_1, a_2, \dots, a_N\}$  (set of agent nodes of the network).

$t_p \in \{t_0, t_1, t_2, \dots, t_U\}$  (set of resource nodes).

$C_a(a_i)$  = Composite risk attribute for agent  $a_i$  as defined in equation (1.7).

$C_t(t_p)$  = Standardised sensitivity/criticality of task  $t_p$  as defined in equation (1.9).

The maximum possible value for the metric is one. It occurs when three conditions are satisfied:

- 1. Agent  $a_i$  exclusively holds all the knowledge required for task  $t_p$ .
- 2. The agent has a maximum risk attribute value (which is equal to 1).
- 3. The task has the maximum standardised sensitivity/criticality (equal to 1).

The  $EKT(a_i,t_p)$  metric is calculated in the same way as the  $EKR(a_i,r_j)$  metric described earlier while the only difference is that  $EKT(a_i,t_p)$  focus on task assignments of agents instead of resource authorisations.

### 5.6 Metrics for the assessment of risks occurring due to social relationships combined with resource authorisations or task assignments

Access risks in organisations also occur due to combinations of social relationships and other factors such as information resource access authorisations or task assignments. Some of the insider threat cases in Table 4-1 occur due to such combinations, which are indicated under this category in Table 5-1. Although they cannot be strictly regarded as security vulnerabilities, they still present risks that should be analysed. Five types of such risks are listed in Table 5-7.

Table 5-7: Risks occurring due to social relationships combined with resource authorisations or task assignments

No	Risk	Example Case Number (from Table 4-1)
1	An employee has indirect access to information resources	10, 29, 30, 36, 37
2	An employee has transitive access to dependent information resources	10, 37
3	An employee obtains transitive assignment to dependent tasks	37
4	A closely associated group of employees control a resource	31, 32
5	A closely associated group of employees perform a task	32

#### 5.6.1 An employee has indirect access to information resources

Even if users are not directly authorised to access some information resources they can still obtain indirect access through socio-technical pathways. In an organisation, employees need to exchange information with others to perform their duties. These information

exchange paths can involve technology (e.g., email or collaboration systems) or direct interaction (e.g., face-to-face discussions). Due to the assigned role or position of some employees in these organisational information exchange pathways, there exists a greater likelihood of accessing information resources indirectly. In addition to the work related information exchange, some employees can obtain indirect access to information owing to the friendships they have with others or due to the social power associated with them through relationships such as giving advice or occupying powerful positions in the organisational hierarchy. Therefore, this research identifies four different types of relationships that enable employees to obtain indirect access to information, each of which can be modelled as a social network of people:

1. Both formal and informal work related information exchange pathways within the organisation.
2. Friendship and kinship links of employees.
3. Advice relationships among employees.
4. Formal hierarchical relationships in the organisation.

A metric termed the *Indirect Access Capability* is defined to quantify the risk of indirect access per each person (agent centric) and each person-resource pair (agent resource access centric) in the organisation. The analyst can select either one type of relationship mentioned above or use the cumulative effect of a combination of relationship types in calculating the access capability metric values. Borgatti (2005) has emphasized that measures for analysing different types of flows should be selected based on the flow characteristics. The same argument also applies to the problem of indirect access to information. Therefore, this research considers the following attributes of indirect access to information resources via socio-technical pathways in defining the metrics:

1. A path for indirect access will originate from an agent (e.g., employee) and terminate at a specific information resource (resource node).
2. The most damaging forms of indirect access related to insider threats will probably be intentional. Although it is possible for an agent to receive indirect access to information resources unintentionally, it is unlikely that such access would be used for malicious purposes.
3. Based on (2), it is highly likely that an agent will select one of the easiest or shortest paths to obtain indirect access.

4. Agents will likely use strong social links to obtain indirect access since it will be easier to obtain access through people they can trust and influence. Chances of such attempts being reported are also less.
5. The risk of indirect access increases with the increasing sensitivity/criticality of the resource and increasing risk attribute value of the source agent.
6. The risk of indirect access increases with the increase in the risk attribute values of agents involved in the shortest access paths.

Although there are no existing metrics that are appropriate for the attributes mentioned above Freeman’s (1978) closeness measure, based on the geodesic distances between two nodes, have some similarities to the metric defined below. Figure 5-11 illustrates a simple example used to demonstrate the notation and the Indirect Access Capability (IAC) metric calculations. Furthermore, a short description of the metric developed for assessing this risk is presented in Table 5-8. The table also compares the Freeman’s (1978) closeness metric with the metric developed in this research.

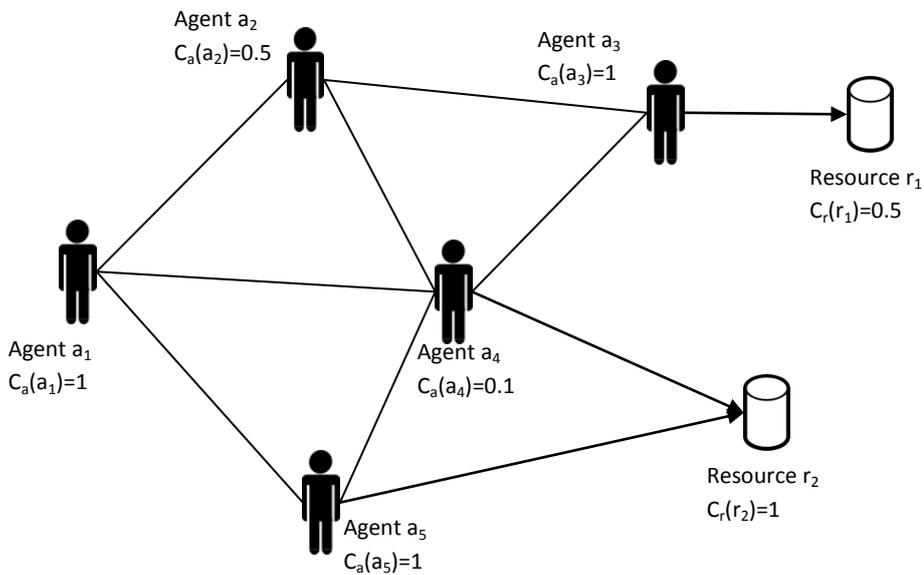


Figure 5-11: A simple example used to illustrate IAC metrics

**Indirect Access Capability of an agent with respect to a resource (IAC(a<sub>i</sub>,r<sub>j</sub>))**

Let  $p_x$  be one of the many possible shortest paths for agent  $a_i$  to access information resource  $r_j$  through the social network. (Note that there can be more than one shortest path of equal length for an agent to access a resource through a social network.)

$$p_x = \{a_i, a_1, a_2, \dots, a_n, r_j\} \quad (1.37)$$

If the shortest path length for  $a_i$  to access  $r_j$  is  $L(a_i, r_j)$  (path length  $L(a_i, r_j)$  is the number of hops from  $a_i$  to  $r_j$  via the path  $p_x$ ), then the average risk attribute value of all agents (including the source agent  $a_i$ ) involved in path  $p_x$ , denoted by  $C_A(p_x)$  is given by:

$$C_A(p_x) = \frac{C_a(a_i) + C_a(a_1) + C_a(a_2) + \dots + C_a(a_n)}{L(a_i, r_j)} \quad (1.38)$$

Therefore, the indirect access capability for agent  $a_i$  to access resource  $r_j$  via a specific shortest path  $p_x$  is given by:

$$\frac{C_A(p_x)}{L(a_i, r_j)}$$

Assuming that there are  $W$  shortest paths between  $a_i$  and  $r_j$  the indirect access capability of  $a_i$  with respect to resource  $r_j$  is given by:

$$IAC(a_i, r_j) = \frac{C_r(r_j)}{W \cdot L(a_i, r_j)} \sum_{x=1}^W C_A(p_x) \quad (1.39)$$

Where;

$a_i, \in \{a_0, a_1, a_2, \dots, a_N\}$  (set of agent nodes of the network).

$r_j \in \{r_0, r_1, r_2, \dots, r_M\}$  (set of resource nodes).

$C_a(a_i)$  = Composite risk attribute for agent  $a_i$  as defined in equation (1.7).

$C_r(r_j)$  = Standardised sensitivity/criticality of information resource  $r_j$  as defined in equation (1.8).

$L(a_i, r_j)$  = length of the shortest path from  $a_i$  to  $r_j$ .

$W$  = number of shortest paths of equal length available for  $a_i$  to access  $r_j$ .

According to the equation (1.39) derived above, indirect access capability increases with the decrease in shortest path length. It also increases with the increase in the risk attribute

values of agents involved and the increase in the resource sensitivity/criticality. When there is more than one shortest path of equal length, the equation finds an average metric value over all these shortest paths. It is important to note that this metric is defined only for resources that are accessible by the agent either through direct authorisation or indirectly through the social networks. If there is no path between the agent and the resource  $IAC(a_i, r_j)$ , metric value is defined to be zero. The maximum possible value for the metric is one (1), which occurs when:

1. The agent has direct access to the resource.
2. The agent has a maximum composite risk attribute ( $C_a(a_i)$ ) value of 1.
3. The resource has a maximum sensitivity/criticality ( $C_r(r_j)$ ) of 1.

The  $IAC(a_i, r_j)$  metric calculation can be demonstrated using the example illustrated in Figure 5-11. According to the figure, there are two shortest paths of equal length for agent  $a_1$  to access resource  $r_1$ . They are:

$$p_1 = \{a_1, a_2, a_3, r_1\} \text{ and } p_2 = \{a_1, a_4, a_3, r_1\}$$

Also the shortest path length  $L(a_1, r_1) = 3$

Therefore:

$$C_A(p_1) = \frac{C_a(a_1) + C_a(a_2) + C_a(a_3)}{L(a_1, r_1)} = \frac{1 + 0.5 + 1}{3} = 0.833$$

$$C_A(p_2) = \frac{C_a(a_1) + C_a(a_4) + C_a(a_3)}{L(a_1, r_1)} = \frac{1 + 0.1 + 1}{3} = 0.700$$

Then,

$$IAC(a_1, r_1) = \frac{C_r(r_1)}{W \cdot L(a_1, r_1)} (C_A(p_1) + C_A(p_2))$$

$$IAC(a_1, r_1) = \frac{0.5}{2 \times 3} (0.833 + 0.700) = 0.128$$

Similarly, there are two shortest paths for agent  $a_1$  to access  $r_2$ . They are:

$$p_1 = \{a_1, a_4, r_2\} \text{ and } p_2 = \{a_1, a_5, r_2\}$$

Also the shortest path length  $L(a_1, r_2) = 2$

Therefore:

$$C_A(p_1) = \frac{C_a(a_1) + C_a(a_4)}{L(a_1, r_2)} = \frac{1 + 0.1}{2} = 0.550$$

$$C_A(p_2) = \frac{C_a(a_1) + C_a(a_5)}{L(a_1, r_2)} = \frac{1 + 1}{2} = 1$$

Then,

$$IAC(a_1, r_2) = \frac{C_r(r_2)}{W \cdot L(a_1, r_2)} (C_A(p_1) + C_A(p_2))$$

$$IAC(a_1, r_2) = \frac{1}{2 \times 2} (0.550 + 1) = 0.388$$

Agent  $a_1$  can access the resource  $r_2$  via a shorter path than  $r_1$ . Also, the  $r_2$  has a higher resource criticality. Therefore,  $IAC(a_1, r_2)$  is higher than  $IAC(a_1, r_1)$ .

### Indirect Access Capability of an agent $a_i$ ( $IAC(a_i)$ )

The indirect access capability of an agent  $a_i$  ( $IAC(a_i)$ ) is the cumulative of all indirect access capabilities of the agent with respect to all the resources of the organisation. If the agent  $a_i$  is in an organisation with  $M$  information resources, then the metric  $IAC(a_i)$  is defined as:

$$IAC(a_i) = \frac{1}{M} \sum_{j=1}^M IAC(a_i, r_j) \quad (1.40)$$

Where;

$r \in \{r_1, r_2, r_3, \dots, r_M\}$  is a set of resource nodes of the organisation.

$IAC(a_i, r_j)$  is defined as in equation (1.39).

M = number of information resources of the organisation.

If there is no path for the agent to access a particular resource  $r$ , the metric takes the corresponding  $IAC(a_i, r_j)$  value to be zero. The maximum possible value for this metric is 1, which can only occur if the following conditions are satisfied:

1. The agent has direct authorisations to all the resources of the organisation.
2. The agent has a maximum risk attribute value (equal to 1).
3. All the resources in the organisation have a highest standardised sensitivity value (equal to 1).

The  $IAC(a_i)$  calculation can be demonstrated using the example illustrated in Figure 5-11. The  $IAC(a_1)$  value can be calculated as:

$$IAC(a_1) = \frac{1}{2}(IAC(a_1, r_1) + IAC(a_2, r_2))$$

Note that there are two resources in the diagram. Therefore, value M is two (2). The values of  $IAC(a_1, r_1)$  and  $IAC(a_1, r_2)$  were calculated previously.

$$IAC(a_1) = \frac{1}{2}(0.128 + 0.388) = 0.258$$

### 5.6.2 An employee has transitive access to dependent information resources

Although enforcing dual control ensures that a single agent does not have access to dependent information resources, transitive access to a dependent information resource is still possible through the social networks of the agent. The four types of social relationships mentioned in section 5.6.1 can lead to such transitive access. However, according to Granovetter (1973; 1983), only strong links are important in forming transitive relationships. Therefore, only strong links in the social networks should be considered when assessing risks due to transitive access to dependent information resources. A metric termed Transitive Access to dependent Resources (TAR) is defined for this purpose. The metric is given two definitions:  $TAR(a_i)$  (agent centric), and  $TAR(a_i, r_j)$  (agent resource access centric). Figure 5-12 illustrates a simple example used to demonstrate the notation and the calculation of TAR metrics. Furthermore, a short description of the TAR metrics is presented in Table 5-8 with the aid of a diagram.

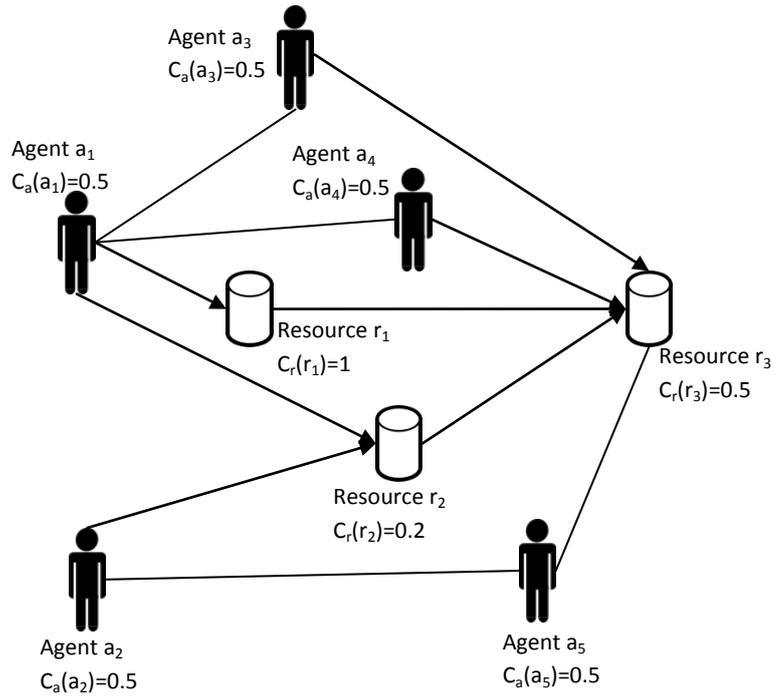


Figure 5-12: A simple example to demonstrate TAR metrics

**Transitive access to dependent resources metric for resource access relationships (TAR(a<sub>i</sub>,r<sub>j</sub>))**

Let Agent x Resource (resource access) matrix, weighted according to resource sensitivities (C<sub>r</sub>(r<sub>j</sub>)), denoted by AR<sub>w</sub>, be defined as:

$$\forall i \forall j : AR_w(a_i, r_j) = C_r(r_j) \cdot AR(a_i, r_j) \tag{1.41}$$

Then let,

$$AR_R = AR_w \times RR \tag{1.42}$$

Each element (a<sub>i</sub>,r<sub>j</sub>) of the AR<sub>R</sub> matrix corresponds to the weighted number of dependent resources of r<sub>j</sub> that are accessible by agent a<sub>i</sub>. Similarly, let the Agent x Agent matrix (social network), weighted according to the risk attribute values of the agent receiving the tie (C<sub>a</sub>(a<sub>s</sub>)), denoted by AA<sub>s</sub>, defined as:

$$\forall i \forall s : AA_s = C_a(a_s) \cdot AA(a_i, a_s) \tag{1.43}$$

Then let,

$$AR_A = AA_S \times AR \quad (1.44)$$

Each element  $(a_i, r_j)$  of the  $AR_A$  matrix corresponds to the weighted number of associates of agent  $a_i$  through which  $a_i$  can access  $r_j$ . Then  $TAR(a_i, r_j)$  can be defined as:

$$TAR(a_i, r_j) = C_a(a_i) \cdot C_r(r_j) \cdot \frac{AR_R(a_i, r_j) \cdot AR_A(a_i, r_j) [AR(a_i, r_j) = 0]}{\left( \sum_{k=1}^M C_r(r_k) [k \neq j] \right) \left( \sum_{s=1}^N C_a(a_s) [s \neq i] \right)} \quad (1.45)$$

Where,

$r_j, r_k \in \{r_1, r_2, r_3, \dots, r_M\}$  is a set of resource nodes of the organisation.

$a_i, a_s \in \{a_1, a_2, a_3, \dots, a_N\}$  is a set of agent nodes of the organisation.

$C_a(a_i), C_a(a_s)$  are the composite risk attributes of agents  $a_i$  and  $a_s$  respectively as defined in equation (1.7).

$C_r(r_j), C_r(r_k)$  are the standardised sensitivities/criticalities of resources  $r_i$  and  $r_k$  respectively as defined in equation (1.8).

According to the equation (1.45),  $TAR(a_i, r_j)$  value increases when there are more resources accessible by  $a_i$  that are dependent on  $r_j$  and when there are more associates of agent  $a_i$  who have access to the resource  $r_j$  (numerator calculates the product of these two quantities provided there is no direct authorisation for agent  $a_i$  to access resource  $r_j$ ). The results are also weighted according to the composite risk attribute value of agent  $a_i$  and the resource sensitivity of  $r_j$ . The denominator represents the product of cumulative sensitivities of all the resources in the organisation (except  $r_j$ ) and the cumulative risk attribute values of all the agents in the organisation (except  $a_i$ ). The maximum possible value for the metric is one (1), which occurs when following conditions are true:

1. All other agents in the social network are associates of agent  $a_i$  and all of them have authorisations to access resource  $r_j$ .
2. Agent  $a_i$  has direct access to all other resources and resource  $r_j$  is dependent on all the other resources.

3. Agent  $a_i$  has a maximum composite risk attribute value of 1.
4. Resource  $r_j$  has a maximum sensitivity/criticality of 1.

TAR( $a_i, r_j$ ) metric calculation can be demonstrated using the example in Figure 5-12.

*AR matrix*

	$r_1$	$r_2$	$r_3$
$a_1$	1	1	0
$a_2$	0	1	0
$a_3$	0	0	1
$a_4$	0	0	1
$a_5$	0	0	1

$$\forall i \forall j : AR_w(a_i, r_j) = C_r(r_j) \cdot AR(a_i, r_j)$$

	$r_1$	$r_2$	$r_3$
$a_1$	1	0.2	0
$a_2$	0	0.2	0
$a_3$	0	0	0.5
$a_4$	0	0	0.5
$a_5$	0	0	0.5

*matrix RR*

	$r_1$	$r_2$	$r_3$
$r_1$	0	0	1
$r_2$	0	0	1
$r_3$	0	0	0

$$AR_R = AR_w \times RR$$

	$r_1$	$r_2$	$r_3$
$a_1$	0	0	1.2
$a_2$	0	0	0.2
$a_3$	0	0	0
$a_4$	0	0	0
$a_5$	0	0	0

*matrix AA*

	$a_1$	$a_2$	$a_3$	$a_4$	$a_5$
$a_1$	0	0	1	1	0
$a_2$	0	0	0	0	1
$a_3$	1	0	0	0	0
$a_4$	1	0	0	0	0
$a_5$	0	1	0	0	0

$$\forall i \forall s : AA_S = C_a(a_s) \cdot AA(a_i, a_s)$$

	$a_1$	$a_2$	$a_3$	$a_4$	$a_5$
$a_1$	0	0	0.5	0.5	0
$a_2$	0	0	0	0	0.5
$a_3$	0.5	0	0	0	0
$a_4$	0.5	0	0	0	0
$a_5$	0	0.5	0	0	0

$$AR_A = AA_S \times AR$$

	$r_1$	$r_2$	$r_3$
$a_1$	0	0	1
$a_2$	0	0	0.5
$a_3$	0.5	0.5	0
$a_4$	0.5	0.5	0
$a_5$	0	0.5	0

Therefore,  $TAR(a_1, r_3)$  can be calculated as:

$$TAR(a_1, r_3) = C_a(a_1) \cdot C_r(r_3) \cdot \frac{AR_R(a_1, r_3) \cdot AR_A(a_1, r_3) [AR(a_1, r_3) = 0]}{(C_r(r_1) + C_r(r_2))(C_a(a_2) + C_a(a_3) + C_a(a_4) + C_a(a_5))}$$

$$TAR(a_1, r_3) = (0.5) \times (0.5) \times \frac{(1.2) \times (1)}{(1 + 0.2)(0.5 + 0.5 + 0.5 + 0.5)} = 0.125$$

Similarly,  $TAR(a_2, r_3)$  can be calculated as:

$$TAR(a_2, r_3) = C_a(a_2) \cdot C_r(r_3) \cdot \frac{AR_R(a_2, r_3) \cdot AR_A(a_2, r_3) [AR(a_2, r_3) = 0]}{(C_r(r_1) + C_r(r_2))(C_a(a_1) + C_a(a_3) + C_a(a_4) + C_a(a_5))}$$

$$TAR(a_2, r_3) = (0.5) \times (0.5) \times \frac{(0.2) \times (0.5)}{(1 + 0.2)(0.5 + 0.5 + 0.5 + 0.5)} = 0.042$$

Although agents  $a_1$  and  $a_2$  have the same composite agent risk,  $(a_1, r_3)$  receives a higher TAR metric score than  $(a_2, r_2)$  due to several reasons. From Figure 5-12 it is clear that  $a_1$  can access  $r_3$  via two associates ( $a_3$  and  $a_4$ ) while  $a_2$  can only access  $r_3$  via  $a_5$ . Furthermore,  $a_1$  has access to two resources ( $r_1$  and  $r_2$ ) that depend on  $r_3$  while  $a_2$  has access to only one resource ( $r_2$ ) that depend on  $r_3$ .

### Transitive access to dependent resources metric for agent $a_i$ ( $TAR(a_i)$ )

Transitive access to dependent resources metric for agents ( $TAR(a_i)$ ) is the cumulative of all the  $TAR(a_i, r_j)$  values of agent  $a_i$  with respect to all the resources of the organisation. If there are M number of resources in an organisation,  $TAR(a_i)$  of agent  $a$  can be defined as:

$$TAR(a_i) = \frac{1}{M} \sum_{j=1}^M TAR(a_i, r_j) \quad (1.46)$$

Where;

$r_j \in \{r_1, r_2, r_3, \dots, r_M\}$  is a set of resource nodes of the organisation.

$TAR(a_i, r_j)$  is defined as in equation (1.45).

$M$  = number of information resources of the organisation.

The maximum possible value for this metric is 1, which occurs when the agent has  $TAR(a_i, r_j)$  values of 1 for all resources of the organisation.  $TAR(a_i)$  metric calculation can also be demonstrated using the example illustrated in Figure 5-12.  $TAR(a_1)$  can be calculated as:

$$TAR(a_1) = \frac{1}{3} (TAR(a_1, r_1) + TAR(a_1, r_2) + TAR(a_1, r_3))$$

$$TAR(a_1) = \frac{1}{3} (0 + 0 + 0.125) = 0.042$$

Note that  $TAR(a_1, r_1)$  and  $TAR(a_1, r_2)$  values are zero (0) since agent  $a_1$  has direct access to  $r_1$  and  $r_2$ .

### 5.6.3 An employee obtains transitive assignment to dependent tasks

Although enforcing separation of duty ensures that a single agent does not perform dependent tasks, transitive assignment to dependent tasks is still possible through the social networks of the agent. The four types of social relationships mentioned in Section 5.6.1 can lead to such transitive assignment. However, as mentioned under 5.6.2 only strong ties are important in the analysis of such transitive relationships. A metric termed Transitive Assignment to dependent Tasks (TAT) is defined for the assessment of risks due to employees obtaining such transitive task assignments. The metric is given two definitions –  $TAT(a_i)$  (agent centric) and  $TAT(a_i, t_p)$  (task assignment centric). Figure 5-13 is an illustration of the notations used to define the TAT metrics. The TAT metrics are defined in the same way as TAR metrics defined under section 5.6.2. The only difference is that TAT metrics focus on task assignments instead of resource access authorisations. Furthermore, a short description of the TAT metrics is presented in Table 5-8 with the aid of a diagram.

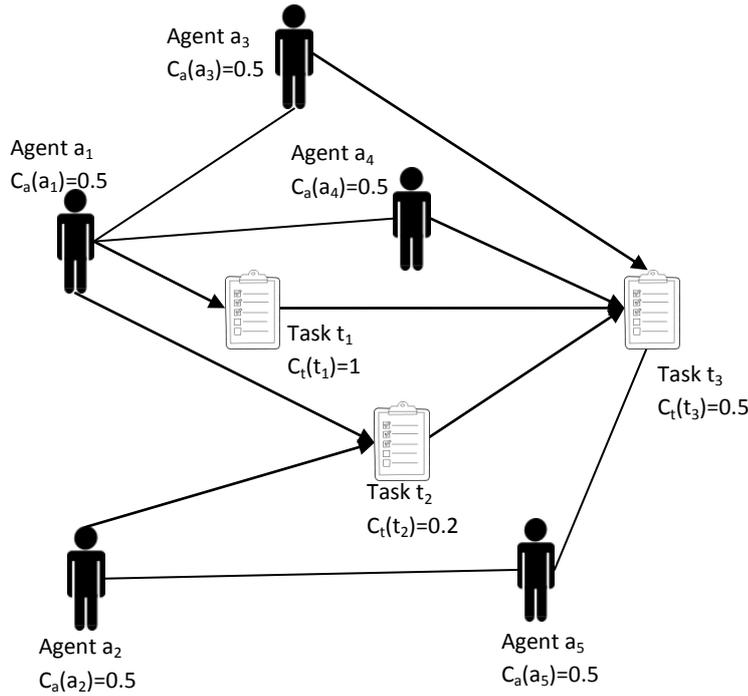


Figure 5-13: A simple example used to illustrate TAT metrics

**Transitive assignment to dependent tasks metric for task assignment relationships (TAT(a<sub>i</sub>, t<sub>p</sub>))**

Let Agent x Task (task assignment) matrix weighted according to task criticalities - C<sub>t</sub>(t<sub>p</sub>), denoted by AT<sub>w</sub>, be defined as:

$$\forall i \forall p : AT_w = C_t(t_p) \cdot AT(a_i, t_p) \tag{1.47}$$

Then let,

$$AT_T = AT_w \times TT \tag{1.48}$$

Each element (a<sub>i</sub>, t<sub>p</sub>) of the AT<sub>T</sub> matrix corresponds to the weighted number of tasks dependent on t<sub>p</sub> that are performed by agent a<sub>i</sub>. Similarly, let Agent x Agent matrix (social network), weighted according to the risk attribute values of the agents receiving the tie (C<sub>a</sub>(a<sub>s</sub>)), denoted by AA<sub>s</sub>, defined as:

$$\forall i \forall s : AA_s = C_a(a_s) \cdot AA(a_i, a_s) \tag{1.49}$$

Then let,

$$AT_A = AA_S \times AT \quad (1.50)$$

Each element  $(a_i, t_p)$  of the  $AT_A$  matrix corresponds to the weighted number of associates of agent  $a_i$  performing the task  $t_p$ . Then  $TAT(a_i, t_p)$  can be defined as:

$$TAT(a_i, t_p) = C_a(a_i) \cdot C_t(t_p) \frac{AT_T(a_i, t_p) \cdot AT_A(a_i, t_p) [AT(a_i, t_p) = 0]}{\left( \sum_{q=1}^U C_t(t_q) [q \neq p] \right) \left( \sum_{s=1}^N C_a(a_s) [s \neq i] \right)} \quad (1.51)$$

Where,

$t_p, t_q \in \{t_1, t_2, t_3, \dots, t_U\}$  is a set of task nodes of the organisation.

$a_i, a_s \in \{a_1, a_2, a_3, \dots, a_N\}$  is a set of agent nodes of the organisation.

$C_a(a_i), C_a(a_s)$  are the composite risk attributes of agents  $a_i$  and  $a_s$  respectively as defined in equation (1.7).

$C_t(t_p), C_t(t_q)$  are the standardised sensitivities/criticalities of tasks  $t_p$  and  $t_q$  as defined in equation (1.9).

According to the equation (1.51),  $TAT(a_i, t_p)$  value increases when there are more tasks performed by  $a_i$  that depend on  $t_p$  and when there are more associates of agent  $a_i$  who perform the task  $t_p$  (numerator calculates the product of these two quantities provided agent  $a_i$  is not assigned to task  $t_p$ ). The results are also weighted according to the composite risk attribute value of agent  $a_i$  and the task criticality of  $t_p$ . The denominator represents the product of cumulative criticalities of all the tasks in the organisation (except  $t_p$ ) and the cumulative risk attribute values of all the agents in the organisation (except  $a_i$ ). The maximum possible value for the metric is one (1), which occurs when following conditions are true:

1. All other agents in the social network are associates of agent  $a_i$  and all of them are assigned to task  $t_p$ .

2. Agent  $a_i$  is assigned to all other tasks and task  $t_p$  is dependent on all other tasks.
3. Agent  $a_i$  has a maximum composite risk attribute value of 1.
4. Task  $t_p$  has a maximum sensitivity/criticality of 1.

#### **Transitive assignment to dependent tasks metric for agent $a_i$ (TAT( $a_i$ ))**

Transitive assignment to dependent tasks metric for agents (TAT( $a_i$ )) is the cumulative of all the TAT( $a_i, t_p$ ) values of agent  $a_i$  with respect to all the tasks of the organisation. If there are  $U$  number of tasks in an organisation, TAT( $a_i$ ) of agent  $a_i$  can be defined as:

$$TAT(a_i) = \frac{1}{U} \sum_{p=1}^U TAT(a_i, t_p) \quad (1.52)$$

Where;

$t_p \in \{t_1, t_2, t_3, \dots, t_U\}$  is a set of task nodes of the organisation.

TAT( $a_i, t_p$ ) is defined as in equation (1.51).

$U$  = Total number of tasks in the organisation.

The maximum possible value for this metric is 1 which occurs when the agent  $a_i$  receives a TAT( $a_i, t_p$ ) score of 1 for all tasks of the organisation.

#### **5.6.4 A closely associated group of employees control a resource**

When a closely associated group of employees control a resource, it can lead to collusion and there is a greater risk of malicious activities taking place without being detected. Clustering Coefficient (Watts and Strogatz 1998), which calculates the proportion of ties actually present among the neighbours of a given node out of the total number of possible ties among them, is a metric commonly used to identify cohesive subgroups. Although clustering coefficient is defined for single mode networks, a similar conceptualisation has been used to define the metric, termed Agent Clustering for Resource (ACR), for the assessment of risks due to closely associated groups of employees controlling a resource. Figure 5-14 illustrates a simple example used to demonstrate the ACR metrics. Furthermore, a short description of the ACR metric is presented in Table 5-8 with the aid of

a diagram. The table also compares the existing clustering coefficient metric with the metric developed in this research.

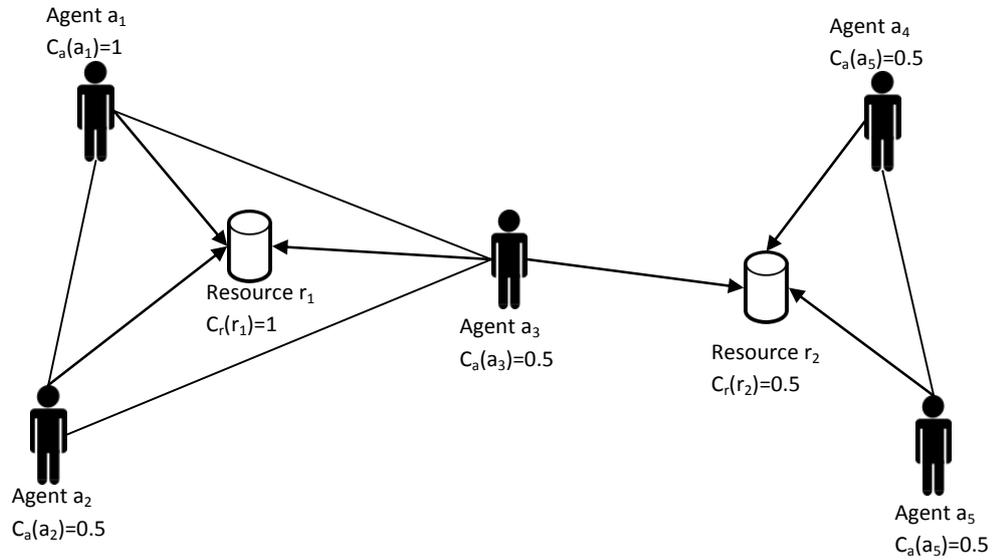


Figure 5-14: Example used to illustrate the ACR metrics

**Agent clustering for resource metric for resource  $r_j$  ( $ACR(r_j)$ )**

Assume that a given resource  $r_j$  in the Agent x Resource network is accessed by the subset of agents denoted by  $A_r = \{a_1, a_2, a_3, \dots, a_N\}$ . Then, let the sub-graph of the Agent x Agent (social) network consisting of the same nodes in  $A_r$  be  $AA_S$ .

Then, Agent Clustering for Resource ( $ACR(r_j)$ ) metric is defined as:

$$ACR(r_j) = \frac{2 \cdot C_r(r_j) \sum_{i=1}^N \sum_{s=1}^N AA_S(a_i, a_s) \cdot C_a(a_i) \cdot C_a(a_s)}{N(N-1)} \quad [N > 1] \tag{1.53}$$

Where,

$N$  = the number of agents in the subset  $A_r$ .

$C_a(a_s)$  and  $C_a(a_i)$  = the composite risk attributes of the agents  $a_s$  and  $a_i$  defined in the equation (1.7).

$C_r(r_j)$  = standardised sensitivity/criticality of the resource  $r_j$  defined in equation (1.8).

$a_i, a_s \in \{a_1, a_2, a_3, \dots\}$  is a set of agent nodes of the organisation.

There should be more than one person accessing the resource for this metric to be meaningful ( $N > 1$ ). Otherwise the metric value is defined to be zero (0). The maximum value possible for this metric is one (1), which occurs when the following conditions are satisfied:

1. All the agents in the subset  $A_r$  are associated with each other.
2. All the agents in the subset have a maximum risk attribute value of 1 and the resource  $r$  has a maximum sensitivity/criticality of 1.

The  $ACR(r_j)$  metric calculation can be demonstrated using the example in Figure 5-14.  $ACR(r_1)$  can be calculated as:

$$ACR(r_1) = \frac{2 \cdot C_r(r_1)(C_a(a_1) \cdot C_a(a_2) + C_a(a_1) \cdot C_a(a_3) + C_a(a_2) \cdot C_a(a_3))}{3(3-1)}$$

$$ACR(r_1) = \frac{2 \times 1(1 \times 0.5 + 1 \times 0.5 + 0.5 \times 0.5)}{3(3-1)} = 0.417$$

Similarly,  $ACR(r_2)$  can be calculated as:

$$ACR(r_2) = \frac{2 \cdot C_r(r_2)(C_a(a_4) \cdot C_a(a_5))}{3(3-1)}$$

$$ACR(r_2) = \frac{2 \times 0.5(0.5 \times 0.5)}{3(3-1)} = 0.042$$

Note that there are three social connections among the three agents ( $a_1, a_2, a_3$ ) accessing resource  $r_1$  while there is only one social connection among the three agents ( $a_3, a_4, a_5$ ) accessing resource  $r_2$ . Also, resource  $r_1$  has a higher sensitivity/criticality than  $r_2$ . Due to these factors  $r_1$  receives a higher ACR metric score than  $r_2$ .

### 5.6.5 A closely associated group of employees perform a task

Similarly to the risk described under 5.6.5, a closely associated group of employees performing a task can also lead to collusion and there is a greater risk of malicious activities taking place without being detected. Therefore, a metric termed Agent Clustering for Task (ACT) is defined for the assessment of such risks based on a similar conceptualisation to the

Clustering Coefficient measure of Watts and Strogatz (1998). The ACT metric is defined in the same way as the ACR metric in section 5.6.4. The only difference between the two metrics is that ACR focuses on agent clustering around a resource while ACT focuses on agent clustering with regards to a task. Figure 5-15 illustrates a simple example used to demonstrate the ACT metric. Furthermore, a short description of the ACT metric is presented in Table 5-8 with the aid of a diagram.

**Agent clustering for task metric for task  $t_p$  ( $ACT(t_p)$ )**

Assume that a given task  $t_p$  in the Agent x Task network is performed by the subset of agents denoted by  $A_t = \{a_1, a_2, a_3, \dots, a_N\}$ . Then let the sub-graph of the Agent x Agent (social) network consisting of the same nodes in  $A_t$  be  $AA_s$ .

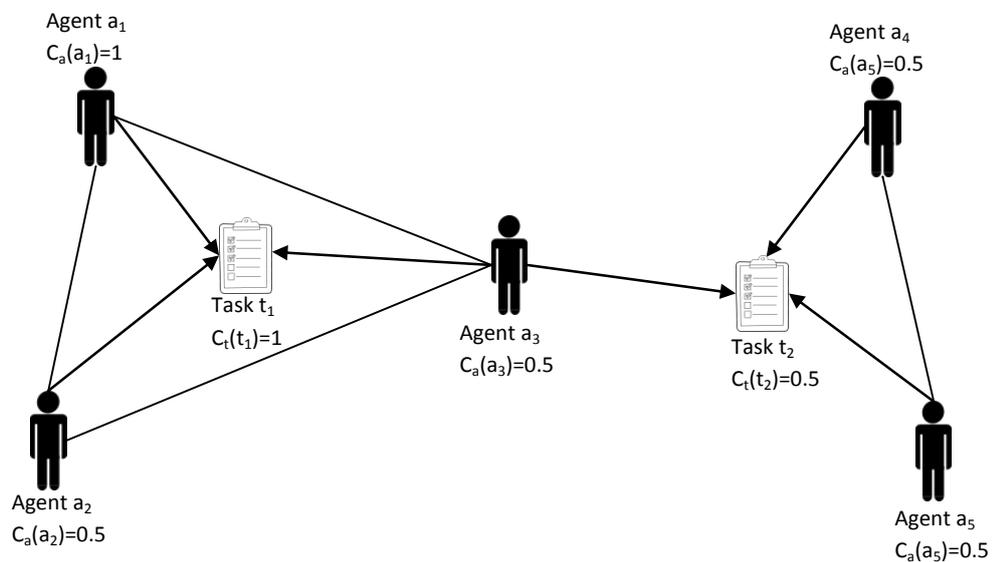


Figure 5-15: Simple example used to demonstrate ACT metric

Then, Agent Clustering for Task ( $ACT(t_p)$ ) metric is defined as:

$$ACT(t_p) = \frac{2 \cdot C_t(t_p) \sum_{i=1}^N \sum_{s=1}^N AA_s \cdot C_a(a_i) \cdot C_a(a_s)}{N(N-1)} [N > 1] \quad (1.54)$$

Where,

$N$  = the number of agents in the subset  $A_t$ .

$C_a(a_i)$  and  $C_a(a_s)$  = composite risk attributes of the agents  $a_i$  and  $a_s$  defined in the equation (1.7).

$C_t(t_p)$  = Standardised criticality of the task  $t$  defined in equation (1.8).

$a_i, a_s \in \{a_1, a_2, a_3, \dots\}$  is a set of agent nodes of the organisation.

There should be more than one person assigned for the task for this metric to be meaningful ( $N > 1$ ). Otherwise the metric value is defined to be zero (0). The maximum value possible for this metric is one (1), which occurs when the following conditions are fulfilled:

1. All the agents in the subset  $A_t$  are associated with each other.
2. All the agents in the subset  $A_t$  have a maximum risk attribute value of 1 and the task  $t$  has a maximum sensitivity/criticality of 1.

## 5.7 Discussion and Summary of Metrics

Definition of information systems security risk, adopted from ISO/IEC 27002:2005 (International Organisation for Standardisation 2005b, 2), is given in Chapter 1 as “combination of the probability of a (threat) event and its consequence.” Therefore, the risk assessment metrics defined here incorporate both the probability (likelihood) of a threat event and its consequence (impact). Note that the metrics are a combination of two factors:

- The relationships of an entity. (or the structure of the networks it is embedded in)
- The intrinsic properties (attributes) of the entity and other related entities.

The relationships primarily account for the likelihood or probability of a threat event. Out of the intrinsic properties, the composite agent risk attribute of an agent  $a_i$  -  $C_a(a_i)$  - is calculated based on six intrinsic characteristics of agents as outlined in Section 5.2.2. According to previous research by Cappelli et al. (2012), agents who exhibit these intrinsic risk characteristics have a greater probability of committing insider attacks. Therefore, the composite agent risk attribute -  $C_a(a_i)$  also represents likelihood criteria in the risk metrics.

On the other hand, the sensitivity/criticality of a resource  $r_j - C_r(r_j)$  and criticality of a task  $t_k - C_t(t_k)$  represent impact criteria in the metrics since they denote the overall importance of the resource or the task in terms of confidentiality, integrity and availability.

The incorporation of likelihood and impact criteria in the risk metrics can be illustrated using an example. VNA( $a_i$ ) metric (agent centric) is defined in equation (1.16) as:

Let  $AR_T$  matrix be

$AR_T = AT \times TR$  then;

$$VNA(a_i) = C_a(a_i) \frac{\sum_{j=0}^M C_r(r_j) \cdot AR(a_i, r_j) [AR_T(a_i, r_j) = 0]}{\sum_{j=0}^M C_r(r_j) \cdot AR(a_i, r_j)}$$

In terms of the relationships, the numerator of the metric represents the number of information resource access authorisations of the agent that are not required to perform tasks assigned to him while the denominator represents the total number of resource access authorisations of the agent. When the agent has access to more resources that are not required for his tasks the value of the metric goes up. In other words, the likelihood of an agent committing an insider threat event is higher when the agent has access to more resources not required for the tasks assigned to him.

In terms of the intrinsic risk properties of agents, the metric is weighted according to the composite risk attribute -  $C_a(a_i)$ . This means that agents with higher  $C_a(a_i)$  values are taken as more likely to commit an insider threat event, which results in higher metric scores. At the same time, both numerator and denominator of the metric are weighted according to resource sensitivity/criticality -  $C_r(r_j)$  - values of the resources involved. This represents impact criteria since an agent having excessive access to more sensitive or critical information resources results in higher metric values. Similar reasoning can be provided for other metrics presented in this chapter.

Table 5-8 provides a summary of metrics presented in this chapter. Legend for the symbols used in Table 5-8 is given below:



Person



Information  
Resources

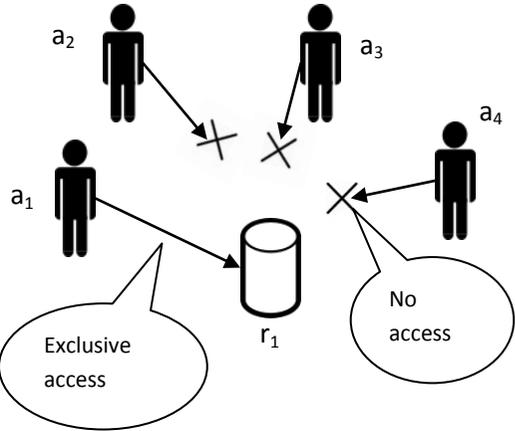


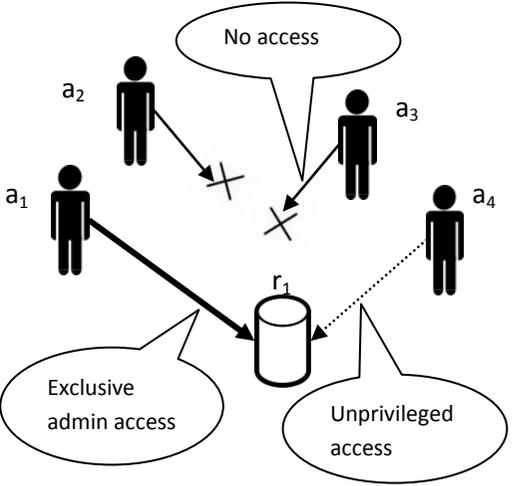
Knowledge

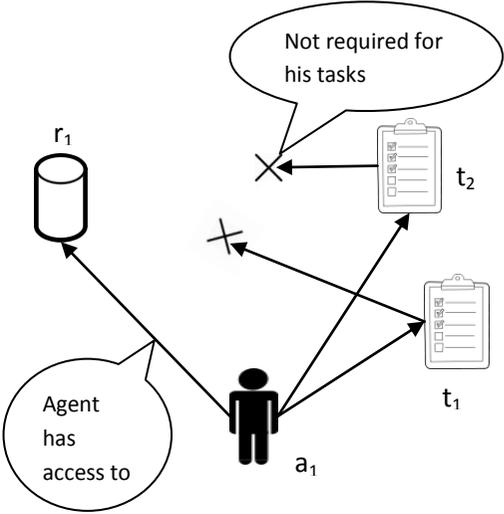


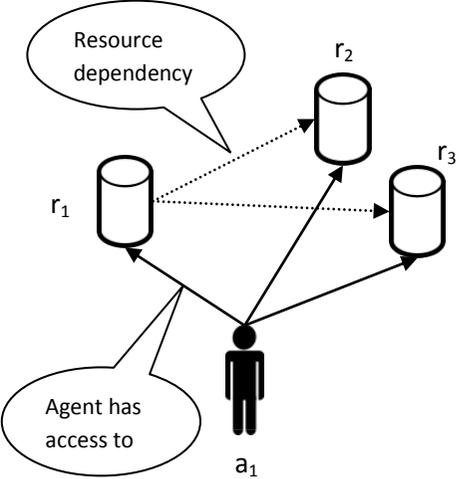
Task

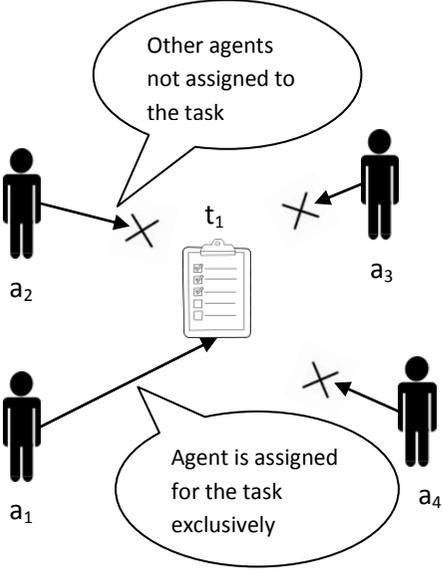
Table 5-8: Summary of the metrics presented in this chapter

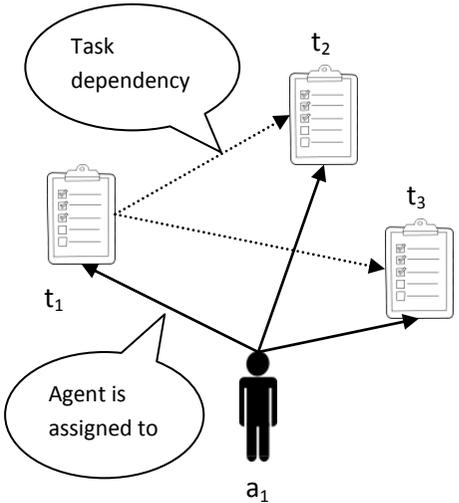
Risk type and metric	Description	Related metric in previous research	Formal definition of the metric
<p>Page 106</p> <p>5.3.1</p> <p>Employee having exclusive access to information resources</p> <p>Metric: ERA</p>	 <p>ERA metric is used to analyse and highlight instances where only one (or very few) employees has exclusive access to an information resource</p>	<p>Resource Exclusivity (RE) from (Carley et al. 2012) restated using the notation used in this chapter:</p> $RE = \sum_{j=0}^M AR(a_i, r_j) \cdot e^{1 - \sum_{s=0}^N AR(a_s, r_j)}$ <p>Where;</p> <p>RE=Resource exclusivity of agent <math>a_i</math></p> <p><math>AR(a_i, r_j)</math> = Value at row <math>i</math> and column <math>j</math> of the binarized Agent x Resource matrix</p> <p><math>r_j \in \{r_0, r_1, r_2, \dots, r_M\}</math> (set of resource nodes)</p> <p><math>a_i, a_s \in \{a_0, a_1, a_2, \dots, a_N\}</math> (set of agent nodes)</p> <p>Note:</p> <ul style="list-style-type: none"> <li>• This metric has only an agent centric definition</li> <li>• It does not incorporate agent risk values or resource criticalities</li> </ul>	<p>ERA(<math>r_j</math>) – Resource centric – equation (1.10)</p> $ERA(r_j) = C_r(r_j) \cdot e^{1 - \sum_{i=0}^N \frac{1}{C_a(a_i)} \cdot AR(a_i, r_j)}$ <p>ERA(<math>a_i, r_j</math>) – Resource access authorisation centric (per agent, resource pair) – equation (1.12)</p> $ERA(a_i, r_j) = AR(a_i, r_j) \cdot C_a(a_i) \cdot ERA(r_j)$ <p>ERA(<math>a_i</math>) – Agent centric – equation (1.11)</p> $ERA(a_i) = C_a(a_i) \cdot \frac{\sum_{j=0}^M AR(a_i, r_j) \cdot ERA(r_j)}{\sum_{j=0}^M C_r(r_j)}$ <p>Where;</p> <p><math>AR(a_i, r_j)</math> = Value at row <math>i</math> and column <math>j</math> of the binarized Agent x Resource matrix</p> <p><math>r_j \in \{r_0, r_1, r_2, \dots, r_M\}</math> (set of resource nodes)</p> <p><math>a_i, a_s \in \{a_0, a_1, a_2, \dots, a_N\}</math> (set of agent nodes)</p> <p><math>C_a(a_i)</math> = Composite risk attribute of the agent <math>a_i</math> as defined in equation (1.7)</p> <p><math>C_r(r_j)</math> = Standardised sensitivity/criticality of the information resource <math>r_j</math> as defined in equation (1.8)</p>

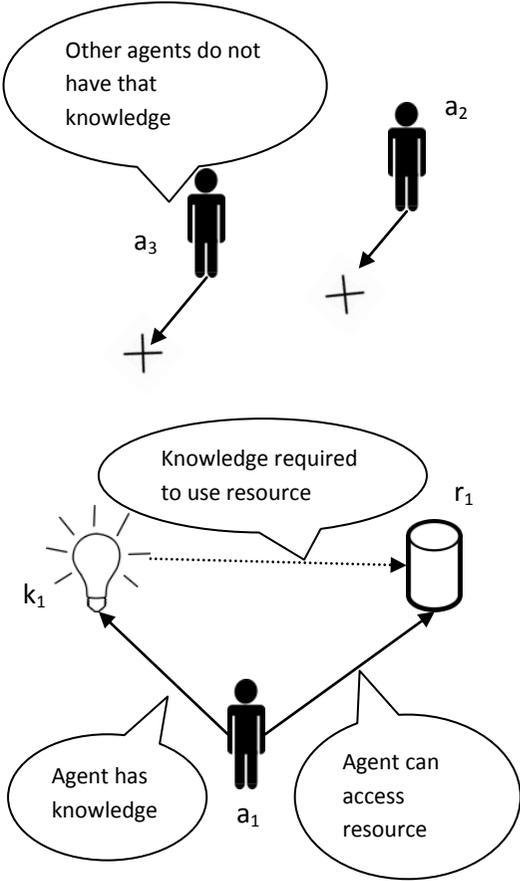
Risk type and metric	Description	Related metric in previous research	Formal definition of the metric
<p>Page 112</p> <p>5.3.2</p> <p>Employees having exclusive privileged (admin) access to information resources</p> <p>Metric: EAA</p>	 <p>The EAA metric is used to analyse and highlight instances where employees have exclusive privileged access to information resources.</p>	<p>Resource Exclusivity (RE) from (Carley et al. 2012) restated using the notation used in this chapter:</p> $RE = \sum_{j=0}^M AR(a_i, r_j) \cdot e^{1 - \sum_{s=0}^N AR(a_s, r_j)}$ <p>Where;</p> <p>RE=Resource exclusivity of agent <math>a_i</math></p> <p><math>AR(a_i, r_j)</math> = Value at row <math>i</math> and column <math>j</math> of the binarized Agent x Resource matrix</p> <p><math>r_j \in \{r_0, r_1, r_2, \dots, r_M\}</math> (set of resource nodes)</p> <p><math>a_i, a_s \in \{a_0, a_1, a_2, \dots, a_N\}</math> (set of agent nodes)</p> <p>Note:</p> <ul style="list-style-type: none"> <li>• This metric has only an agent centric definition</li> <li>• It does not incorporate agent risk values or resource criticalities</li> </ul>	<p>EAA(<math>r_j</math>) – Resource centric – equation</p> <p>Let any given element of the <math>AR_x</math> matrix defined as:</p> $\forall i \forall j: AR_x(a_i, r_j) = \lfloor AR(a_i, r_j) = x \rfloor$ <p>where <math>x</math> = link weight of administrative links. Then EAA(<math>r_j</math>) is defined as:</p> $EAA(r_j) = C_r(r_j) \cdot e^{1 - \sum_{i=0}^N \frac{1}{C_a(a_i)} \cdot AR_x(a_i, r_j)}$ <p>EAA(<math>a_i</math>) – Agent centric – equation (1.14)</p> <p>Let any given element of the <math>AR_x</math> matrix defined as:</p> $AR_x(a_i, r_j) = \lfloor AR(a_i, r_j) = x \rfloor$ <p>where <math>x</math> = link weight of administrative links. Then:</p> $EAA(a_i) = C_a(a_i) \cdot \frac{\sum_{j=0}^M AR_x(a_i, r_j) \cdot EAA(r_j)}{\sum_{j=0}^M C_r(r_j)}$ <p>EAA(<math>a_i, r_j</math>) – Resource access authorisation centric (per agent, resource pair) – equation (1.15)</p> <p>Let any given element of the <math>AR_x</math> matrix defined as:</p> $AR_x(a_i, r_j) = \lfloor AR(a_i, r_j) = x \rfloor$ <p>where <math>x</math> = link weight of administrative links. Then:</p> $EAA(a_i, r_j) = AR_x(a_i, r_j) \cdot C_a(a_i) \cdot EAA(r_j)$

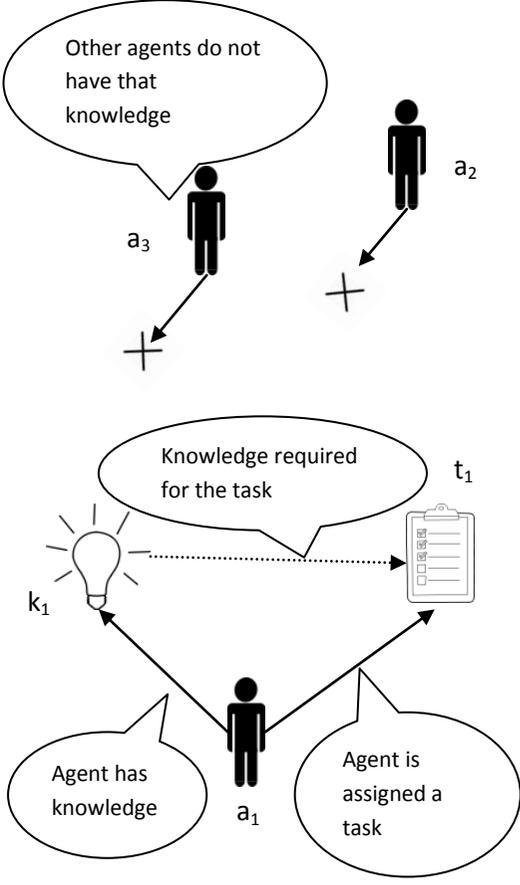
Risk type and metric	Description	Related metric in previous research	Formal definition of the metric
<p>Page 115</p> <p>5.3.3</p> <p>Employees have access to resources not required for their tasks</p> <p>Metric: VNA</p>	 <p>The VNA metric is used to analyse and highlight instances where an employee has access to resources not required for his assigned tasks.</p>	<p>Agent Resource Waste Congruence (AWRC) from (Carley et al. 2012) restated according to the notation used in this chapter</p> <p>Let <math>AR_T = AT \times TR</math></p> <p>then;</p> $ARWC = \frac{\sum_{j=0}^M AR(a_i, r_j) [AR_T(a_i, r_j) = 0]}{\sum_{j=0}^N AR(a_i, r_j)}$ <p>Note:</p> <ul style="list-style-type: none"> <li>• This metric has only an agent centric definition</li> <li>• It does not incorporate agent risk values or resource criticalities</li> </ul>	<p>VNA(<math>a_i</math>) – agent centric – equation (1.16)</p> <p>Let <math>AR_T</math> matrix be</p> <p><math>AR_T = AT \times TR</math> then;</p> $VNA(a_i) = C_a(a_i) \frac{\sum_{j=0}^M C_r(r_j).AR(a_i, r_j) [AR_T(a_i, r_j) = 0]}{\sum_{j=0}^M C_r(r_j).AR(a_i, r_j)}$ <p>VNA(<math>a_i, r_j</math>) - Resource access authorisation centric (per agent, resource pair) – equation (1.17)</p> <p>Let <math>AR_T</math> matrix be :</p> <p><math>AR_T = AT \times TR</math></p> <p>then;</p> $VNA(a_i, r_j) = C_a(a_i).C_r(r_j).AR(a_i, r_j) [AR_T(a_i, r_j) = 0]$ <p>Where, AT = Agent x Task matrix (binarized); TR = Task x Resource matrix (binarized); AR(<math>a_i, r_j</math>) = Value at row <math>i</math> and column <math>j</math> of the binarized Agent x Resource matrix; <math>a_i, a_s \in \{a_0, a_1, a_2, \dots, a_N\}</math> (set of agent nodes); <math>r_j \in \{r_0, r_1, r_2, \dots, r_M\}</math> (set of resource nodes); <math>C_a(a_i)</math> = Composite risk attribute of the agent <math>a_i</math>, as defined in equation (1.7); <math>C_r(r_j)</math> = Standardised sensitivity/criticality of the information resource <math>r_j</math> as defined in equation (1.8)</p>

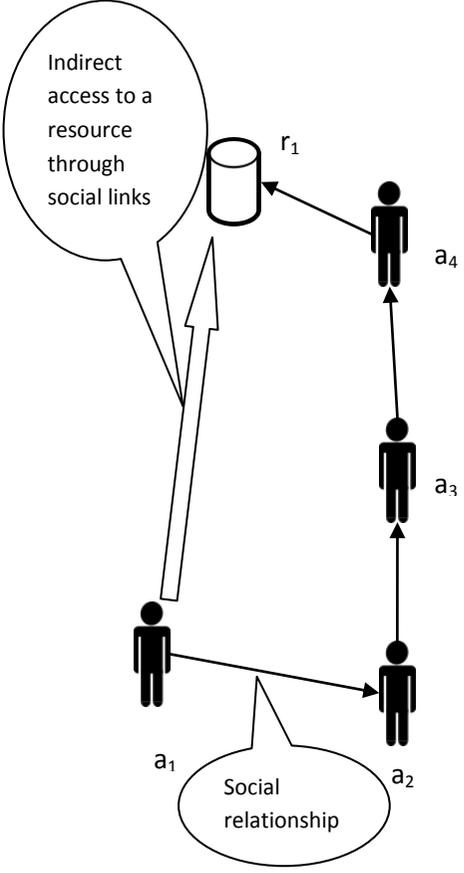
Risk type and metric	Description	Related metric in previous research	Formal definition of the metric
<p>Page 119</p> <p>5.3.4</p> <p>Employee has access to two dependent information resources</p> <p>Metric: ADR</p>	 <p>The ADR metric is used to analyse and highlight instances where people have access to dependent information resources creating a conflict of interest, opening opportunities to cause wider damage or providing means to conceal a breach.</p>	<p>None</p>	<p>ADR(a<sub>i</sub>)- Agent centric – equation (1.20)</p> <p>Let <math>\forall i \forall j : AR_w(a_i, r_j) = C_r(r_j). AR(a_i, r_j)</math></p> <p>and <math>AR_R = AR_w \times RR</math></p> <p>then;</p> $ADR(a_i) = C_a(a_i) \cdot \frac{\sum_{j=0}^M C_r(r_j). AR_R(a_i, r_j) [AR(a_i, r_j) > 0]}{\sum_{j=0}^M \sum_{k=0}^M C_r(r_j). C_r(r_k). RR(r_j, r_k)}$ <hr/> <p>ADR(a<sub>i</sub>,r<sub>j</sub>)- Resource access authorisation centric (per agent, resource pair) – equation (1.21)</p> <p>Let <math>\forall i \forall j : AR_w(a_i, r_j) = C_r(r_j). AR(a_i, r_j)</math></p> <p>and <math>AR_R = AR_w \times RR</math> then;</p> $ADR(a_i, r_j) = C_a(a_i). C_r(r_j) \cdot \frac{AR_R(a_i, r_j) [AR(a_i, r_j) > 0]}{\sum_{k=0}^M C_r(r_k). AR(a_i, r_k) [k \neq r]}$ <p>Where; AR(a<sub>i</sub>,r<sub>j</sub>) = Value at row <i>i</i> and column <i>j</i> of the binarized Agent x Resource matrix; a<sub>i</sub>,a<sub>s</sub> ∈ {a<sub>0</sub>, a<sub>1</sub>, a<sub>2</sub>,.....,a<sub>N</sub>} (set of agent nodes; r<sub>j</sub> ∈ {r<sub>0</sub>, r<sub>1</sub>, r<sub>2</sub>, ..... , r<sub>M</sub>} (set of resource nodes); C<sub>a</sub>(a<sub>i</sub>) = Composite risk attribute of the agent <i>a</i>, as defined in equation (1.7); C<sub>r</sub>(r<sub>j</sub>) = Standardised sensitivity/criticality of the information resource <i>r<sub>j</sub></i> as defined in equation (1.8)</p>

Risk type and metric	Description	Related metric in previous research	Formal definition of the metric
<p>Page 126</p> <p>5.4.1</p> <p>Employees exclusively assigned to tasks</p> <p>Metric: ETA</p>	 <p>The ETA metric is used to analyse instances where agents are assigned exclusively for tasks thereby creating opportunities for fraud, sabotage and theft of confidential information without being detected.</p>	<p>Task Exclusivity (TE) from (Carley et al. 2012) restated using the notation used in this chapter:</p> $TE = \sum_{p=0}^U AT(a_i, t_p) \cdot e^{1 - \sum_{s=0}^N AT(a_s, t_p)}$ <p>Where;</p> <p>TE = Task exclusivity of agent <math>a_i</math></p> <p><math>AT(a_i, t_p)</math> = Element at row <math>i</math> and column <math>p</math> of the binarized Agent x Task matrix</p> <p><math>t_p \in \{t_0, t_1, t_2, \dots, t_U\}</math> (set of resource nodes)</p> <p><math>a_i, a_s \in \{a_0, a_1, a_2, \dots, a_N\}</math> (set of agent nodes)</p> <p>Note:</p> <ul style="list-style-type: none"> <li>• This metric has only an agent centric definition</li> <li>• It does not incorporate agent risk values or task criticalities</li> </ul>	<p>ETA(<math>t_p</math>) – Task centric – equation (1.22)</p> $ETA(t_p) = C_t(t_p) \cdot e^{1 - \sum_{i=0}^N \frac{1}{C_a(a_i)} \cdot AT(a_i, t_p)}$ <p>ETA(<math>a_i</math>) – Agent centric – equation (1.23)</p> $ETA(a_i) = C_a(a_i) \cdot \frac{\sum_{p=0}^U AT(a_i, t_p) \cdot ETA(t_p)}{\sum_{p=0}^U C_t(t_p)}$ <p>ETA(<math>a_i, t_p</math>) – Task assignment centric (per agent, task pair) – equation (1.24)</p> $ETA(a_i, t_p) = AT(a_i, t_p) \cdot C_a(a_i) \cdot ETA(t_p)$ <p>Where,</p> <p><math>AT(a_i, t_p)</math> = Element at row <math>i</math> and column <math>p</math> of the binarized Agent x Task matrix; <math>t_p \in \{t_0, t_1, t_2, \dots, t_U\}</math> (set of resource nodes); <math>a_i, a_s \in \{a_0, a_1, a_2, \dots, a_N\}</math> (set of agent nodes); <math>C_a(a_i)</math> = Composite risk attribute of the agent <math>a_i</math> as defined in equation (1.7); <math>C_t(t_p)</math> = Standardised sensitivity/criticality of task <math>t_p</math> as defined in equation (1.9)</p>

Risk type and metric	Description	Related metric in previous research	Formal definition of the metric
<p>Page 130</p> <p>5.4.2</p> <p>Employee performs two dependent tasks</p> <p>Metric: ADT</p>	 <p>The ADT metric is used to analyse instances where a person is assigned to two dependent tasks thereby creating a conflict of interest</p>	<p>None</p>	<p>ADT(a<sub>i</sub>) – Agent centric – equation (1.27)</p> <p>Let <math>\forall i \forall p : AT_w(a_i, t_p) = C_t(t_p) \cdot AT(a_i, t_p)</math></p> <p>and <math>AT_T = AT_w \times TT</math> then;</p> $ADT(a_i) = C_a(a_i) \cdot \frac{\sum_{p=0}^U C_t(t_p) \cdot AT_T(a_i, t_p) [AT(a_i, t_p) > 0]}{\sum_{p=0}^U \sum_{k=0}^U C_t(t_p) \cdot C_t(t_k) \cdot TT(t_p, t_k)}$ <p>ADT(a<sub>i</sub>, t<sub>p</sub>) – Task assignment centric (per agent, task pair) – equation (1.28)</p> <p>Let <math>\forall i \forall p : AT_w(a_i, t_p) = C_t(t_p) \cdot AT(a_i, t_p)</math></p> <p>and <math>AT_T = AT_w \times TT</math></p> <p>then;</p> $ADT(a_i, t_p) = C_a(a_i) \cdot C_t(t_p) \cdot \frac{AT_T(a_i, t_p) [AT(a_i, t_p) > 0]}{\sum_{k=0}^U C_t(t_k) \cdot AT(a_i, t_k) [k \neq p]}$ <p>Where;</p> <p>AT(a<sub>i</sub>, t<sub>p</sub>)=Element at row <i>i</i> and column <i>p</i> of the binarized Agent x Task matrix</p> <p>t<sub>p</sub> ∈ {t<sub>0</sub>, t<sub>1</sub>, t<sub>2</sub>, …, t<sub>U</sub>} (set of resource nodes)</p> <p>a<sub>i</sub>, a<sub>s</sub> ∈ {a<sub>0</sub>, a<sub>1</sub>, a<sub>2</sub>, …, a<sub>N</sub>} (set of agent nodes)</p> <p>C<sub>a</sub>(a<sub>i</sub>) = Composite risk attribute of the agent a<sub>i</sub> as defined in equation (1.7)</p> <p>C<sub>t</sub>(t<sub>p</sub>) = Standardised sensitivity/criticality of task t<sub>p</sub> as defined in equation (1.9)</p>

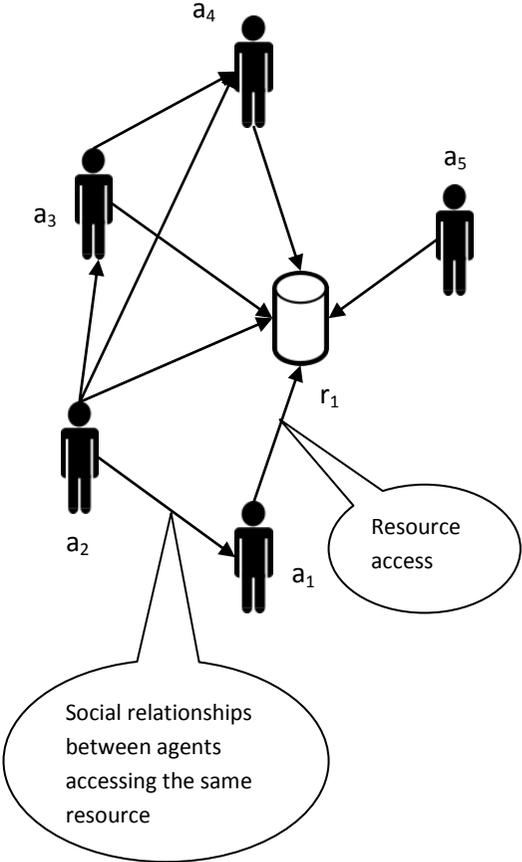
Risk type and metric	Description	Related metric in previous research	Formal definition of the metric
<p>Page 133</p> <p>5.5.1</p> <p>Employee has exclusive knowledge to operate an information resource</p> <p>Metric: EKR</p>	 <p>The EKR metric is used to analyse instances where agents have exclusive knowledge to operate a resource.</p>	<p>None.</p>	<p>EKR(a<sub>i</sub>) – Agent centric – equation (1.31)</p> <p>Let <math>AR_K = AK \times KR</math></p> <p>The total number of <math>a_s, k_q</math> pairs where agent <math>a_s</math> has knowledge <math>k_s</math> required to use resource <math>r_j</math> is given by: <math>\sum_{s=0}^N AT_K(a_s, t_p)</math></p> <p>Therefore, the proportion of knowledge possessed by agent <math>a_i</math> required for resource <math>r_j</math> out of all <math>a_s, k_q</math> pairs where agent <math>a_s</math> has knowledge <math>k_q</math> required to use resource <math>r_j</math>, denoted by <math>X(a_i, r_j)</math> is given by:</p> $X(a_i, r_j) = \frac{AR_K(a_i, r_j)}{\sum_{s=0}^N AR_K(a_s, r_j)} \left[ \sum_{s=0}^N AR_K(a_s, r_j) \neq 0 \right]$ <p>Then EKR(a<sub>i</sub>) can be defined as:</p> $EKR(a_i) = C_a(a_i) \cdot \frac{\sum_{j=0}^M AR(a_i, r_j) \cdot X(a_i, r_j) \cdot C_r(r_j)}{\sum_{j=0}^M C_r(r_j)}$ <p>EKR(a<sub>i</sub>, r<sub>j</sub>) – Resource authorisation centric (per agent, task pair) – equation (1.32)</p> $EKR(a_i, r_j) = AR(a_i, r_j) \cdot C_a(a_i) \cdot C_r(r_j) \cdot X(a_i, r_j)$ <p>Where; AK = Agent x Knowledge matrix; KR = Knowledge x Resource matrix; AR(a<sub>i</sub>, r<sub>j</sub>) = Value at row <math>i</math> and column <math>j</math> of the binarized Agent x Resource matrix; <math>a_i, a_s \in \{a_0, a_1, a_2, \dots, a_N\}</math> (set of agent nodes); <math>r_j \in \{r_0, r_1, r_2, \dots, r_M\}</math> (set of resource nodes) <math>C_a(a_i)</math> = Composite risk attribute of the agent <math>a_i</math> as defined in equation (1.7); <math>C_r(r_j)</math> = Standardised sensitivity/criticality of the information resource <math>r_j</math> as defined in equation (1.8)</p>

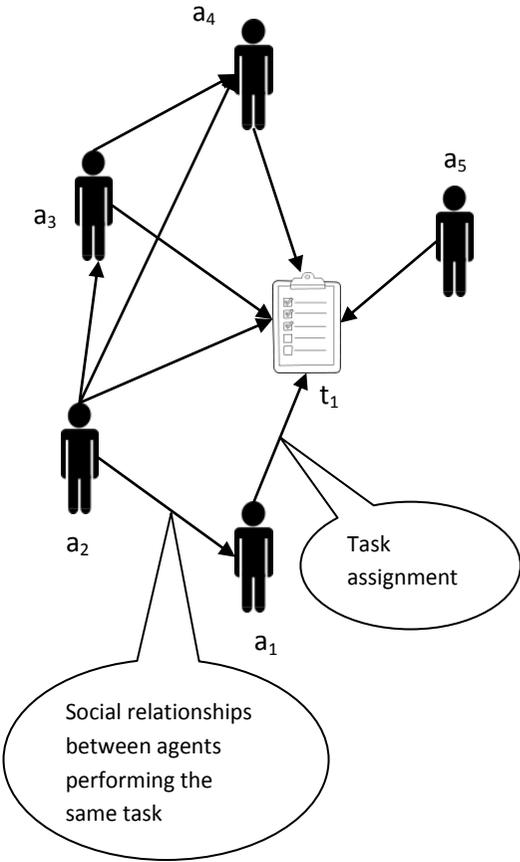
Risk type and metric	Description	Related metric in previous research	Formal definition of the metric
<p>Page 139</p> <p>5.5.2</p> <p>Employee having exclusive knowledge to perform a task</p> <p>Metric: EKT</p>	 <p>EKT metric is used to analyse instances where agents have exclusive knowledge to perform a task</p>	<p>None.</p>	<p>EKT(a<sub>i</sub>) – Agent centric – equation (1.35)</p> <p>Let <math>AT_K = AK \times KT</math></p> <p>The number of a<sub>s</sub>,k<sub>q</sub> pairs where agent a<sub>s</sub> has knowledge k<sub>q</sub> required to perform task t<sub>p</sub> is given by: <math>\sum_{a=a_0}^{a_N} AT_K^{(a,t)}</math></p> <p>Therefore, the proportion of knowledge possessed by agent a<sub>i</sub> required to perform task t<sub>p</sub> out of all a<sub>s</sub>,k<sub>q</sub> pairs where agent a<sub>s</sub> has knowledge k<sub>q</sub> required to perform task t<sub>p</sub>, denoted by Y(a<sub>i</sub>,t<sub>p</sub>) is given by:</p> $Y(a_i, t_p) = \frac{AT_K(a_i, t_p)}{\sum_{s=0}^N AT_K(a_s, t_p)} \left[ \sum_{s=0}^N AT_K(a_s, t_p) \neq 0 \right]$ <p>Then EKT(a<sub>i</sub>) can be defined as:</p> $EKT(a_i) = C_a(a_i) \cdot \frac{\sum_{p=0}^U AT(a_i, t_p) \cdot Y(a_i, t_p) \cdot C_t(t_p)}{\sum_{p=0}^U C_t(t_p)}$ <p>EKT(a<sub>i</sub>,t<sub>p</sub>) – Resource authorisation centric (per agent, task pair) – equation (1.36)</p> $EKT(a_i, t_p) = AT(a_i, t_p) \cdot C_a(a_i) \cdot C_t(t_p) \cdot Y(a_i, t_p)$ <p>Where; K = Agent x Knowledge matrix; KT = Knowledge x Task matrix; AT(a<sub>i</sub>,t<sub>p</sub>)=Element at row i and column p of the binarized Agent x Task matrix; t<sub>p</sub> ∈ {t<sub>0</sub>, t<sub>1</sub>, t<sub>2</sub>, …, t<sub>U</sub>} (set of resource nodes); a<sub>i</sub>, a<sub>s</sub> ∈ {a<sub>0</sub>, a<sub>1</sub>, a<sub>2</sub>, …, a<sub>N</sub>} (set of agent nodes); C<sub>a</sub>(a<sub>i</sub>) = Composite risk attribute of the agent a<sub>i</sub> as defined in equation (1.7); C<sub>t</sub>(t<sub>p</sub>) = Standardised sensitivity/criticality of task t<sub>p</sub> as defined in equation (1.9)</p>

Risk type and metric	Description	Related metric in previous research	Formal definition of the metric
<p>Page 142</p> <p>5.6.1</p> <p>An employee has indirect access to information through social connections</p> <p>Metric: IAC</p>	 <p>Metric is used to measure the likelihood of an agent obtaining indirect access to resources via social links</p>	<p>No metrics defined for the same purpose in research literature. There is one similarity between Freeman’s (1978) closeness centrality measure and IAC since both are based on geodesic path lengths.</p> <p>If the number of nodes linking two nodes <math>a_i</math> and <math>a_s</math> along geodesic is given by <math>d(a_i, a_s)</math> then the closeness centrality of <math>a_i</math> is given by:</p> $\frac{N - 1}{\sum_{s=1}^N d(a_i, a_s)}$ <p>Where,  <math>N</math> = number of nodes in network  <math>a_i, a_s \in \{a_1, a_2, \dots, a_N\}</math> set of nodes in the network</p>	<p><math>IAC(a_i, r_j)</math>– Metric calculated per agent, resource pair – equation (1.39)</p> <p>Let <math>p_x</math> be one of the many possible shortest paths for agent <math>a_i</math> to access information resource <math>r_j</math> through the social network</p> $p_x = \{a_i, a_1, a_2, \dots, a_n, r_j\}$ <p>If the shortest path length for <math>a_i</math> to access <math>r_j</math> is <math>L(a_i, r_j)</math>, then the average risk attribute value of all agents (including the source agent <math>a_i</math>) involved in path <math>p_x</math>, denoted by <math>C_A(p_x)</math> is given by:</p> $C_A(p_x) = \frac{C_a(a_i) + C_a(a_1) + C_a(a_2) + \dots + C_a(a_n)}{L(a_i, r_j)}$ <p>Therefore, the indirect access capability for agent <math>a_i</math> to access resource <math>r_j</math> via a specific shortest path <math>p_x</math> is given by:</p> $\frac{C_A(p_x)}{L(a_i, r_j)}$ <p>Assuming that there are <math>W</math> shortest paths between <math>a_i</math> and <math>r_j</math> the indirect access capability of <math>a_i</math> with respect to resource <math>r_j</math> is given by:</p> $IAC(a_i, r_j) = \frac{C_r(r_j)}{W \cdot L(a_i, r_j)} \sum_{x=1}^W C_A(p_x)$ <p><math>IAC(a_i)</math> – Agent centric – equation (1.40)</p> $IAC(a_i) = \frac{1}{M} \sum_{j=1}^M IAC(a_i, r_j)$ <p>Where;  <math>a_i \in \{a_0, a_1, a_2, \dots, a_N\}</math> (set of agent nodes of the network); <math>r_j \in \{r_0, r_1, r_2, \dots, r_M\}</math> (set of resource nodes); <math>C_a(a_i)</math> = Composite risk attribute for agent <math>a_i</math> as defined in equation (1.7); <math>C_r(r_j)</math> = Standardised sensitivity/criticality of information resource <math>r_j</math> as defined in equation (1.8); <math>L(a_i, r_j)</math> = length of the shortest path from <math>a_i</math> to <math>r_j</math>; <math>W</math> = number of shortest paths of equal length</p>

Risk type and metric	Description	Related metric in previous research	Formal definition of the metric
<p>Page 148</p> <p>5.6.2</p> <p>An employee have transitive access to dependent information resources</p> <p>Metric: TAR</p>		<p>None</p>	<p>The TAR metric calculates the likelihood of an agent having direct access to one resource obtaining indirect access to a second dependent resource through his social links</p> <p><math>TAR(a_i, r_j)</math> – Metric calculated per agent, resource pair – equation (1.45)</p> <p>Let Agent x Resource (resource access) matrix weighted according to resource sensitivities (<math>C_r(r_j)</math>), denoted by <math>AR_w</math>, be defined as:</p> $\forall i \forall j : AR_w(a_i, r_j) = C_r(r_j) \cdot AR(a_i, r_j)$ <p>Then let,</p> $AR_R = AR_w \times RR$ <p>Each element (<math>a_i, r_j</math>) of the <math>AR_R</math> matrix corresponds to number of resources accessible by agent <math>a_i</math> which <math>r_j</math> depends on. Similarly, let Agent x Agent matrix (social network) weighted according to the risk attribute values of the agent receiving the tie (<math>C_a(a_s)</math>), denoted by <math>AA_s</math>, defined as:</p> $\forall i \forall s : AA_s = C_a(a_s) \cdot AA(a_i, a_s)$ <p>Then let,</p> $AR_A = AA_s \times AR$ <p>Each element (<math>a_i, r_j</math>) of the <math>AR_A</math> matrix corresponds to the weighted number of associates of agent <math>a_i</math> through which <math>a_i</math> can access <math>r_j</math>. Then <math>TAR(a_i, r_j)</math> can be defined as:</p> $TAR(a_i, r_j) = C_a(a_i) \cdot C_r(r_j) \cdot \frac{AR_R(a_i, r_j) \cdot AR_A(a_i, r_j) [AR(a_i, r_j) = 0]}{\left( \sum_{k=1}^M C_r(r_k) [k \neq j] \right) \left( \sum_{s=1}^N C_a(a_s) [s \neq i] \right)}$ <p><math>TAR(a_i)</math> – Agent centric – equation (1.46)</p> $TAR(a_i) = \frac{1}{M} \sum_{j=1}^M TAR(a_i, r_j)$

Risk type and metric	Description	Related metric in previous research	Formal definition of the metric
<p>Page 153</p> <p>5.6.3</p> <p>An employee obtains transitive access to dependent tasks</p> <p>Metric: TAT</p>	<p>The diagram illustrates the Transitive Assignment of Task (TAT) metric. It shows two agents, <math>a_1</math> and <math>a_2</math>, and two tasks, <math>t_1</math> and <math>t_2</math>. Agent <math>a_1</math> is directly assigned task <math>t_1</math>. Agent <math>a_2</math> is socially related to agent <math>a_1</math>. Task <math>t_2</math> is dependent on task <math>t_1</math>. The diagram shows a direct assignment of task <math>t_1</math> to agent <math>a_1</math>, a social relationship between <math>a_1</math> and <math>a_2</math>, and a task dependency from <math>t_1</math> to <math>t_2</math>. A transitive assignment of task <math>t_2</math> is shown to agent <math>a_1</math> through the social link and task dependency.</p>	<p>None</p>	<p>The TAT metric calculates the likelihood of an agent having direct assignment of one task obtaining indirect assignment to a second dependent task through his social links</p> <p><math>TAT(a_i, t_p)</math> – metric calculated per agent, task pair – equation (1.51)</p> <p>Let Agent x Task (task assignment) matrix weighted according to task criticalities (<math>C_i(t_p)</math>), denoted by <math>AT_w</math>, be defined as:</p> $\forall i \forall p : AT_w = C_i(t_p) \cdot AT(a_i, t_p)$ <p>Then let,</p> $AT_T = AT_w \times TT$ <p>Each element (<math>a_i, t_p</math>) of the <math>AT_T</math> matrix corresponds to number of tasks performed by agent <math>a_i</math> which <math>t_p</math> depends on. Similarly, let Agent x Agent matrix (social network) weighted according to the risk attribute values of the agents receiving the tie (<math>C_a(a_s)</math>), denoted by <math>AA_s</math>, defined as:</p> $\forall i \forall s : AA_s = C_a(a_s) \cdot AA(a_i, a_s)$ <p>Then let,</p> $AT_A = AA_s \times AT$ <p>Each element (<math>a_i, t_p</math>) of the <math>AT_A</math> matrix corresponds to the weighted number of associates of agent <math>a_i</math> performing the task <math>t_p</math>. Then <math>TAT(a_i, t_p)</math> can be defined as:</p> $TAT(a_i, t_p) = C_a(a_i) \cdot C_i(t_p) \frac{AT_T(a_i, t_p) \cdot AT_A(a_i, t_p) [AT(a_i, t_p) = 0]}{\left( \sum_{q=1}^U C_i(t_q) [q \neq p] \right) \left( \sum_{s=1}^N C_a(a_s) [s \neq i] \right)}$ <p><math>TAT(a_i)</math> – Agent centric – equation (1.52)</p> $TAT(a_i) = \frac{1}{U} \sum_{p=1}^U TAT(a_i, t_p)$

Risk type and metric	Description	Related metric in previous research	Formal definition of the metric
<p>Page 156</p> <p>5.6.4</p> <p>A closely associated group of employees control a resource</p> <p>Metric: ACR</p>		<p>Clustering coefficient (Watts and Strogatz 1998) is a metric defined for single mode networks. If there is a node <math>n</math>, which has <math>N</math> neighbours and there are <math>C_n</math> edges between the nodes in the neighbourhood clustering coefficient <math>C</math> is defined as:</p> $C = \frac{2.C_n}{N(N-1)}$	<p>The ACR metric calculates the extent to which the agents accessing a resource are associated with each other.</p> <p>ACR(<math>r_j</math>) – Resource centric – equation (1.53)</p> <p>Assume that a given resource <math>r_j</math> in the Agent x Resource network is accessed by the subset of agents denoted by <math>A_r = \{a_1, a_2, a_3, \dots, a_N\}</math>. Then let the sub-graph of the Agent x Agent (social) network consisting of the same nodes in <math>A_r</math> be <math>AA_S</math>.</p> <p>Then, Agent Clustering for Resource (ACR(<math>r_j</math>)) metric is defined as:</p> $ACR(r_j) = \frac{2.C_r(r_j) \sum_{i=1}^N \sum_{s=1}^N AA_S(a_i, a_s).C_a(a_i).C_a(a_s)}{N(N-1)} \quad [N > 1]$ <p>Where;</p> <p><math>N</math> = the number of agents in the subset <math>A_r</math>  <math>C_a(a_s)</math> and <math>C_a(a_i)</math> = the composite risk attributes of the agents <math>a_s</math> and <math>a_i</math> defined in the equation (1.7)  <math>C_r(r_j)</math> = Standardised sensitivity/criticality of the resource <math>r_j</math> defined in equation (1.8)  <math>a_i, a_s \in \{a_1, a_2, a_3, \dots\}</math> is a set of agent nodes of the organisation</p>

Risk type and metric	Description	Related metric in previous research	Formal definition of the metric
<p>Page 158</p> <p>5.6.5</p> <p>A closely associated group of employees perform a task</p> <p>Metric: ACT</p>		<p>Clustering coefficient (Watts and Strogatz 1998) is a metric defined for single mode networks. If there is a node <math>n</math>, which has <math>N</math> neighbours and there are <math>C_n</math> edges between the nodes in the neighbourhood clustering coefficient <math>C</math> is defined as:</p> $C = \frac{2.C_n}{N(N-1)}$	<p>The ACT metric calculates the extent to which the agents assigned to a task are associated with each other</p> <p>ACT(<math>t_p</math>) – Task centric – equation (1.54)</p> <p>Assume that a given task <math>t_p</math> in the Agent x Task network is performed by the subset of agents denoted by <math>A_t = \{a_1, a_2, a_3, \dots, a_N\}</math>. Then let the sub-graph of the Agent x Agent (social) network consisting of the same nodes in <math>A_t</math> be <math>AA_S</math>.</p> <p>Then, Agent Clustering for Task (ACT(<math>t_p</math>)) metric is defined as:</p> $ACT(t_p) = \frac{2.C_t(t_p) \sum_{i=1}^N \sum_{s=1}^N AA_S.C_a(a_i).C_a(a_s)}{N(N-1)} [N > 1]$ <p>Where,</p> <p><math>N</math> = the number of agents in the subset <math>A_t</math></p> <p><math>C_a(a_i)</math> and <math>C_a(a_s)</math> = composite risk attributes of the agents <math>a_i</math> and <math>a_s</math> defined in the equation (1.7)</p> <p><math>C_t(t_p)</math> = Standardised criticality of the task <math>t</math> defined in equation (1.8)</p> <p><math>a_i, a_s \in \{a_1, a_2, a_3, \dots\}</math> is a set of agent nodes of the organisation</p>

## 5.8 Risk Assessment Method

In addition to the model representing important socio-technical interactions and the risk assessment metrics, the third component (artefact) of the methodology is the risk assessment method (workflow) to be followed by the analysts (security professionals). Some activities in the analysis method followed in this research are different from the ones prescribed for the security professionals since the research involved analysing common types of insider threats and defining a suitable model and metrics. However, security professionals need not go through all these steps since they can utilise the proposed model and the metrics. Figure 5-16 compares the risk assessment activities carried out in the research and the analysis method recommended for the security professionals.

### 5.8.1 Risk assessment activities carried out in the research

The risk assessment activities unique to this research are grouped inside the green box at the top-right corner. The last three steps inside the pink box at the bottom of the diagram are activities that are common to both the research and the analysis method prescribed for the security professionals. The activities shown in the diagram directly correspond to the ones given in Table 3-3 under the research methodology (Chapter 3) as shown in Table 5-9.

Table 5-9: Equivalent activities in the research methodology to the activities in Figure 5-16

Activity in Figure 5-16	Equivalent activity in the research methodology (Table 3-3)
R1 and R2 combined	<i>Activity 1: List and categorise details of insider threat events</i>
R3 and R4 combined	Combination of <i>Activity 2: Initial theory building</i> and <i>Activity 3: Develop an initial methodology</i> (first iteration of artefact development) and Combination of <i>Activity 5: Reform theory</i> and <i>Activity 6: Enhance model and metrics</i> (second iteration of artefact development)
R5/A5 and R6/A6 combined	Combination of <i>Activity 4: Evaluate initial artefacts</i> (first, formative evaluation) and <i>Activity 7: Evaluate artefacts</i> (final evaluation)
R7/A7	Combination of <i>Activity 7: Evaluate artefacts</i> and <i>Activity 8: Finalise and report theoretical contributions</i>

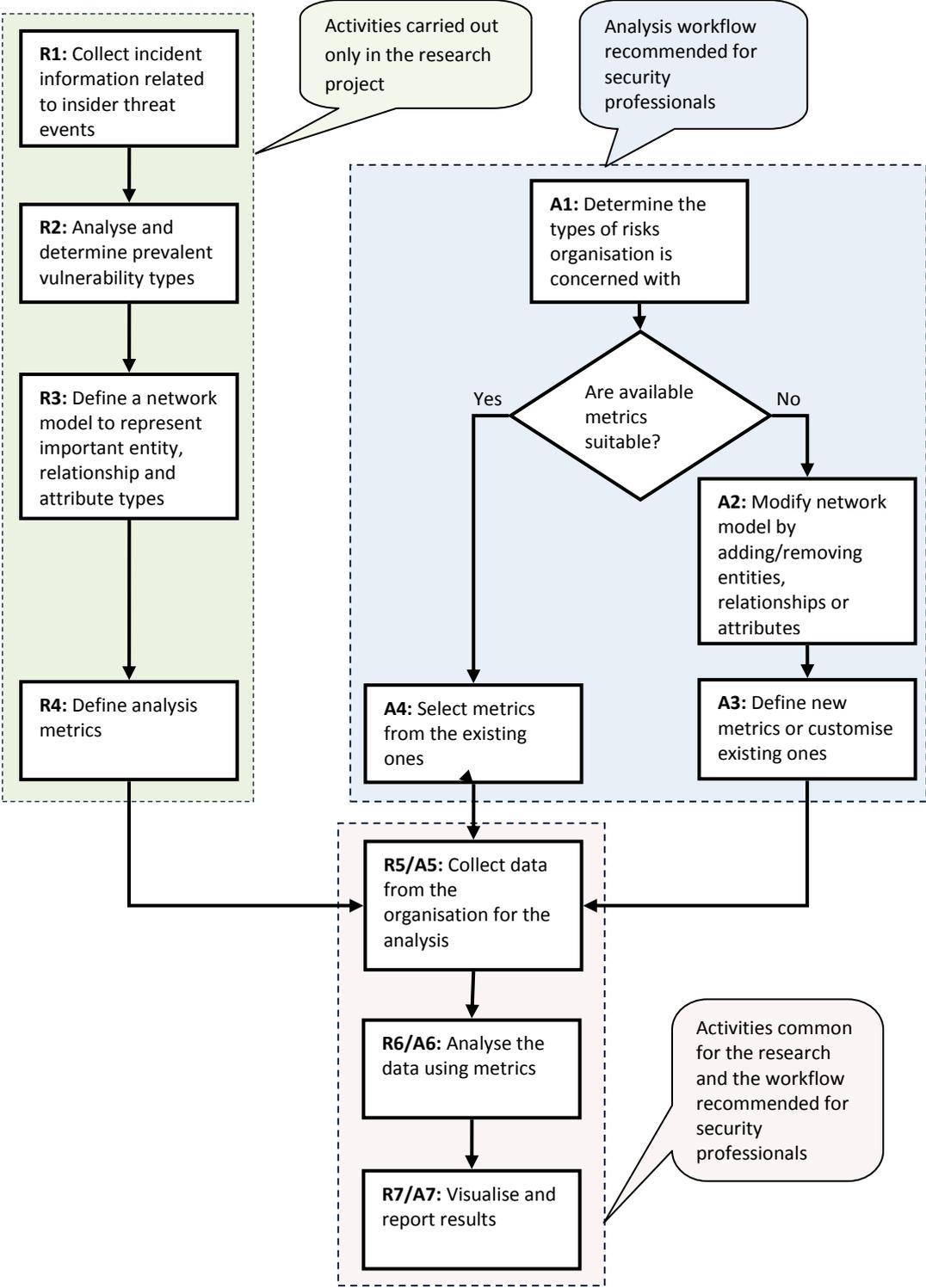


Figure 5-16: The risk assessment activities followed in the research and the assessment method recommended for information security professionals

### 5.8.2 Risk assessment method recommended for the security professionals

The first activity that should be carried out by the security professionals is to analyse and understand the risk landscape they are concerned about (Activity A1). They need to find what types of risks they should be concerned about and what type of vulnerabilities cause them. There can be many ways to carry out this task and several possibilities are suggested below:

- If the organisation has experienced past insider threat events, by analysing the incident reports.
- By analysing known incident reports from other similar organisations or ones shared by incident response teams.
- By having a brainstorming session with the participation of key personnel.

Then, the security professionals need to decide whether the identified types of risks can be analysed using the metrics presented in this research. They also need to make sure that the data required for the metrics can be collected from the organisation. If the answers to the above questions are yes, they can proceed with the available metrics (Activity A4). Else, they might need to make changes to the model in terms of adding or removing specific entity types, relationship types or attributes (Activity A2) and redefine or modify relevant metrics (Activity A3). Once the metrics are finalised, analysts need to collect the necessary data from their organisation (Activity R5/A5). Then, the analysis can be carried out using the software tools developed in this research (Activity R6/A6). However, if the analysts have made changes to the metrics they will need to recode some of the software. Finally, the results obtained can be reported to the decision makers using visualisations such as network diagrams, graphs and heat-maps (Activity R7/A7). Available network and statistical visualisation tools can be used for this purpose.

## 5.9 Chapter Summary

The primary objective of Chapter 5 is to describe the risk assessment model, metrics and method developed in this research. First, this chapter presented an access risk classification based on the socio-technical vulnerabilities that cause the risks. Then, a model that incorporate important entity and relationship types for information systems access risk assessments has been presented followed by thirteen metrics that use the model to quantify risks. The ability of the metrics to incorporate both likelihood and impact criteria,

as per the definition of information systems security risk, has also been demonstrated in this chapter. Finally, the chapter presents a method to be followed by the analysts in order to assess information systems access security risks in a socio-technical perspective.

Since this research adopts a design science paradigm, as discussed in Chapter 3, it is important to evaluate the risk assessment model, metrics and method using real data collected from organisations. The next chapter presents results of three risk analysis case studies carried out using data collected from organisations.

## 6. Assessment and Visualisation of Risks

This chapter presents the results of the assessment of information systems access risks of the three organisations described in Chapter 4. The risk assessment has been carried out using the model and metrics described in Chapter 5. Figure 6-1 presents the progression of the topics in this chapter. First, the chapter gives a brief overview of the analysis workflow and the software tools used. Next four subtopics present the results of the security risk assessment carried out using the metrics described in Chapter 5. Final sub-topic of the chapter provides a discussion of the results obtained.

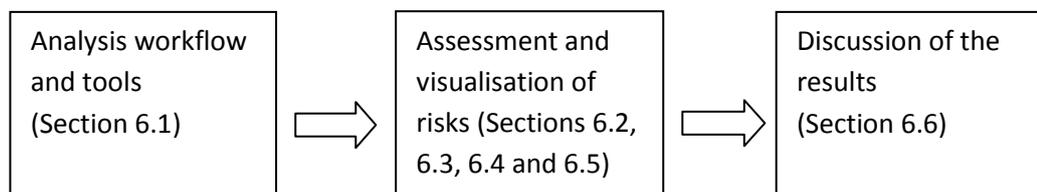


Figure 6-1: Arrangement of chapter sub-topics

### 6.1 Analysis workflow and tools used

All the data collected from the three organisations described in Chapter 4 were entered in to Microsoft Excel Worksheets and converted to comma separated value (.csv) files. Since the existing network analysis tools do not provide the ability to define new metrics, Python programming language was used to code the metrics described in Chapter 5. Python library NetworkX (Hagberg et al. 2008) has been used to instantiate and manipulate networks. In order to code the metrics Python libraries Scipy and Numpy (Jones et al. 2001) were utilised. Researcher will provide all Python source code used for the metric calculations to the interested readers upon request. Once the metrics had been calculated results were visualised using a range of tools. All the bar charts presented in this chapter were plotted using Microsoft Excel while the statistical software package R (R-core-team 2013) was used to create the heat-maps. Network visualisations presented in this chapter were obtained using the Microsoft Excel Template – NodeXL (Smith et al. 2010). The next four sections of this chapter (sections 6.2, 6.3, 6.4 and 6.5) present the risk values obtained by using the metrics defined in Chapter 5. The risk values are also illustrated using visual representations such as bar charts, heat-maps and network diagrams. The primary utility of the bar charts and heat-maps is to highlight the agents and relationships causing high risks. Additionally, network representations enable the visualisation of structural features of networks that cause high risk scores.

## 6.2 Assessment of risks due to resource access authorisations

Four types of security risks that occur due to resource access authorisations have been identified in this research and listed in Table 5-4 in Chapter 5. The next four subtopics present the results of the assessment of access security risks occurring due to resource access authorisations in the three organisations introduced in Chapter 4.

### 6.2.1 Risks due to agents having exclusive access to resources

Agents having exclusive access to information resources provide them the ability to commit sabotage, theft of information and fraud with minimum chance of being detected. The overall risk of exclusive access is calculated using the ERA metrics described in Chapter 5 by combining three factors - the extent to which agents have exclusive access to resources, the sensitivity or criticality of the resources and intrinsic risk properties of the agents. The ERA metric can be calculated per resource -  $ERA(r_j)$ , per agent -  $ERA(a_i)$  and per resource access authorisation -  $ERA(a_i, r_j)$ . Figure 6-2 presents  $ERA(r_j)$  values of the top-five resources in each organisation in terms of the metric score (refer equation (1.10) in page 108 for the definition of this metric).

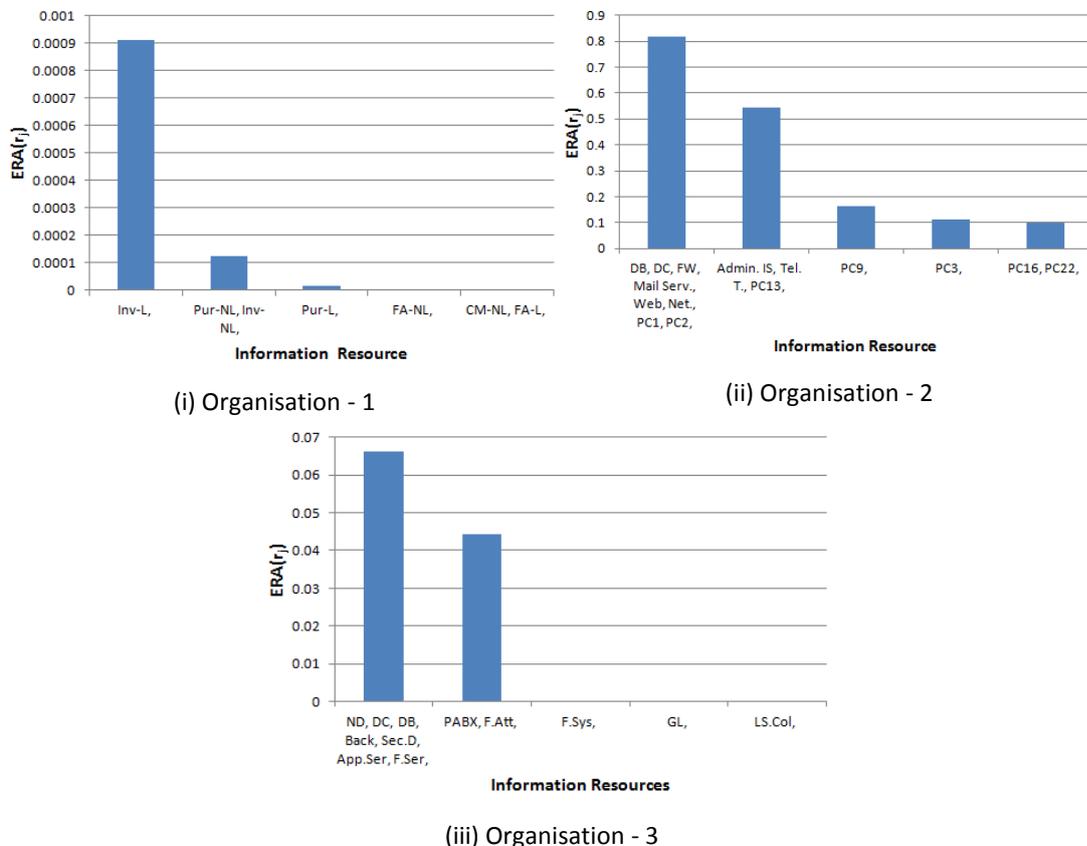


Figure 6-2: Information resources that score top-five  $ERA(r_j)$  values in Organisations 1,2 and 3

In all three organisations, only a small fraction of information resources can be clearly distinguished as having comparatively high  $ERA(r_j)$  scores. Higher risk scores are obtained by the resources in Organisation – 2, in comparison to the resources of the other two organisations, as evident from the metric scales used in the three graphs in Figure 6-2. In Organisation -2, resources - *DB, DC, FW, Mail Serv., Web, Net., PC1*, and *PC2* receive the highest  $ERA(r_j)$  metric score. All these information resources, except for *PC1* and *PC2*, are either servers or network devices. The same trend occurs in Organisation -3, where the resources that receive the highest metric score (*ND, DC, DB, Back, Sec.D, App.Ser* and *F.Ser*) are either servers or network devices. This suggests that major exclusive access risks are associated with critical hardware components of the IT infrastructure of the two organisations. This trend is not visible for Organisation – 1 since the hardware systems such as network devices and servers were not included in data collected from this company. In Organisation-1, the ERP module *Inv-L* scores the highest exclusive access risk value. Relative to the other two organisations, the exclusive access risk values of the resources of Organisation – 1 are significantly lower. This also illustrates the sensitivity of the metric to the number of agents accessing a resource. The metric value decreases exponentially with the each additional agent who has access to the resource concerned.

Looking from another perspective, agents contributing to high exclusive access risks can be identified using the  $ERA(a_i)$  metric (refer equation (1.11) in page 109 for the definition of this metric). Figure 6-3 illustrates the  $ERA(a_i)$  values of the agents who receive top-five metric scores in each of the three organisations.

Similar to the resources, only a few agents in each organisation obtain high  $ERA(a_i)$  values while all others have relatively low metric scores. In Organisation -2, employee labelled *Emp 2* receives the highest score while in Organisation – 3, two employees labelled *IT. Adm* and *M.IT* score the highest values. All three agents are IT administrators or managers in the respective organisations. Since IT Administrators of Organisation – 1 were not included in the data collection this pattern is not visible in the metric scores of that company. Furthermore, the highest  $ERA(a_i)$  risk value obtained by an agent in Organisation – 1 is significantly less than that of the other two organisations. In Organisation-1, four agents labelled – *SM.F&P, A.M, ACC* and *FA1* score the highest  $ERA(a_i)$  metric values. The first three agents in the above list occupy senior to mid-level management positions of the company.

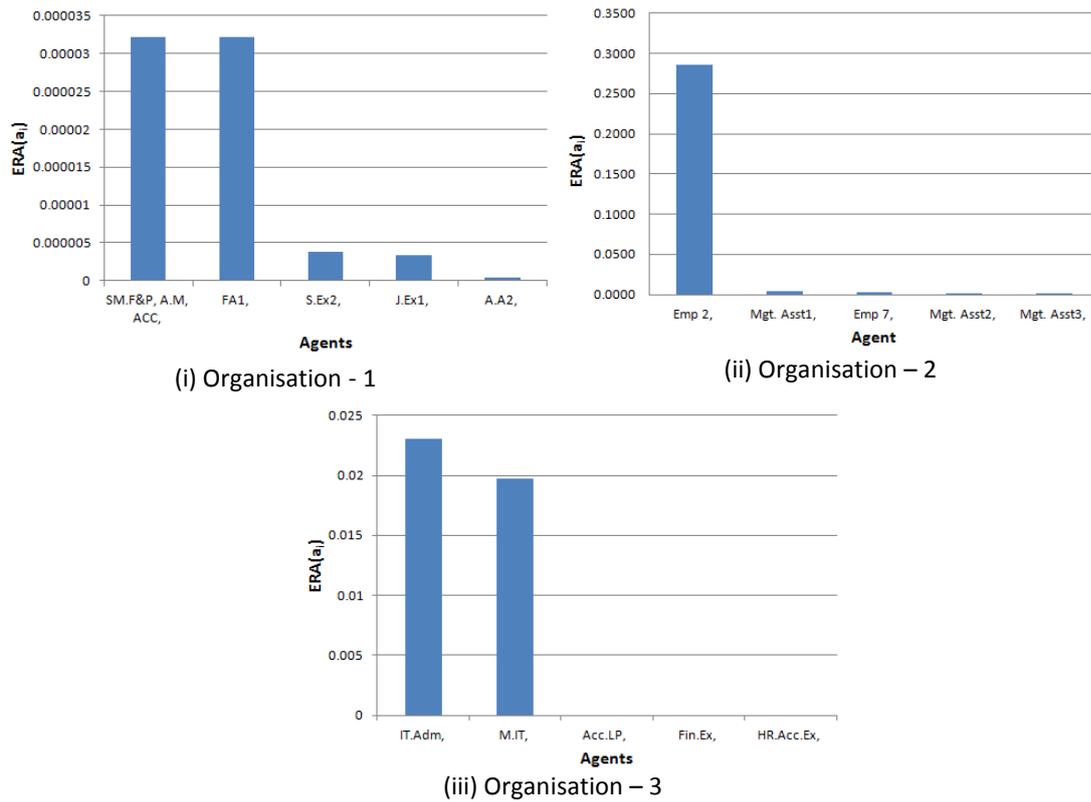
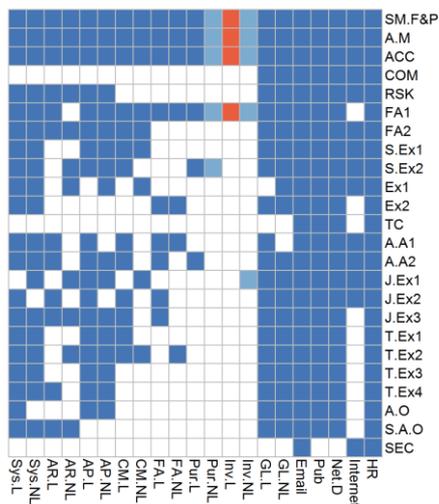


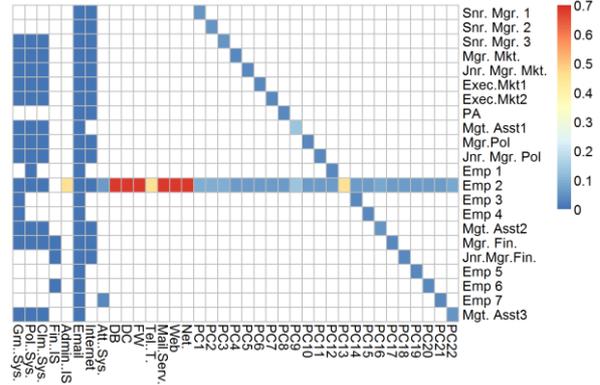
Figure 6-3: Agents who score top-five ERA(a<sub>i</sub>) values of organisations 1,2 and 3

In addition to identifying agents and resources that contribute to higher exclusive access risks, further analysis can be carried out using the ERA(a<sub>i</sub>,r<sub>j</sub>) metric (refer equation (1.12) in page 111 for the definition of this metric) by using it to find the access authorisations that cause the greatest risks. Figure 6-4 depicts heat-map representations of ERA(a<sub>i</sub>,r<sub>j</sub>) values for all agent resource combinations of the three organisations. Rows of the heat-maps represent agents while columns represent information resources. Cell colours represent the ERA(a<sub>i</sub>,r<sub>j</sub>) risk score of the access authorisations where the highest risks in each organisation are indicated by red and lowest risks are indicated by dark blue (refer the legends of the heat-maps for numerical comparisons). White cells indicate that there is no access authorisation for the corresponding agent, resource pair.

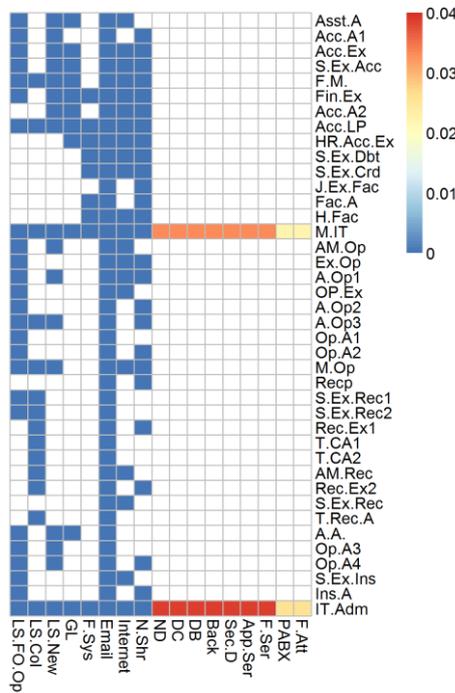
The same information is depicted as resource access networks of three organisations in Figure 6-5. In the figure, blue spheres represent agents while triangles represent information resources. Links represent resource access authorisations. Link width and colour correspond to the ERA(a<sub>i</sub>,r<sub>j</sub>) metric scores, where thicker and darker links represent larger risks. Nodes have been sized proportionately to the highest ERA(a<sub>i</sub>,r<sub>j</sub>) score they are associated with. The information resources that are accessed by many agents (which results in very low exclusive access risks) are clustered toward the centre of the networks and are demarcated by circles drawn around them.



(i) Organisation – 1



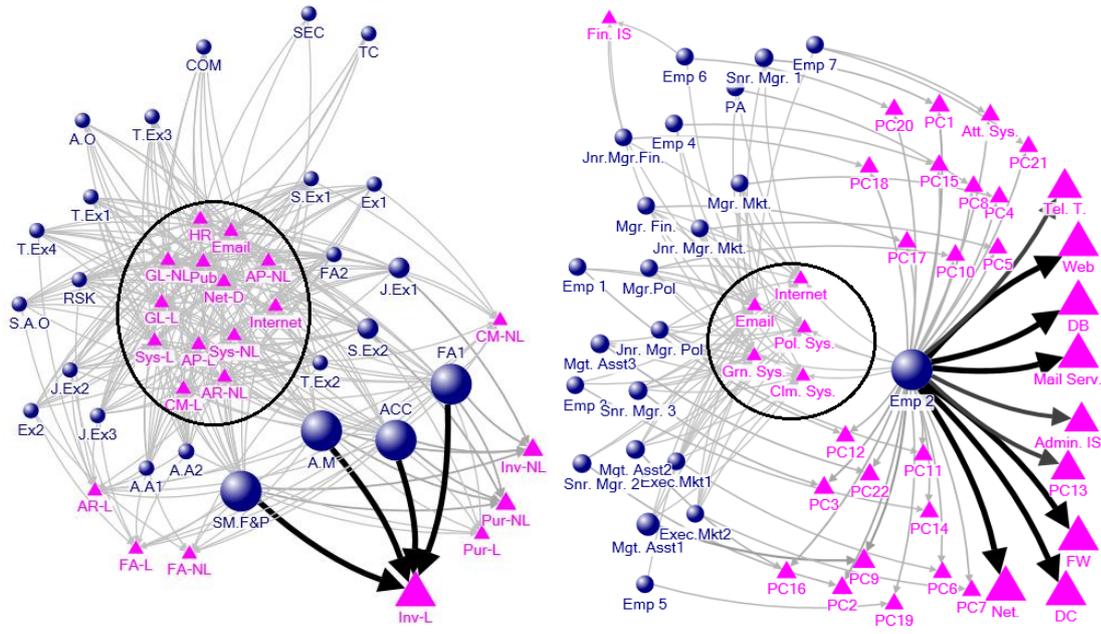
(ii) Organisation – 2



(iii) Organisation - 3

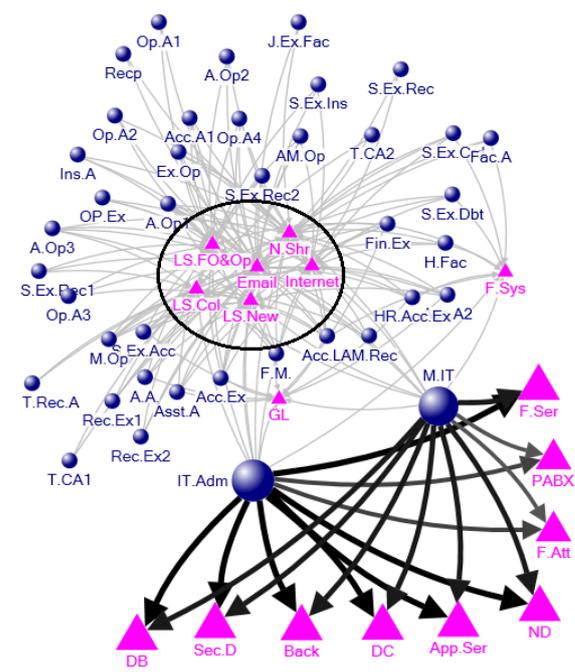
Figure 6-4: Heat-map representations of the exclusive access risks per resource access authorisation of the three organisations. Rows represent agents while columns represent information resources. Cell colours represent the ERA(ai,rj) risk score of the access authorisations where the highest risks are indicated by red and lowest risks are indicated by dark blue (refer the legend of each heat-map for a numerical comparison). (Note that the scales differ for each organisation and the colours cannot be used to compare risks across organisations). White cells indicate that there is no access authorisation for the corresponding agent, resource pair

In all three organisations most of the resource access authorisations have low exclusive access risks as indicated by the numerous dark blue cells in the heat-maps in Figure 6-4 although a few authorisations receive comparatively high scores.



(i) Organisation - 1

(ii) Organisation - 2



(iii) Organisation - 3

Legend: ● Agent ▲ Resource

Figure 6-5: Resource access networks of the three organisations. Blue spheres represent agents while triangles represent information resources. Links represent resource access authorisations. Link width and colour correspond to the  $ERA(a_i, r_j)$  metric scores where thicker and darker links represent larger metric values. Nodes have been sized proportionately to the highest  $ERA(a_i, r_j)$  score they are associated with. The resource clusters in the middle of the networks, demarcated by circles, have low exclusive access risk scores.

As illustrated in Figure 6-4 (i), there are four resource access authorisations that carry the highest exclusive access risk (indicated by red cells) and all four correspond to the *Inv.L* ERP module used by the company. This can also be observed in the network in Figure 6-5 (i) where the four thicker links corresponding to high  $ERA(a_i, r_j)$  metric values converge on the same resource. In contrast to Organisation -1, higher exclusive access risk values in Organisation -2 occur due to a single agent – *Emp 2* as indicated by Figure 6-4 (ii) (Note that red cells span across the row corresponding to *Emp 2* instead of vertically along a column as in the case of Organisation -1). The same can be observed in the network in Figure 6-5(ii) where all the thick links corresponding to higher risk values originate from the node labelled *Emp 2*. All resource access authorisations in Organisation-2 that receive high exclusive access risk scores are related to this employee, who is the IT administrator. Due to this role, he has exclusive access to servers and network devices of the organisation as evident from the network in Figure 6-5 (ii). Despite corresponding to an exclusive access authorisation, *Emp 2* → *Tel. T.* has a slightly lower risk score (indicated by orange in the heat map in Figure 6-4 (ii)). This is due to the lower resource criticality of the *Tel. T.* system. Higher  $ERA(a_i, r_j)$  metric scores of Organisation -3 correspond to two agents labelled *M.IT* and *IT.Adm* as shown in Figure 6-4 (iii). (Note that red and orange colour cells depicting high metric scores occur across the rows corresponding to these two agents.) Same can be observed in the resource access network in Figure 6-5 (iii), where the thicker links representing higher exclusive access links originate from the agents *M.IT* and *IT.Adm*. As in the case of Organisation -2, these links represent the two agents having exclusive access to servers and network devices in Organisation -3.

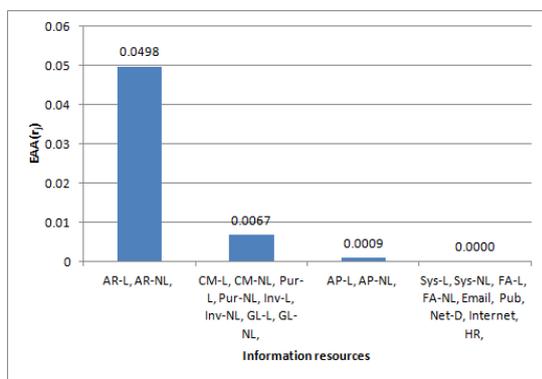
In order to summarise the results of the assessment of exclusive access risks, it is clear that in Organisations 2 and 3, higher risks occur due to agents such as IT managers and administrators having exclusive access to critical hardware components (e.g., servers and network devices). However, this trend cannot be confirmed in Organisation -1 since the sample does not contain information on the access authorisations of the key IT personnel.

### 6.2.2 Risks due to agents having exclusive privileged access to resources

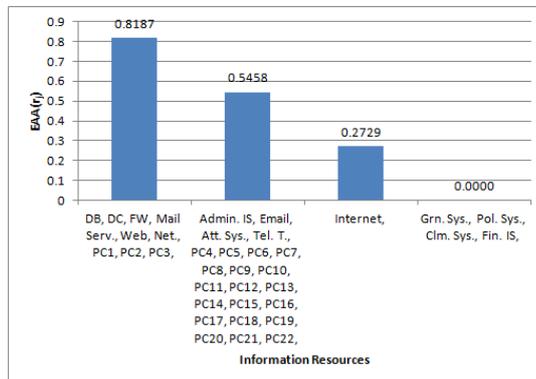
The results presented in the previous section (6.2.1) suggest that in Organisations 2 and 3 higher exclusive access risks occur due to the access authorisations given to key IT personnel. Typically, such IT personnel will have privileged access (also called administrative or root access privileges) to critical information resources. Sometimes, only one employee will have administrative access to information systems even when other

agents have user-level access to the same resource. Risks due to employees having exclusive privileged or administrative access to information systems can be quantified using the EAA metrics defined in Chapter 5, which combines three criteria for calculating the risks – the extent to which agents have exclusive access to resources, the sensitivity or criticality of the resources and the intrinsic risk characteristics of the agents. Like the ERA metric, EAA can be calculated per resource –  $EAA(r_j)$ , per agent –  $EAA(a_i)$  and per resource access authorisation –  $EAA(a_i, r_j)$ . Since the IT administrators of Organisation – 1 did not take part in the data collection, privileged access in Organisation -1 is defined as super user or user champion level access to the ERP software systems of the company. Although these users do not have full administrative control of the resources, they inherit many more privileges than a regular user. In the case of Organisations 2 and 3, privileged access is defined as administrative access to information resources since agents with administrative privileges are included in the data.

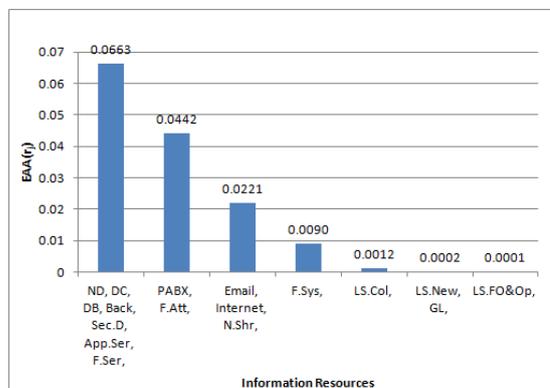
Figure 6-6 presents the  $EAA(r_j)$  scores of the information resources of the three organisations. A resource obtaining a metric value of zero indicates that none of the agents included in the study have administrative access to that resource.



(i) Organisation - 1



(ii) Organisation – 2

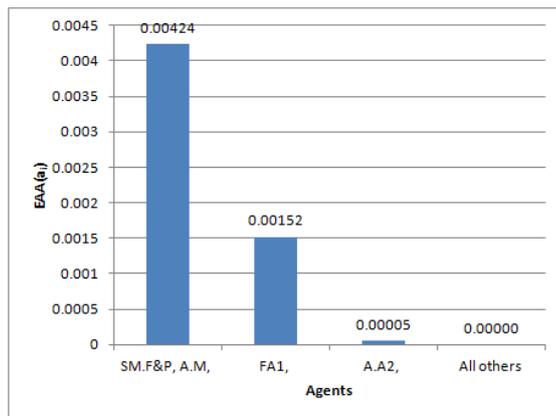


(iii) Organisation – 3

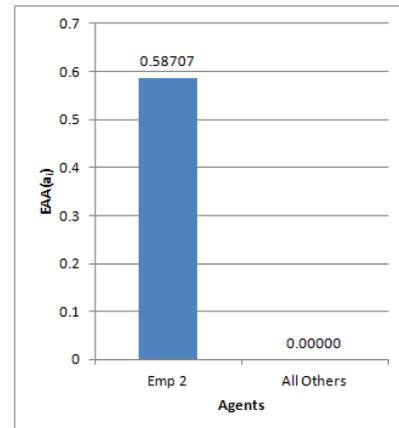
Figure 6-6:  $EAA(r_j)$  metric scores of information resources of organisations 1, 2 and 3

In Organisation-1, two ERP modules *AR-L* and *AR-NL* receive significantly higher  $EAA(r_j)$  scores than the other resources. Information resources -*DB, DC, FW, Mail Serv., Web, Net., PC1, PC2* and *PC3* receive the highest metric score in Organisation -2 while information resources - *ND, DC, DB, Back, Sec.D, App.Ser* and *F.Ser* receives the highest score in Organisation – 3. All resources in latter two lists, except for *PC1, PC2* and *PC3*, are critical hardware systems such as servers or network devices.

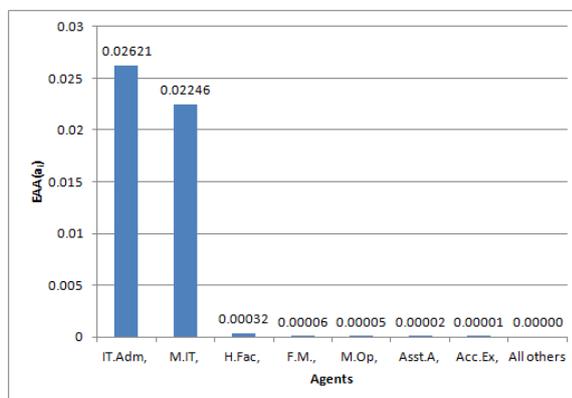
Figure 6-7 presents the  $EAA(a_i)$  metric scores of the agents in the three organisations. It is clear that only a very few agents in each organisation have privileged access and a great majority of users do not have privileged access capabilities to any resource (this is indicated by a metric value of zero). In Organisation-1, two managers – *SM.F&P* and *A.M.* receive the highest  $EAA(a_i)$  score. IT administrator labelled *Emp 2* is the only agent receiving a metric score grater than zero in Organisation-2. The two IT personnel labelled *IT. Adm* and *M.IT* are the only ones in Organisation -3 receiving significant  $EAA(a_i)$  values. As one would expect, in all three organisations, key IT staff members and unit managers carry the highest risk of exclusive privileged access to information resources.



(i) Organisation - 1



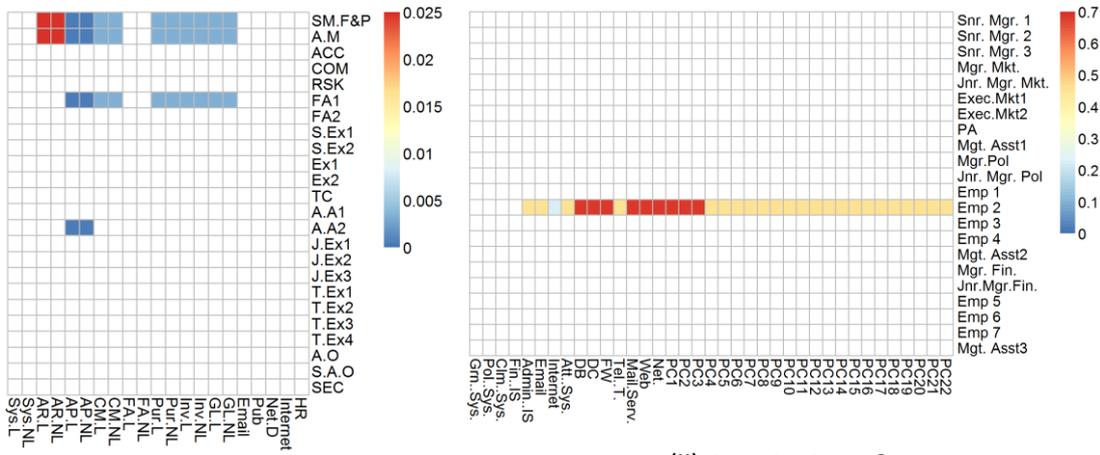
(ii) Organisation – 2



(iii) Organisation – 3

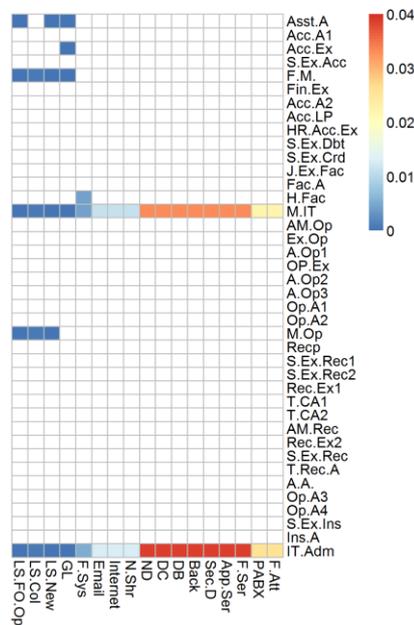
Figure 6-7:  $EAA(a_i)$  values of agents of organisations 1, 2 and 3

Risks due to exclusive administrative access can be further examined using the  $EAA(a_i, r_j)$  metric, which calculates the risk per access authorisation. Figure 6-8 depicts heat-map representations of exclusive privileged access risks of the three organisations. Rows represent agents while columns represent information resources. Cell colours represent the  $EAA(a_i, r_j)$  risk score of the resource access authorisations. The highest risks are indicated by red and lowest risks are indicated by dark blue. White cells indicate that there is no privileged access authorised for the corresponding agent, resource pair.



(i) Organisation - 1

(ii) Organisation - 2



(iii) Organisation - 3

Figure 6-8: Heat-map representations of exclusive privileged access risks per resource access authorisation of the three organisations. Rows represent agents while columns represent information resources. Cell colours represent the  $EAA(a_i, r_j)$  risk score of the authorisations where the highest risks are indicated by red and lowest risks are indicated by dark blue (Note that colour codes cannot be compared across organisations due to different scales used). White cells indicate that there is no privileged access authorised for the corresponding agent, resource pair.

The same information is depicted as network diagrams in Figure 6-9, which show the resource access networks of the three organisations. Blue spheres represent agents while triangles represent information resources. Links represent privileged access authorisations and all other types of access authorisations have been omitted. Link width and colour correspond to the  $EAA(a_i, r_j)$  metric scores, where thicker and darker links represent larger metric values. Nodes have been sized proportionately to the highest  $EAA(a_i, r_j)$  score they are associated with.

In Organisation – 1, privileged access authorisations  $SM.F\&P \rightarrow AR-L$ ,  $SM.F\&P \rightarrow AR-NL$ ,  $A.M \rightarrow AR-L$ , and  $A.M \rightarrow AR-NL$  receive the highest  $EAA(a_i, r_j)$  metric score as indicated in the corresponding heat-map by the red cells. Figure 6-9 (i) clearly shows that only two agents ( $SM.F\&P$  and  $A.M$ ) have privileged access to resources  $AR-L$  and  $AR-NL$  while all other resources have more than two agents with privileged access. However, in the context of this organisation, even the resource authorisations with this highest  $EAA(a_i, r_j)$  value could be acceptable since there are two agents with privileged access. The attributes of two staff members also indicate that they have not been flagged for any concerning behaviour. Furthermore, the IT staff members not included in this research study will have custodianship of the resources further minimising the chances of misuse of privileged access.

As indicated by the heat-map in Figure 6-8 (ii), agent labelled *Emp 2* has administrative access to all information resources, except for four, in Organisation -2. The variation of the risk value indicated in the heat-map is due to different sensitivity/criticality levels of the information resources. The same can be observed in the network in Figure 6-9 (ii), where all the privileged access links originate from *Emp 2*. In the context of Organisation-2, these exclusive privileged access risks are concerning since there is only one agent having administrative access over almost all the resources. Furthermore, this employee has been flagged for concerning behaviours according to attribute data. In the absence of proper controls, this agent can misuse the privilege access resulting in insider threat events. In Organisation-3, two agents have exclusive privileged access to all information resources, except five, as indicated in the heat-map in Figure 6-8 (iii) and the network in Figure 6-9 (iii). The variations of the risk values indicated in the heat-map are due to the differences in the sensitivity/criticality of information resource and the composite risk attribute values of the agents. Highest  $EAA(a_i, r_j)$  risk values occur due to access authorisations agents *IT. Adm* and *M. IT* have for resources *NC, DC, DB, Back, Sec. D, App. Ser* and *F*. Out of these, access

authorisations of agent *IT. Adm* (indicated by red cells in the heat-map) are higher than that of *M. IT* (indicated by orange cells in the heat-map). This difference is due to the agent *IT. Adm* Having a higher composite risk attribute since he is an external contractor.

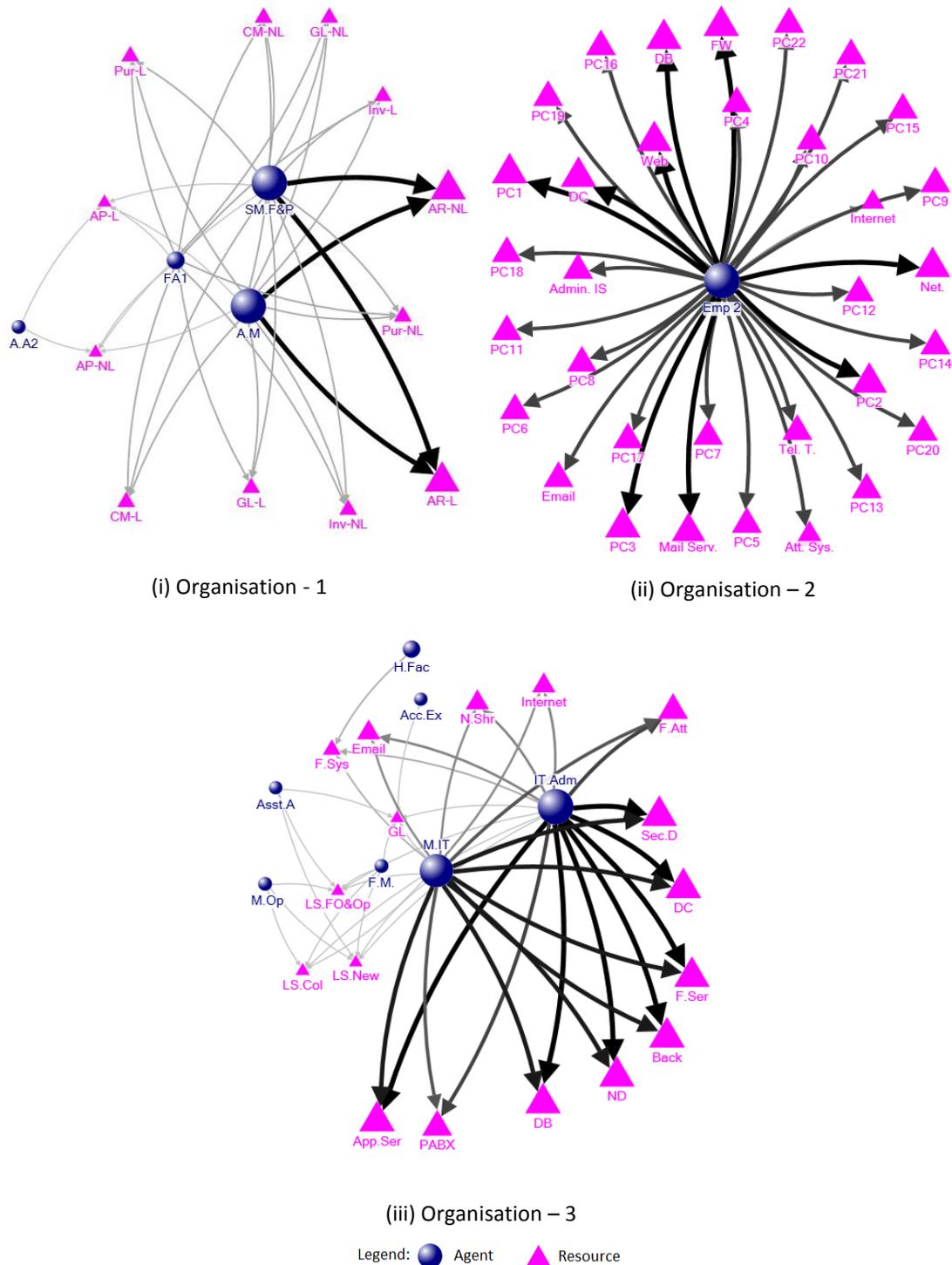


Figure 6-9: Resource access networks of the three organisations only showing the privileged access authorisations. Blue spheres represent agents while triangles represent information resources. Links represent privileged resource access authorisations. Link width and colour correspond to the  $EAA(a_i, r_j)$  metric scores where thicker and darker links represent larger metric values . Nodes have been sized proportionately to the highest  $EAA(a_i, r_j)$  score they are associated with.

### 6.2.3 Risks due to agents having access to resources not required for the tasks

Organisations must ensure that users only have access to information resources required to perform their tasks. Users having access to resources not required for their tasks is a violation of the principle of least privilege. The overall risk of excessive resource access can be calculated using the VNA metrics described in Chapter 5 by combining three factors – whether a given resource is required for the tasks performed by an agent, intrinsic risk properties of the agent and the sensitivity or criticality of the resource. The VNA metric can be calculated per agent –  $VNA(a_i)$  and per resource access authorisation -  $VNA(a_i, r_j)$ .

Figure 6-10 illustrates the  $VNA(a_i)$  scores of the agents of the three organisations (refer equation (1.16) in page 116 for the definition of this metric). If an agent only has access to resources required for his tasks and no more, the metric value of that agent would be zero. In Organisation-1, only employees labelled *COM*, *S.Ex1*, *TC*, *T.Ex3*, *SEC* receive a metric value of zero and majority of the agents have access to information resources not required for the tasks they perform. On the other hand, majority of the employees in Organisations 2 and 3 receive  $VNA(a_i)$  metric scores of zero.

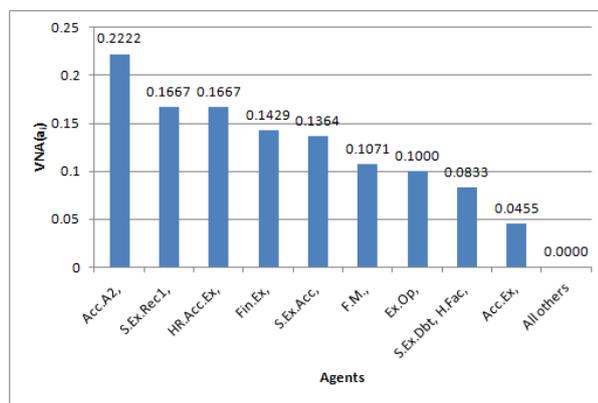
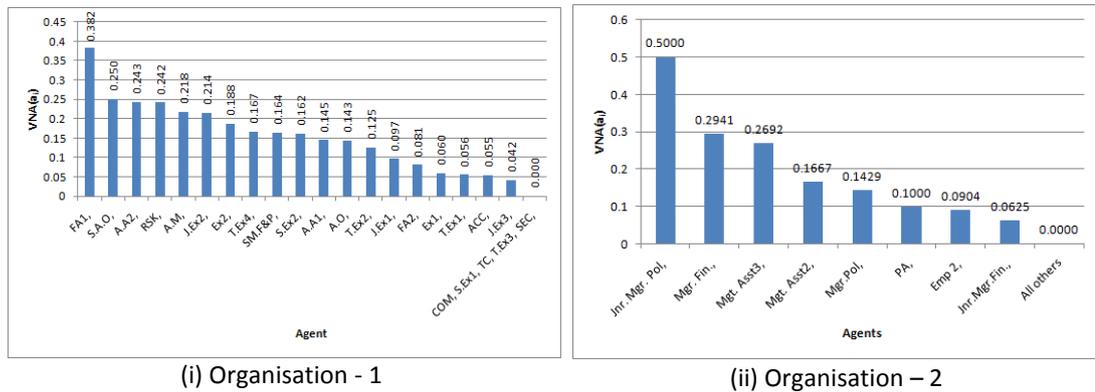


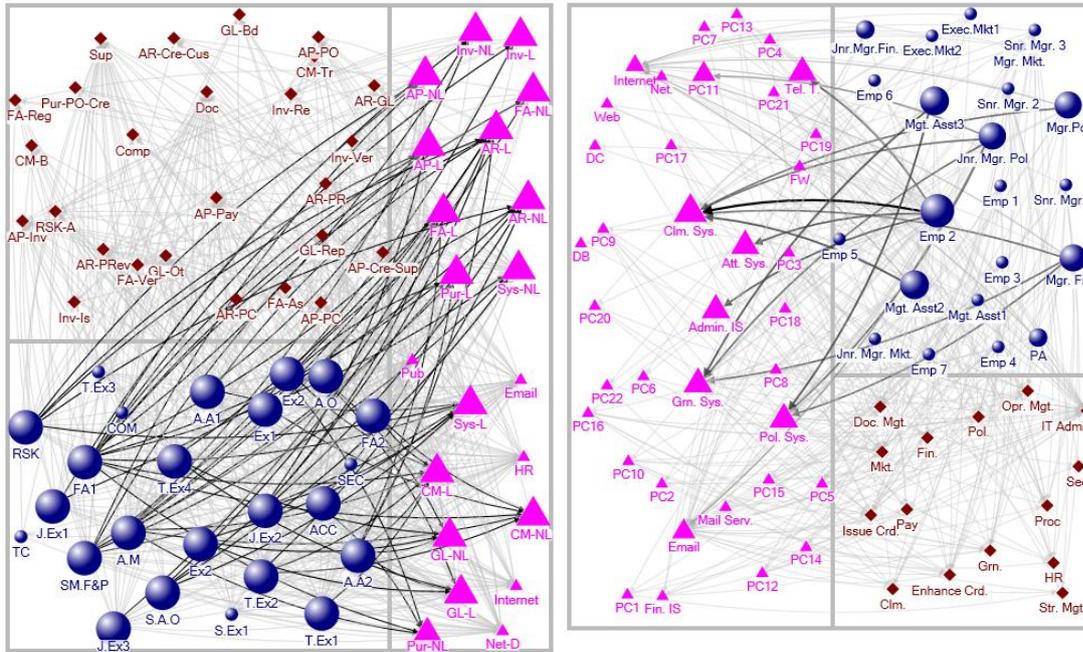
Figure 6-10:  $VNA(a_i)$  metric scores of agents in Organisations 1, 2 and 3

The access authorisations of agents receiving high  $VNA(a_i)$  scores can be further analysed using the  $VNA(a_i, r_j)$  metric, which is calculated per resource access authorisation (refer equation (1.17) in page 118 for the definition of  $VNA(a_i, r_j)$  metric). Figure 6-11 depicts the heat-map representations of risks due to agents having access to resources not required for their tasks. Rows represent agents while columns represent information resources. Cell colours represent the  $VNA(a_i, r_j)$  risk score of the authorisations where the highest risks are indicated by red and lowest risks are indicated by dark blue (refer the legend of each heat-map for a numerical comparison). White cells indicate that there is no access authorisation for the corresponding agent, resource pair.

Many pink coloured cells in the heat-map in Figure 6-11 (i) indicate that all those resource access authorisations are not required for the tasks performed by the relevant agents. In contrast to this, fewer cells in Figure 6-11 (ii) and (iii) have shades of pink or red. A set of pink coloured cells spanning across the row *FA1* in Figure 6-11 (i) show that this agent has access to many resources not required for his tasks. Confirming this further, *FA1* also receives the highest  $VNA(a_i)$  score in Organisation-1 as shown in the bar chart in Figure 6-10 (i). Similarly, in Figure 6-11 (ii), it can be observed that agent - *Jnr. Mgr. Pol* has five resources access authorisations while none of those have a dark blue shade (According to the scale used, dark blue indicate zero or very low risk). This implies that all resource access authorisations of the agent violate need to access requirements of the Organisation-2. Although this seems an unusual result, it occurs since the agent - *Jnr. Mgr. Pol* was on long-term leave during the data collection phase of the research. Hence, there were no task assignments for the agent but Organisation-2 did not disable his access credentials creating a vulnerability.

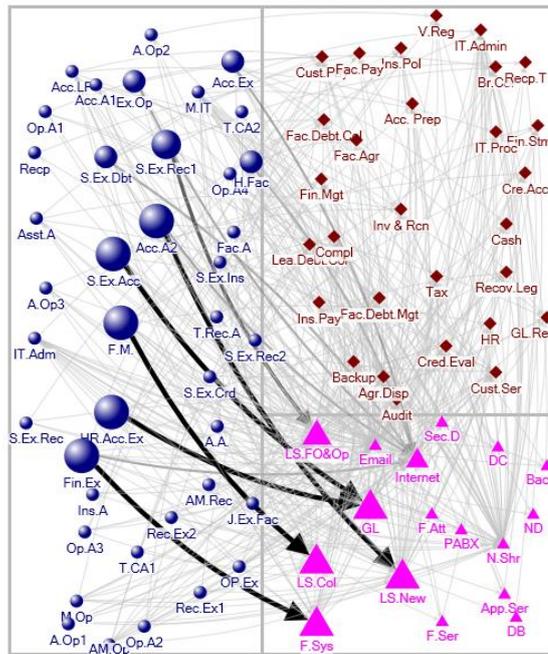
Figure 6-12 depicts multi-partite networks of Organisations 1, 2 and 3 depicting agent, resource and task nodes. The resource access links (links between agents and resources) have been shaded according to the  $VNA(a_i, r_j)$  score where darker links represent higher risk values. Agent and resource nodes have also been sized proportionately to the highest  $VNA(a_i, r_j)$  metric value they are associated with. Numerous dark links in Figure 6-12(i) show the access authorisations that violate any need to access requirements of Organisation-1. Also, there are only a few smaller-sized agent and resource nodes in the same diagram, indicating violation of need to access risks are widespread in Organisation-1.





(i) Organisation - 1

(ii) Organisation – 2



(iii) Organisation – 3

Legend: ● Agent ▲ Resource ◆ Task

Figure 6-12: Multi-partite networks of Organisations 1, 2 and 3 consisting of agent, resource and task nodes. The resource access authorisations that receive comparatively high  $VNA(a_i, r_j)$  scores are indicated by darker links. agent and resource nodes have been sized proportionately to the highest  $VNA(a_i, r_j)$  score they are associated with.

In comparison to Organisation–1, in Organisations 2 and 3 there are fewer risks due to agents having access to resources not required for their tasks as evident from networks

given in Figure 6-12(i) and (ii). Organisations can drill-down these networks to identify vulnerabilities that result in higher risk metric scores. For example, resource access authorisations and task assignments of three agents scoring high  $VNA(a_i)$  risk values are illustrated in Figure 6-13. Information resources that agents can access but are not required for the tasks they perform are circled in the diagrams. As shown in Figure 6-13(i) agent labelled *FA1* has access to thirteen (13) such resources while agents *Mgr. Fin.* and *Acc. A2* have access to four (4) and two (2) such resources respectively. The other agents who score non-zero  $VNA(a_i)$  values can be similarly analysed.

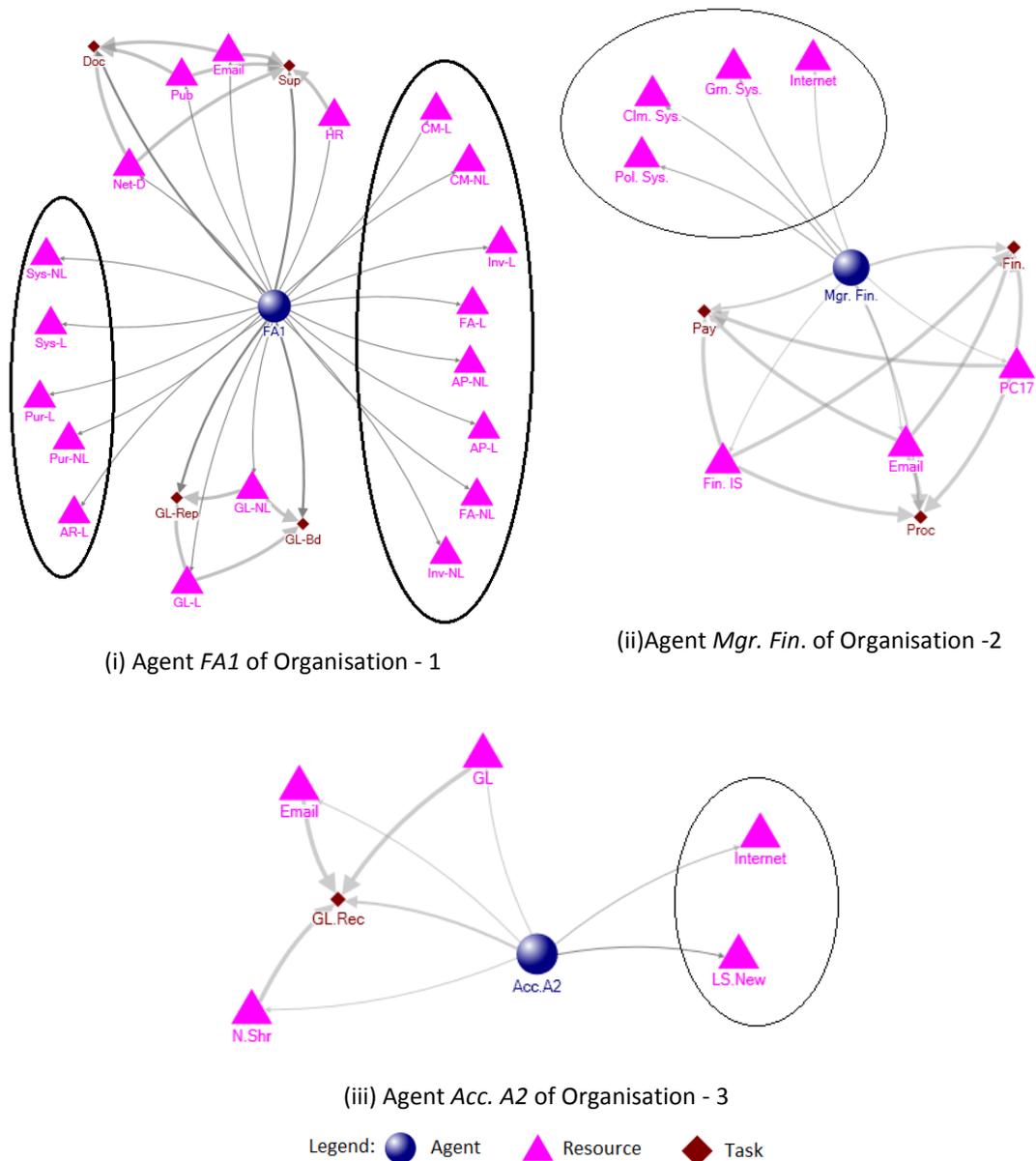
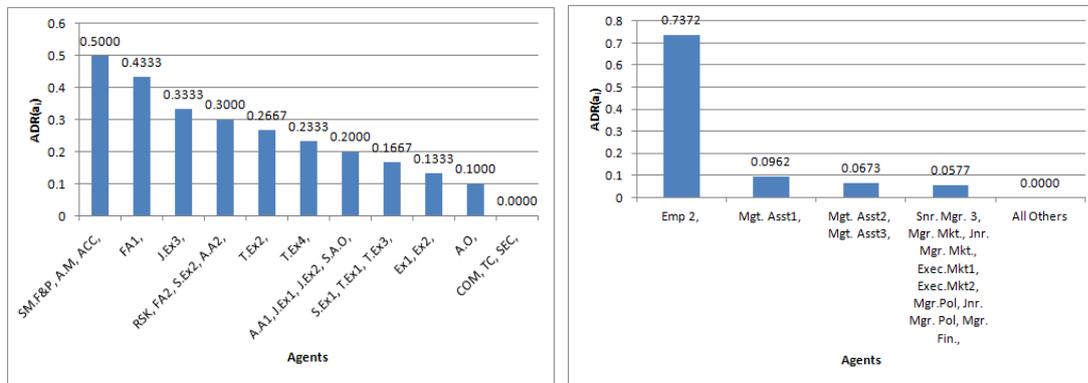


Figure 6-13: Multipartite networks illustrating resource access authorisations and task assignments of three agents receiving high  $VNA(a_i)$  risk scores – (i) *FA1* of Organisation -1 (ii) *Mgr. Fin.* in Organisation -2 and (iii) *Acc.A2* of Organisation – 3. The resources that agents can access but are not required for their tasks have been circled.

### 6.2.4 Risks due to agents having access to two dependent information resources

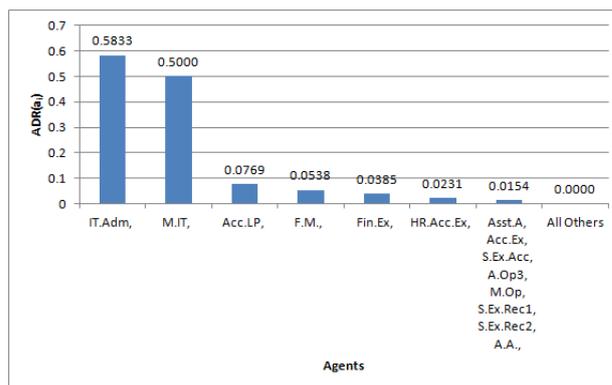
Sometimes, agents having access to two dependent information resources can create insider risks as described in Chapter 5. The ADR metrics defined in the same chapter can be used to quantify risks due to this vulnerability by combining three criteria – number of dependent resources that an agent can access, the sensitivity or criticality of the resources involved and intrinsic risk properties of the agents. The ADR metric can be calculated per agent –  $ADR(a_i)$  and per resource access authorisation –  $ADR(a_i, r_j)$ .

Figure 6-14 presents  $ADR(a_i)$  risk scores of agents in Organisations 1,2 and 3 (refer equation (1.20) in page 121 for the definition of this metric).



(i) Organisation - 1

(ii) Organisation – 2



(iii) Organisation – 3

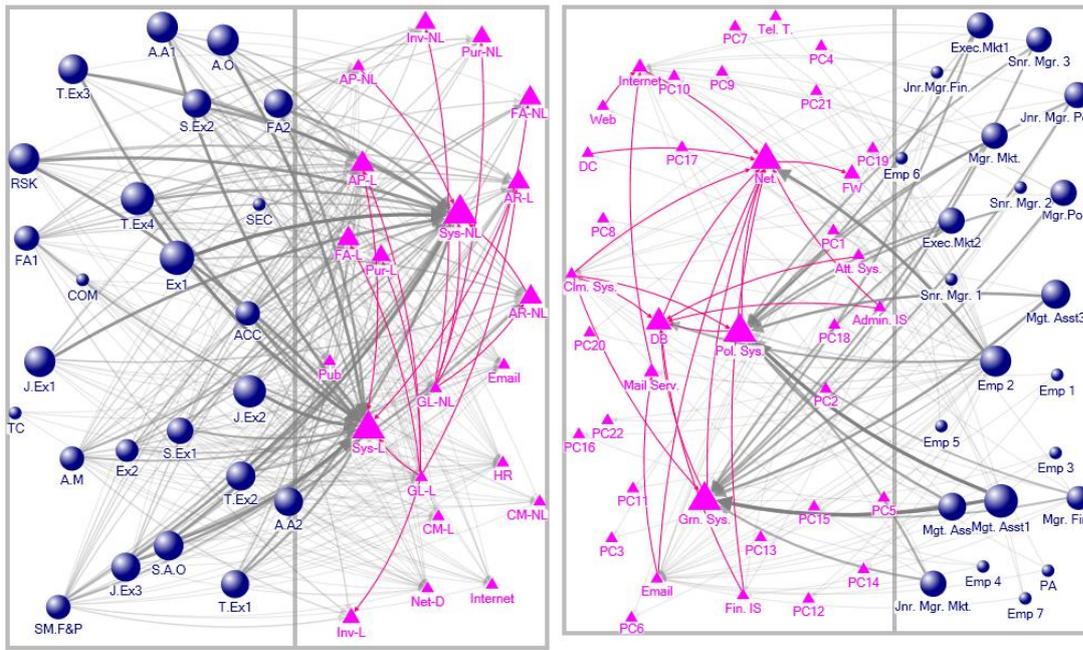
Figure 6-14:  $ADR(a_i)$  metric scores of agents of Organisation 1,2 and 3

In Organisation-1, three agents *SM.F&P*, *A.M.*, and *ACC* receive the highest risk scores. All three of them occupy managerial positions of the company. Agent labelled *Emp 2*, who is

the systems administrator, receives the highest  $ADR(a_i)$  risk score in the second company. Unlike in Organisation-1, in Organisation-2 there is a clear gap between the metric scores of *Emp 2* and others, who either score a risk score of zero or very low values, the former value indicating that relevant agents do not have access to any dependent information resources. In Organisation 3, two employees *IT.Adm* and *M.IT* receive significantly higher metric scores when compared with others in the same company. Again, the two employees concerned are the Systems Administrator and the IT Systems Manager. According to the above results, it is clear that relative  $ADR(a_i)$  risk scores of agents who play information technology or managerial roles are higher than that of others. Moreover, this difference is more conspicuous for agents involved in IT administrative tasks.

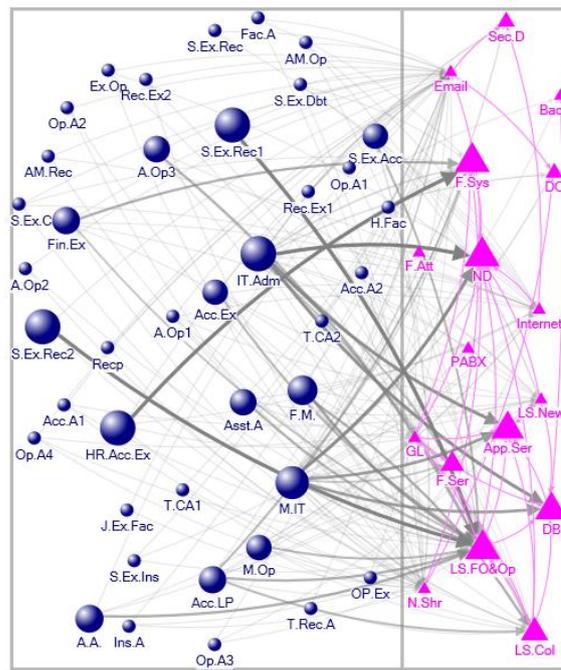
The risk of access to dependent resources per access authorisation can be assessed utilising the  $ADR(a_i, r_j)$  metric scores (refer equation (1.21) in page 124 for the definition of this metric). Figure 6-15 illustrate the resource access and resource dependency networks of the three organisations. The grey colour links represent resource access authorisations while the links in pink represent resource dependencies. Nodes have been sized proportionately to the highest  $ADR(a_i, r_j)$  risk score they are associated with. Also the darker and thicker resource access links represent authorisations with greater dependent resource access risks. The same information can be depicted in heat-maps as illustrated in Figure 6-16. In the heat-maps, rows represent agents while columns represent information resources. Cell colours represent the  $ADR(a_i, r_j)$  risk score of the authorisations where the highest risks are indicated by red and lowest risks are indicated by dark blue. If there is no resource access authorisation for a given agent, resource pair it is indicated by a white cell.

From Figure 6-15(i), it is clear that majority of the high risk authorisations in Organisation-1 are associated with the two resources *Sys-L* and *Sys-NL* (these two resource nodes are visibly larger and many darker and thicker links terminate in the two nodes). This can also be observed in the heat-map in Figure 6-16 (i), where the two columns corresponding to *Sys-L* and *Sys-NL* have many yellow and orange coloured cells. The reasons for the high risk scores can be examined by drilling down the network to find the related resource access authorisations and resource dependencies. For example, Figure 6-17 (i) is a sub-graph of the network in Figure 6-15(i) depicting the agents who has access to *Sys-L* as well as other resources that depend on it. The sub-graph demonstrates that, except for the agent labelled *Ex1*, all agents having access to *Sys-L* can also access at least one resource that depend on *Sys-L*.



(i) Organisation - 1

(ii) Organisation – 2



(iii) Organisation – 3

Legend: ● Agent ▲ Resource

Figure 6-15: Bipartite networks of Organisations 1, 2 and 3 consisting of agent and resource nodes. The networks depict both resource access links (shown in grey colour) and resource dependency links (shown in pink colour). Resource access authorisations that receive comparatively high  $ADR(a_i, r_j)$  scores are indicated by darker and thicker links. Agent and resource nodes have been sized proportionately to the highest  $ADR(a_i, r_j)$  risk score they are associated with.

According to the network in Figure 6-15 (ii), many access authorisations with high dependent resource access risks are associated with the two resources – *Grn. Sys* and *Pol. Sys* (notice that many thicker and darker links terminate in these two nodes and they are visibly larger). This can also be confirmed using the heat-map in Figure 6-16 (ii), in which the two columns corresponding to above information resources have many yellow, orange or red cells. Sub-graphs showing the resource access authorisations and dependencies of the two information resources *Grn. Sys* and *Pol. Sys* can be used to scrutinise the reasons for the pattern mentioned above. Figure 6-17 (ii) illustrates resource access authorisations and resource dependencies associated with *Grn. Sys*. According to the figure all the agents, except for *Emp 3* and *Emp 4*, accessing *Grn. Sys*. have access to the information resource *Clm. Sys*. that depends on the former. Since many dependent resource access risks in Organisation-2 occur due to agents having access to the *Grn. Sys*. and *Clm. Sys*. concurrently, organisation must decide whether such access is necessary for the employees. If it is unavoidable, other risk mitigating strategies should be considered.

In contrast to Organisations 1 and 2, resource access links with high  $ADR(a_i, r_j)$  scores are more evenly distributed among information resources of Organisation-3 (refer Figure 6-15 (iii)). On the other hand, heat-map in Figure 6-16 (iii) makes it clear that there are several high risk resource access links associated with agents labelled *M.IT* and *IT.Adm*. Figure 6-17 (iii) depicts resource access authorisations of agent - *IT.Adm* and dependencies between those resources. It can be clearly seen that there are numerous dependencies between resources accessed by this agent. Some of these concurrent access authorisations can create serious insider risks. For example, Figure 6-17 (iii) shows that the agent *IT.Adm* has access to both the database (resource labelled *DB*) and the backup of the database (resource labelled *Back*). Such authorisations can contribute to insider threats as demonstrated by case 24 and 27 listed in Table 4-1, where a malicious employee had access to original information and its backup enabling him to destroy both resources. However, in Organisation – 3, this threat has been mitigated to an extent by assigning another employee - *M.IT* to supervise the backup process.

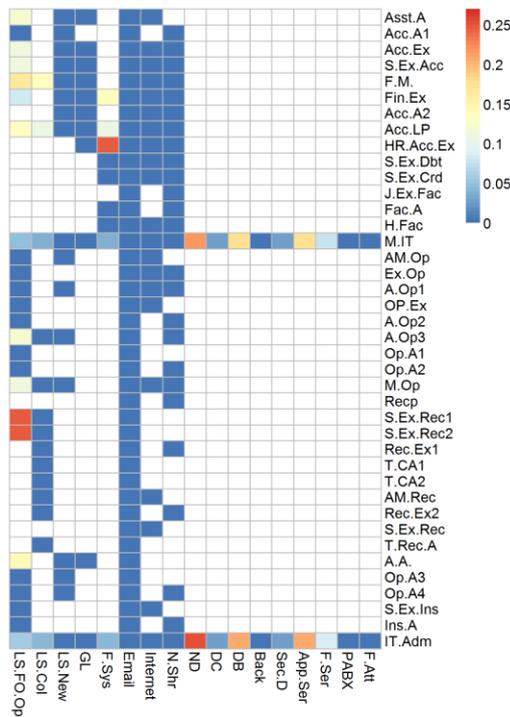
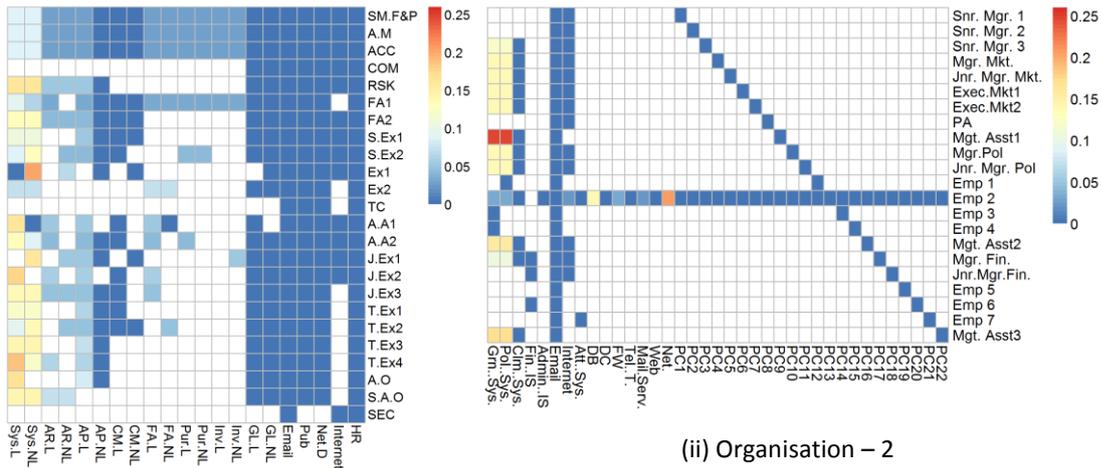
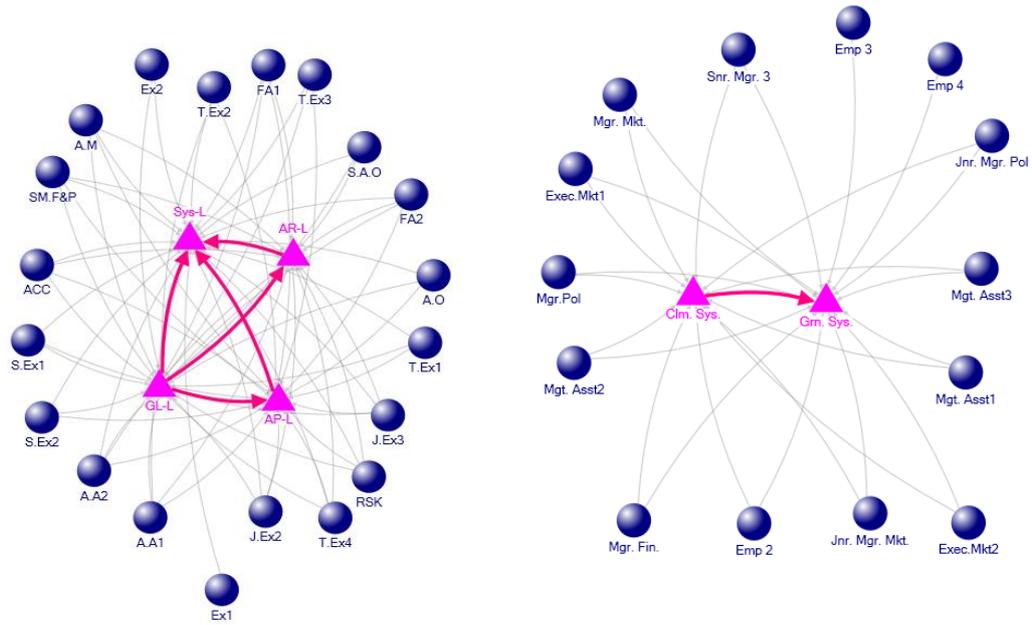
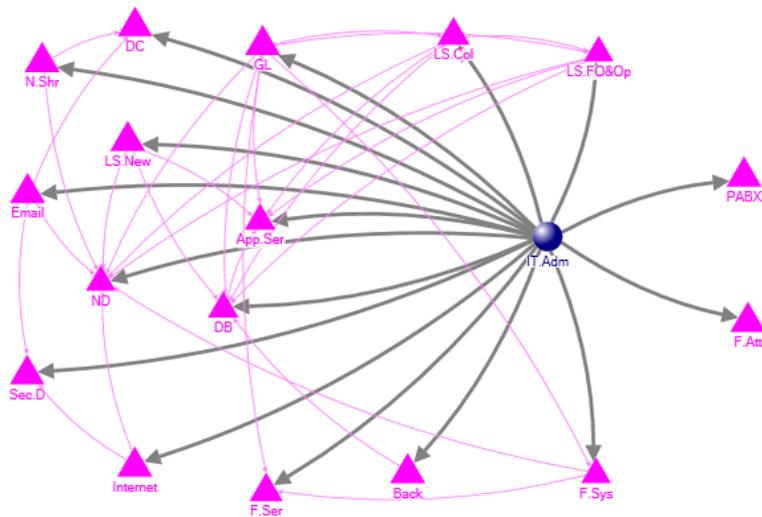


Figure 6-16: Heat-map representations of risks due to agents having access dependent information resources. Rows represent agents while columns represent information resources. Cell colours represent the  $ADR(a_i, r_j)$  risk score of the authorisations where the highest risks are indicated by red and lowest risks are indicated by dark blue (refer the legend of each heat-map for a numerical comparison). Same scale has been used in all three heat-maps). White cells indicate that there is no access authorisation for the corresponding agent, resource pair.



(i) Agents accessing the resource *Sys-L* and other resources that depend on it in Organisation-1. (ii) Agents accessing the resource *Grn. Sys* and other resources that depend on it in Organisation-2.



(iii) Resource access authorisations of agent - *IT.Adm* and dependencies between those resources in Organisation -3.

Legend: ● Agent ▲ Resource

Figure 6-17: Selected sub-graphs from Organisation 1,2 and 3. The grey coloured links represent resource access authorisations while the pink coloured ones represent resource dependencies.

### 6.3 Assessment of risks due to task assignments

Two types of risks that occur due to task assignments have been listed in Table 5-5 in Chapter 5. This section presents the results of the assessment of risks arising due to task assignments in the three organisations analysed in this research.

### 6.3.1 Risks due to agents performing tasks exclusively

As described in section 5.4, an agent performing a task exclusively can lead to fraud, sabotage or information leakage, particularly in the absence of any supervision. The ETA metrics defined in the same section can be used to assess risks arising due to exclusive task assignments by considering three criteria – the extent to which agents are exclusively assigned to tasks, the criticality of the task and the intrinsic risk properties of the agents. The ETA metric can be calculated per task –  $ETA(t_p)$ , per agent –  $ETA(a_i)$  and per task assignment –  $ETA(a_i, t_p)$ . Figure 6-18 presents the metric values of the tasks that receive the top five  $ETA(t_p)$  risk scores in the three organisations (refer equation (1.22) in page 127 for the definition of this metric).

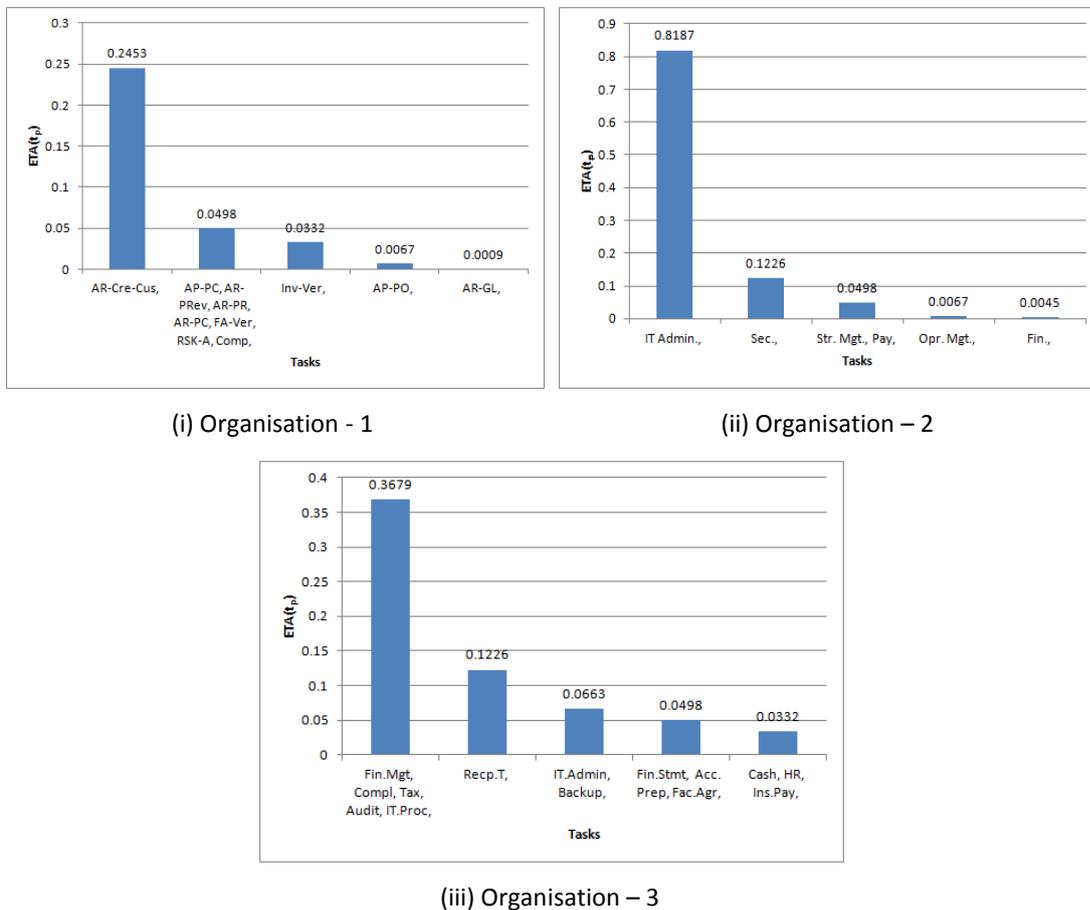
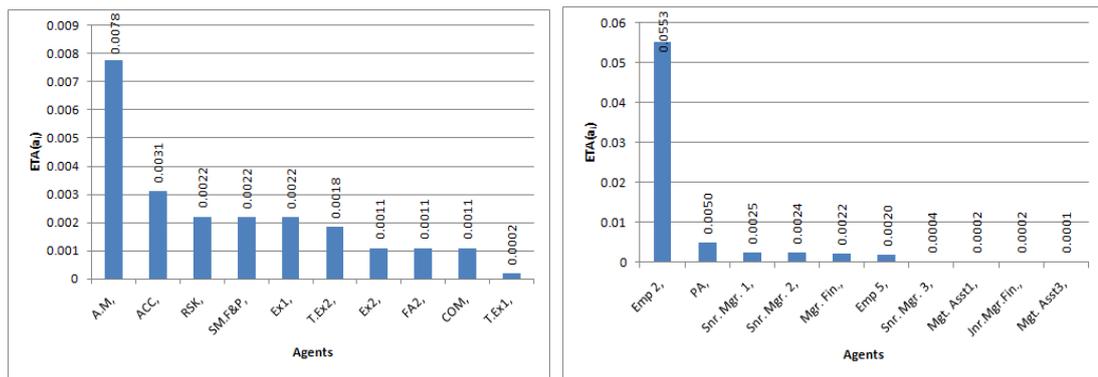


Figure 6-18:  $ETA(t_p)$  values of the tasks receiving the top-five metric scores in organisations 1, 2 and 3

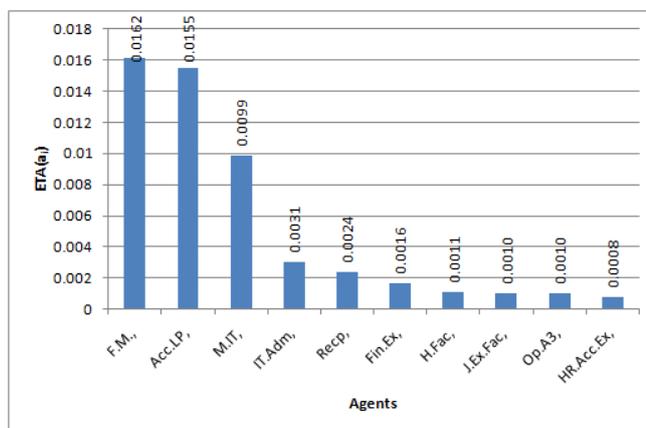
According to the bar chart in Figure 6-18 (i), the task - *Ar-Cre-Cus* receives a significantly higher risk score than all others in Organisation-1. The task – *IT Admin* scores a high  $ETA(t_p)$  risk score in Organisation-2 while five tasks - *Fin.Mgt, Compl, Tax, Audit* and *IT.Proc* receive the highest score in Organisation-3. Two of these – *IT Admin* (IT systems administration) in organisation-2 and *IT.Proc* (Requisition, procurement and approval of new IT systems) in

Organisation-3 are IT related tasks. Furthermore, two other IT related tasks - *IT.Admin* (IT systems administration) and *Backup* (creating, verifying and maintaining backups) score the third highest risk value in Organisation-3. The information technology related tasks do not appear in the results for Organisation-1 since they were absent from the data collected from that organisation. Agents whose task assignments create high exclusive assignment risks can be identified using the  $ETA(a_i)$  metric (refer equation (1.23) in page 128 for the definition of this metric). The top ten  $ETA(a_i)$  risk scores of the three organisations are presented in Figure 6-19.



(i) Organisation - 1

(ii) Organisation - 2



(iii) Organisation - 3

Figure 6-19: The top-ten  $ETA(a_i)$  risk scores of the agents in Organisations 1,2 and 3.

As shown in Figure 6-19 a small number of agents in each organisation can be distinguished from others based on the  $ETA(a_i)$  risk values. In Organisation-1, agent labelled *A.M.* receives the highest score while agent - *Emp 2* receives the highest score in Organisation-2. The three agents – *F.M.*, *Acc.LP* and *M.IT* receive significantly larger metric values in Organisation-3. All the agents scoring high exclusive task assignment risks in their respective organisations are managers or IT administrators, except for the agent labelled *Acc.LP*, who performs a senior accounting role.

The exclusive task assignments can be further analysed using the  $ETA(a_i, t_p)$  metric scores (refer equation (1.24) in page 129 for the definition of this metric). The  $ETA(a_i, t_p)$  metric values for the task assignments of the three organisations are illustrated in the heat-maps given in Figure 6-20. In the heat-maps rows represent agents while columns represent tasks assigned to them. Cell colours represent the  $ETA(a_i, t_p)$  risk scores of task assignments, where the highest risks are indicated by red and lowest risks are indicated by dark blue (refer the legend for a numerical comparison. Note that the scales differ for each organisation and colours cannot be used to compare risks across organisations). White cells indicate that the corresponding agent is not assigned for the corresponding task. Furthermore, task assignment networks of the three organisations are depicted in Figure 6-21. In the network diagrams, blue spheres represent agents while diamonds represent tasks. Links represent task assignments. Link width and colour correspond to the  $ETA(a_i, t_p)$  metric scores where thicker and darker links represent larger metric values. Also, nodes have been sized proportionately to the largest  $ETA(a_i, t_p)$  risk value they are associated with.

According to the heat-map in Figure 6-20 (i), the task assignment  $A.M \rightarrow Ar.Cre.Cus$  has a distinctly high risk value in comparison to other task assignments of the organisation. This task assignment is also highlighted in Figure 6-21 (i) and it can be clearly seen that only one agent has been assigned for the task. All other tasks assignments have at least two agents assigned for them. In the network diagram in Figure 6-21 (i), tasks which are performed by a lesser number of agents appear towards the network edge. As a result of this exclusive task assignment, the corresponding agent –  $A.M$  and the task –  $Ar.Cre.Cus$  receive the highest  $ETA(a_i)$  and  $ETA(t_p)$  metric scores in Organisation-1. Similarly, in Organisation-2, one task assignment –  $Emp 2 \rightarrow IT.Admin.$  receives a significantly higher risk score as indicated in Figure 6-20 (ii). This task assignment can be also seen in the network diagram in Figure 6-21 (ii), where it is highlighted. This task assignment corresponds to the IT systems administrator ( $Emp 2$ ) performing all IT system administration tasks ( $IT.Admin.$ ) exclusively. In this particular case, it might be not be practical for smaller organisations such as Organisation-2 to allocate more than one staff member for IT administration. However, the risk can be somewhat mitigated by assigning another staff member to supervise the duties of the only IT systems administrator. Another strategy would be to outsource some of the IT services although this has to be done after evaluating the risks of outsourcing against the current setup.

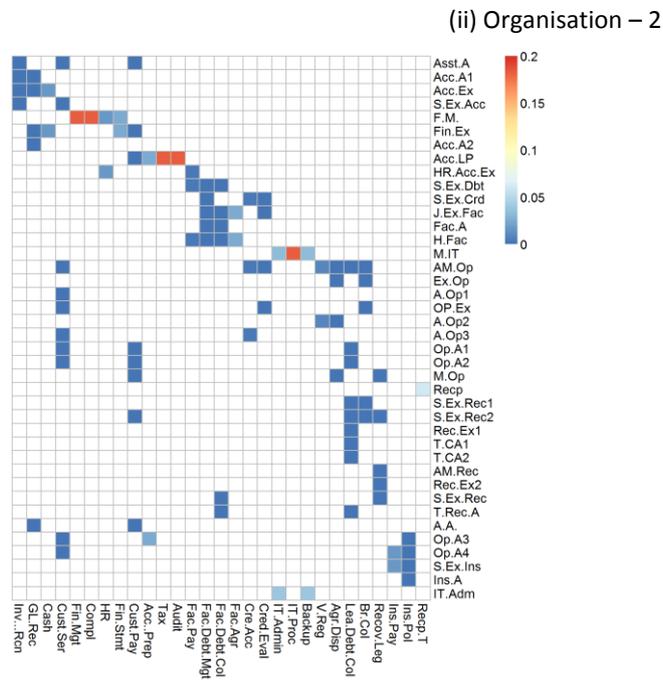
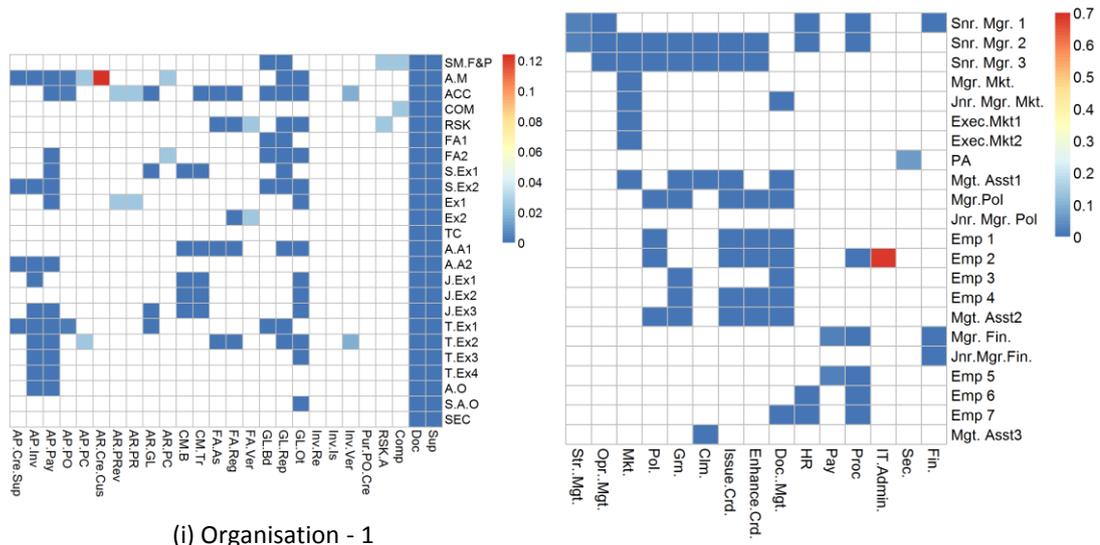
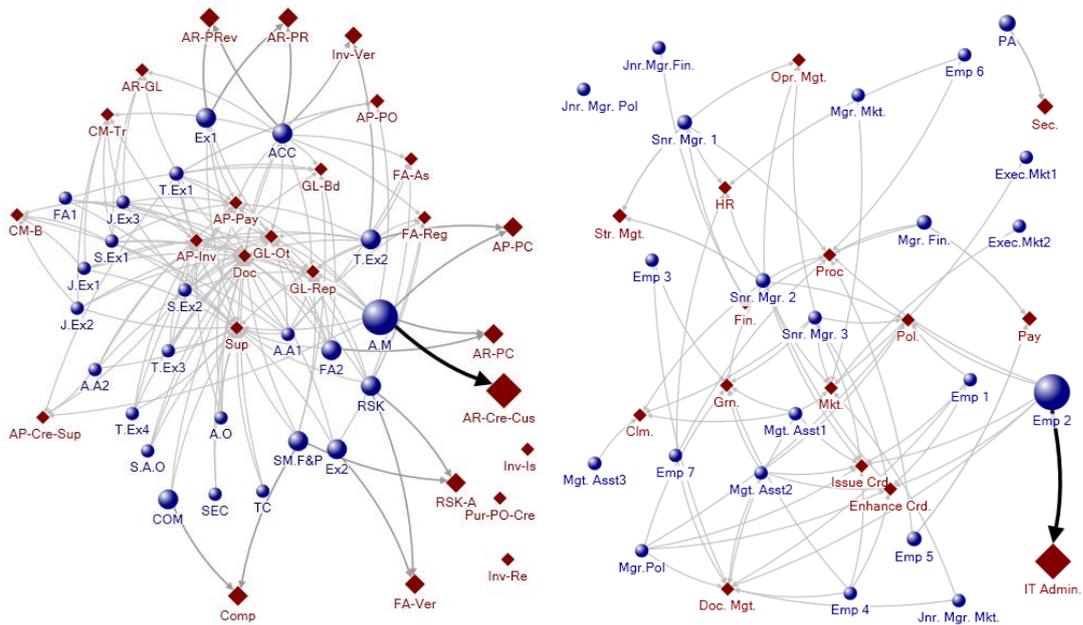


Figure 6-20: Heat-map representations of the exclusive task assignment risks of Organisations 1, 2 and 3. Rows represent agents while columns represent tasks. Cell colours represent the  $ETA(a_i, t_p)$  risk scores of task assignments where the highest risks are indicated by red and lowest risks are indicated by dark blue (Note that the scales differ in each organisation and colours cannot be used to compare risks across organisations). White cells indicate that the corresponding agent is not assigned for the given task.

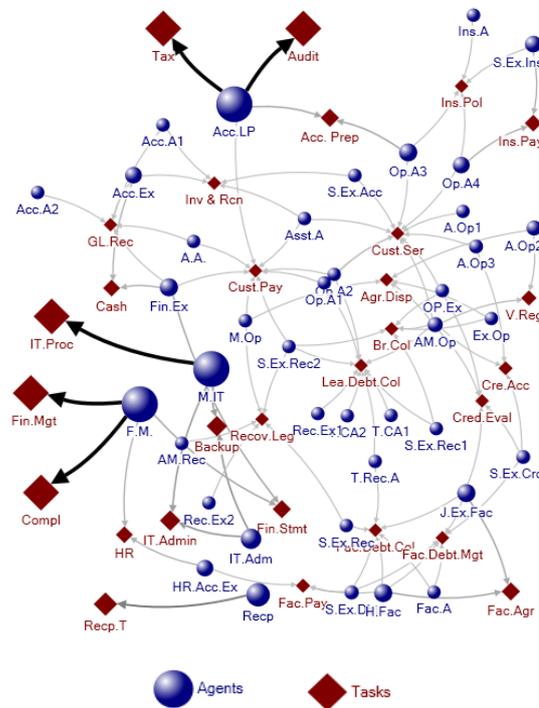
Five task assignments -  $F.M. \rightarrow Fin.Mgt$ ,  $F.M. \rightarrow Compl$ ,  $Acc.LP \rightarrow Tax$ ,  $Acc.LP \rightarrow Audit$ ,  $M.IT \rightarrow IT.Proc$  stand out as ones with high  $ETA(a_i, t_p)$  risk scores in Organisation-3 according to the heat-map in Figure 6-20 (iii). All five correspond to a sole agent performing a task as indicated in the network diagram in Figure 6-21 (iii). Some of these tasks such as taxation ( $Tax$ ) and requisition, procurement and approval of new IT systems ( $IT.Proc.$ ) clearly need some supervision from additional staff members to mitigate any risks of fraud or sabotage.

Network diagram in Figure 6-21 (iii) shows another task - *Recp.T* (reception duties) which is performed by a single staff member. However, this task assignment receives a much lower risk score due to lower criticality of the task.



(i) Organisation - 1

(ii) Organisation - 2

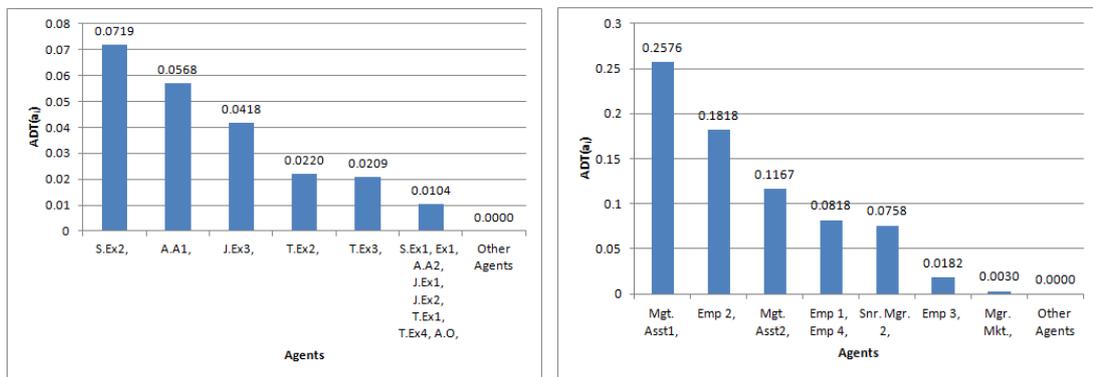


(iii) Organisation - 3

Figure 6-21: Task assignment networks of the three organisations. Blue spheres represent agents while diamonds represent tasks. Links represent task assignments. Link width and colour correspond to the  $ETA(a_i, t_p)$  metric scores where thicker and darker links represent larger metric values. Nodes have been sized proportionately to the largest  $ETA(a_i, t_p)$  risk value they are associated with.

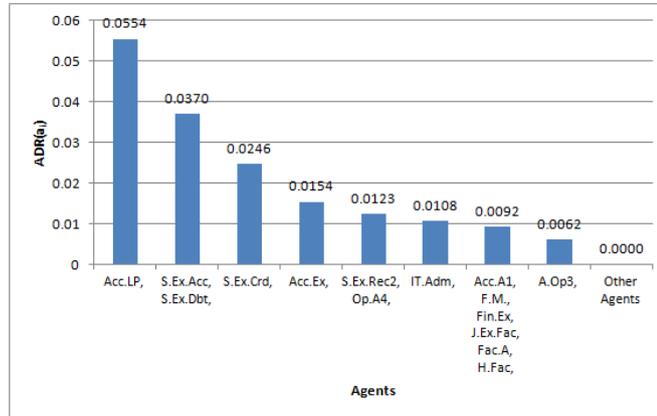
### 6.3.2 Risks due to agents performing two dependent tasks

An agent performing two dependent tasks can be an instance where separation of duty is not enforced as described in section 5.4.2. The ADT metrics defined in the same section can be used to quantify the risks due to agents performing dependent tasks by considering three criteria – number of dependent tasks an agent performs, the criticality of the tasks involved and the intrinsic risk characteristics of the agent. The ADT metric can be calculated per agent –  $ADT(a_i)$  and per task assignment  $ADT(a_i, t_p)$ . Equation (1.27) in page 131 defines  $ADT(a_i)$  metric while equation (1.28) in page 132 defines the  $ADT(a_i, t_p)$  metric. Figure 6-22 presents the  $ADT(a_i)$  risk scores of the agents in Organisations 1, 2 and 3.



(i) Organisation - 1

(ii) Organisation – 2

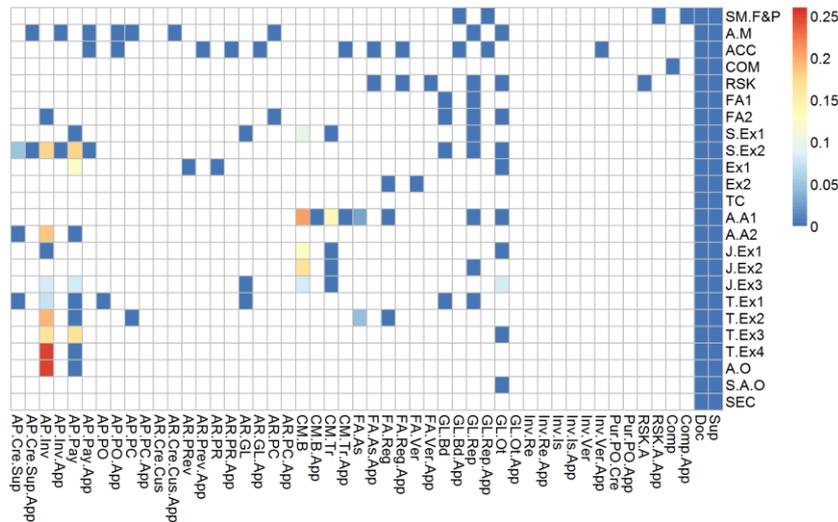


(iii) Organisation – 3

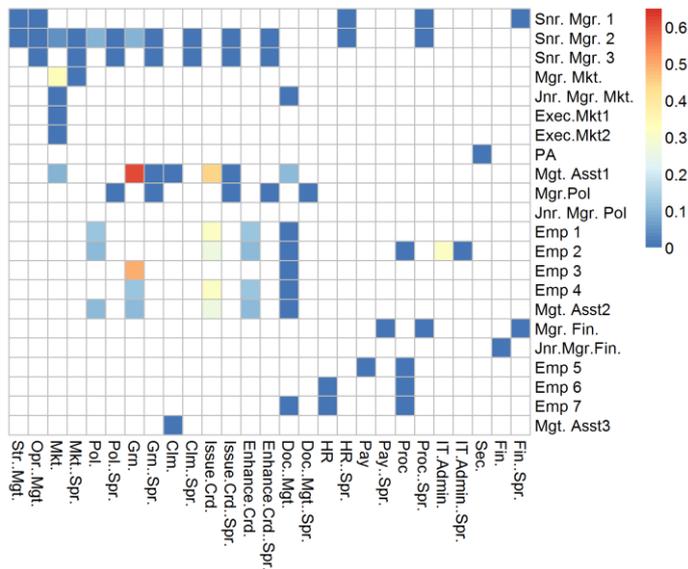
Figure 6-22:  $ADT(a_i)$  risk values of the agents in organisations 1,2 and 3.

In Organisation -1, almost half of the employees (11 out of 24 agents) receive an  $ADT(a_i)$  risk value of zero indicating that they do not have to access to any dependent tasks. Majority of the employees in Organisations 2 and 3 also receive  $ADT(a_i)$  scores of zero. Out of the agents who receive non-zero metric values in Organisation-1, *S.Ex2*, *A.A1*, and *J.Ex3* receive comparatively high metric scores. In Organisation-2, the agents labelled *Mgt. Asst1* and *Emp 2* receive relatively high  $ADT(a_i)$  values while agents - *Acc.LP*, *S.Ex.Acc* and *S.Ex.Dbt* obtain high scores in Organisation-3.

Risks due to dependent task assignments can be analysed further using the  $ADT(a_i, t_p)$  metric. Figure 6-23 depicts the heat-map representations of the dependent task assignment risks of Organisations 1 and 2 while the same for Organisation-3 is shown in Figure 6-24. In all three heat-maps, rows represent agents while columns represent tasks. Cell colours represent the  $ADT(a_i, t_p)$  risk scores of task assignments, where the highest risks are indicated by red and lowest risks are indicated by dark blue. White cells indicate that the corresponding agent is not assigned for the given task.



(i) Organisation - 1

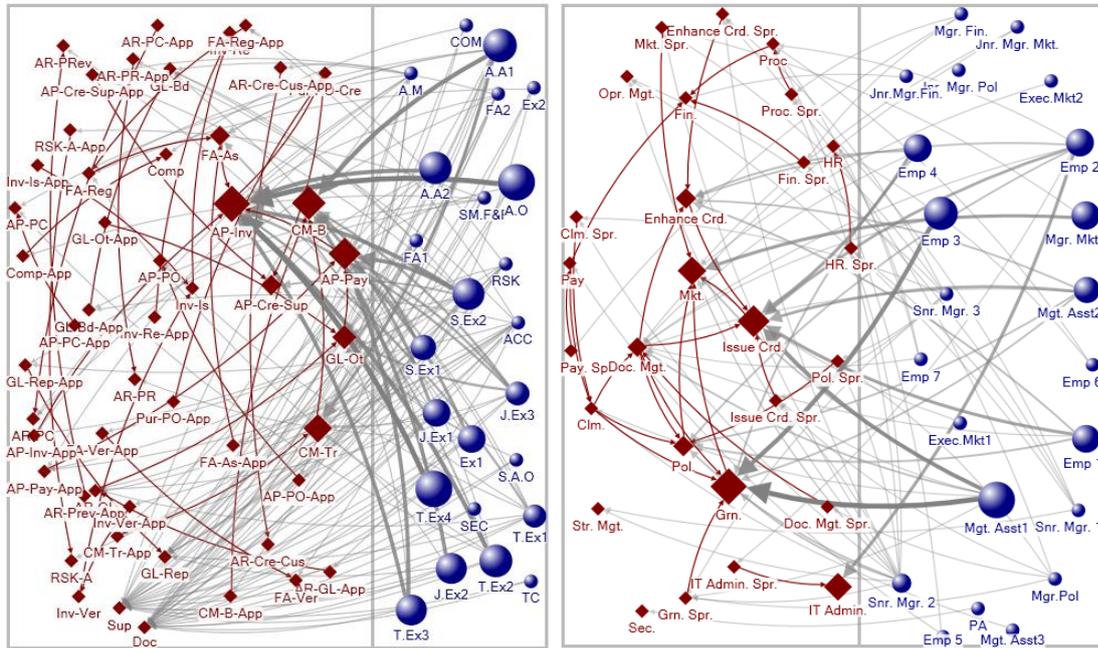


(ii) Organisation – 2

Figure 6-23: Heat-map representations of the dependent task assignment risks of Organisations 1 and 2. Rows represent agents while columns represent tasks. Cell colours represent the  $ADT(a_i, t_p)$  risk scores of task assignments where the highest risks are indicated by red and lowest risks are indicated by dark blue (refer the legend for a numerical comparison. Note that the scales differ for two organisations and colours cannot be used to compare risks across them). White cells indicate that the corresponding agent is not assigned for the given task.

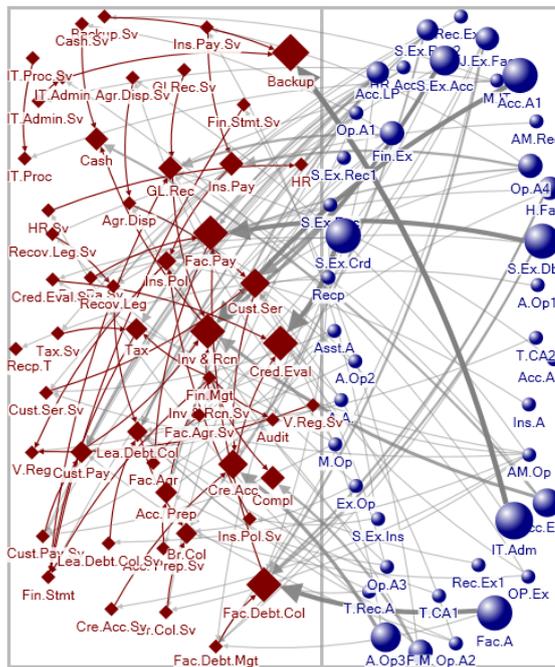


risk values, terminate at them. The three sub-networks consisting of task dependency and task assignment links related to these three nodes are given in Figure 6-26.



(i) Organisation-1

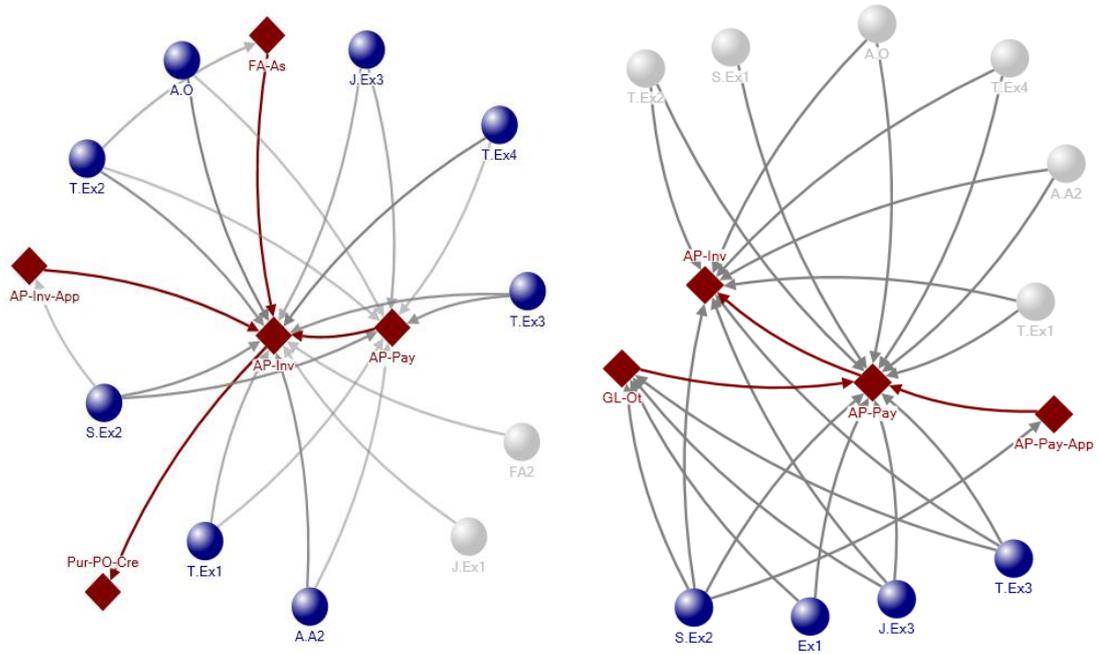
(ii) Organisation-2



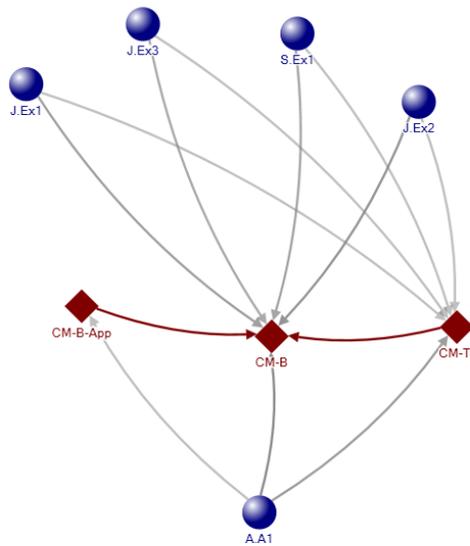
(iii) Organisation – 3



Figure 6-25: Task assignment networks of the three organisations. Blue spheres represent agents while diamonds represent tasks. Grey colour links represent task assignments while the brown ones represent task dependencies. Link width and colour correspond to the  $ADT(a_i, t_p)$  metric scores where thicker and darker links represent larger metric values. Nodes have been sized proportionately to the largest  $ADT(a_i, t_p)$  risk value they are associated with.



(i) Task *AP-Inv*, agents assigned to the task and (ii) Task *AP-pay*, agents assigned to the task and related other tasks



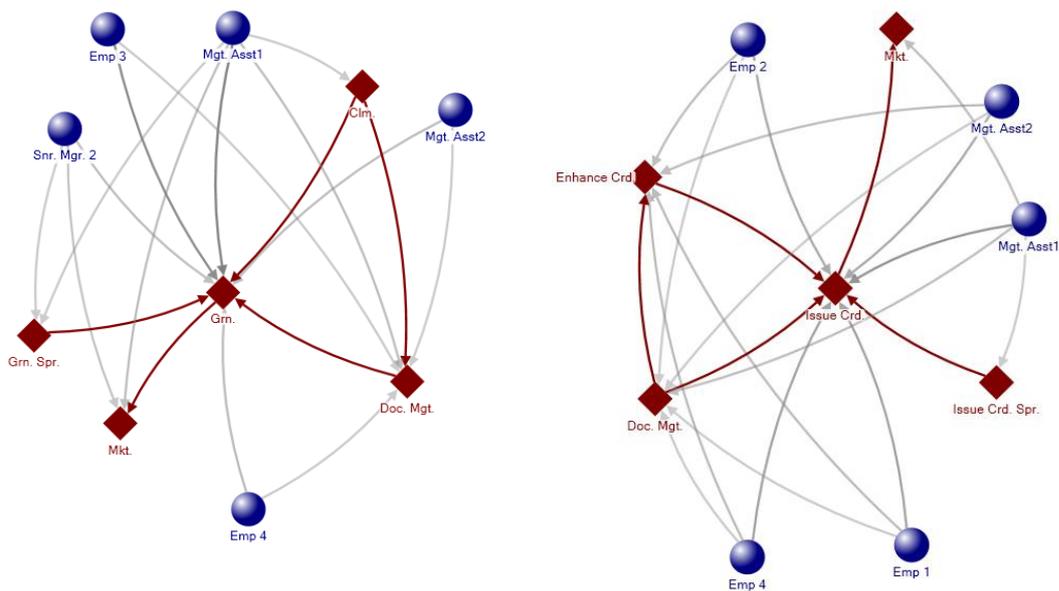
(iii) Task *CM-B*, agents assigned to the task and related other tasks



Figure 6-26: Selected sub-networks of Organisation-1 illustrating task assignment and task dependency links related to the tasks (i) *AP-Inv* (ii) *AP-Pay* and (iii) *CM-B*. Task assignment links appear in grey while task dependency links are brown. In the sub-networks, agents who are also assigned to tasks that depend on the focal task are coloured in blue. The agents who are not assigned to depending tasks of the focal task appear in grey.

Figure 6-26 (i) shows that there are three tasks – *AP-Pay*, *AP-Inv-App* and *FA-As* that depend on the task *AP-Inv*. All agents assigned to *AP-Inv* with the exception of two (nodes

coloured in grey) have also been assigned to at least one of its depending tasks. Organisation-1 should review these dependent task assignments to decide if they create any conflicts of interest. Out of these dependent task assignments, agent *S.Ex2* is allowed to perform both the task *AP-Inv* (*Accounts Payable –Invoicing*) and its supervisory task *AP-Inv-App*. This essentially allows *S.Ex2* to self-manage *AP-Inv* task without any separation of duty. Therefore, the organisation should at least implement dynamic separation of duty requirements for this task so that only one task out of *AP-Inv* and *AP-Inv-App* can be performed by the agent with respect to a specific invoice. Similar dependent task assignments can be observed in relation to the tasks *AP-Pay* and *CM-B*, whose sub-networks are shown in Figure 6-26 (ii) and (iii) respectively. According to Figure 6-23 (ii), the two columns corresponding to tasks *Grn.* and *Issue Crd.* have many cells containing colours associated with higher risk values indicating high dependent task assignment risks related to these two tasks in Organisation-2. Figure 6-27 illustrates the sub-networks containing task assignment and task dependency links related to these two nodes. Links in Figure 6-27 (i) and (ii) reveal that all agents assigned to the tasks *Grn.* and *Issue Crd.* also perform at least one other dependent task. As in the case of Organisation-1, these dependent task assignments must be reviewed by Organisation-2 to ensure that no conflict of interest occurs due them.

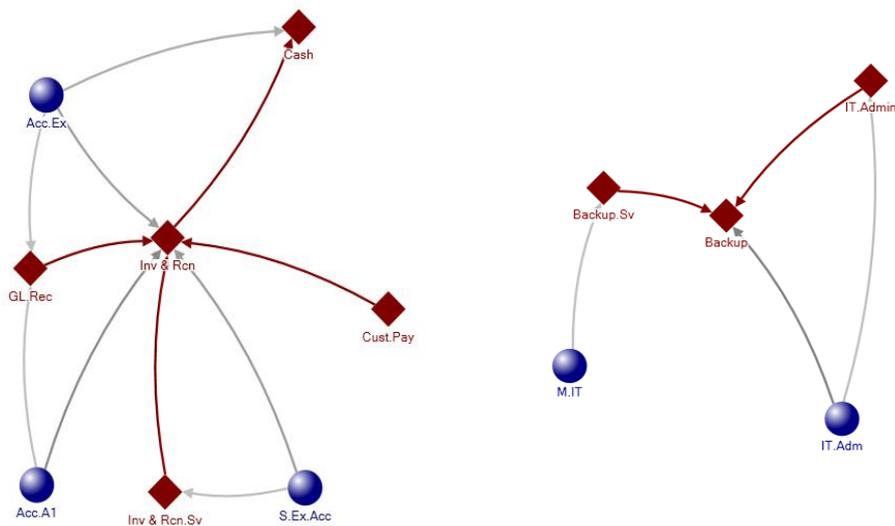


(i) Task *Grn*, agents assigned to the task and related other tasks

(ii) Task *Issue Crd.*, agents assigned to the task and related other tasks

Figure 6-27: Selected sub-networks of Organisation-2 illustrating task assignment and task dependency links related to the tasks (i) *Grn* and (ii) *Issue Crd.* Spheres represent agents while diamonds represent tasks. Task assignment links appear in grey while task dependency links are brown.

The column corresponding to the task - *Inv & Rcn* in the heat-map in Figure 6-24 has several cells containing colours associated with higher risk values. The task assignments and task dependencies related to *Inv & Rcn* are visualised in Figure 6-28 (i). According to the sub-network in the figure, the tasks *GL.Rec*, *Cust.Pay* and *Inv & Rcn.Sv* depend on the task *Inv.Rcn*. The three agents who have been assigned to the task - *Inv.Rcn* are also assigned to one of its depending tasks resulting in a non-zero  $ADT(a_i, t_p)$  metric value. However, according to the heat-map in Figure 6-24, the highest dependent task assignment risk in Organisation-3 occurs due to the task assignment *IT.Adm*→*Backup* (The corresponding cell in the heat-map is coloured in red). Figure 6-28 (ii) illustrates the task assignments and dependencies related to the task *Backup*. The task relationship *IT.Adm*→*Backup* (task *Backup* corresponds to backing up the database) scores high value since the only other task assigned to the same agent – *IT.Admin* (corresponds to IT system administration tasks) depends on the task *Backup*. A single agent being responsible for both the data and the backup of the data can lead to loss of availability of both in an insider threat event. Nevertheless, in the case of Organisation-3, this risk is mitigated to an extent since another agent (*M.IT*) supervises the backup task as shown in Figure 6-28 (ii) (Note that agent *M.IT* is assigned to the task labelled *Backup.Sv* which denotes supervision of the creation, testing and storage of backups).



(i) Task *Inv & Rcn*, agents assigned to the task and related other tasks      (ii) Task *Backup*, agents assigned to the task and related other tasks

Figure 6-28: Selected sub-networks of Organisation-3 illustrating task assignment and task dependency links related to the tasks (i) *Inv & Rcn* and (ii) *Backup*. Spheres represent agents while diamonds represent tasks. Task assignment links appear in grey while task dependency links are brown.

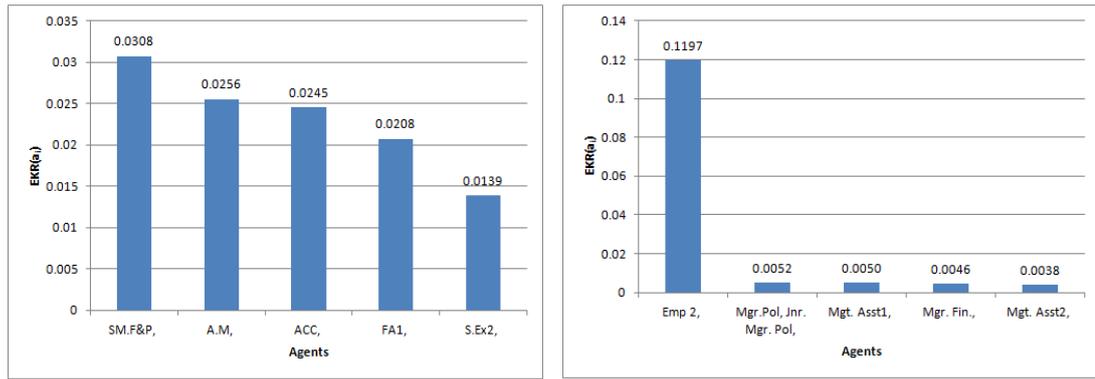
## 6.4 Assessment of risks due to knowledge requirements

Two types of security risks that occur due to knowledge requirements of information resources and tasks have been listed in Table 5-6 in Chapter 5. The next two sub-topics present the results of the assessment of risks occurring due to knowledge requirements in the three organisations analysed in this research.

### 6.4.1 Risks due to agents having exclusive knowledge to operate an information resource

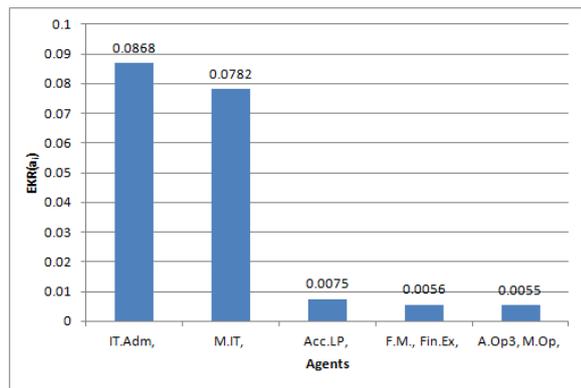
Agents having exclusive knowledge with respect to a resource can compromise the availability, integrity and confidentiality of that resource with minimum chance of being detected. The EKR metrics defined in section 5.5.1 can be used to assess and quantify the risks due to agents holding exclusive knowledge by considering three criteria – the extent to which an agent exclusively holds knowledge required to use an information resource, the intrinsic risk characteristics of the agent and the sensitivity or criticality of the resource. The EKR metrics can be calculated per agent –  $EKR(a_i)$  and resource access authorisation –  $EKR(a_i, r_j)$ . Figure 6-29 presents the  $EKR(a_i)$  values of the agents receiving the top-five metric scores in each organisation.

According to Figure 6-29, although the agent - *SM.F&P* receives the highest  $EKR(a_i)$  risk score in Organisation-1, the difference between risks of individual agents is minimal and the decrease in metric scores from the highest to the lowest is a gradual one. Furthermore, the highest risk scores in Organisation-1 are much lower than that of the other two organisations. On the other hand, graphs for Organisation 2 and 3 are characterised by one or two agents receiving contrastingly high risk scores. Agent *Emp 2* Organisation-2 obtains a metric score which is strikingly high while the same can be observed for the metric scores of the two agents – *IT.Adm* and *M.IT* in Organisation-3. All three agents *Emp 2*, *IT.Adm* and *M.IT* are IT systems administrators or managers in their organisations. It must be noted that IT managers and system administrators are not included in the data collected from Organisation-1. However, in the case of Organisations 2 and 3 it is clear that information system owners and custodians cause high  $EKR(a_i)$  risks.



(i) Organisation - 1

(ii) Organisation - 2

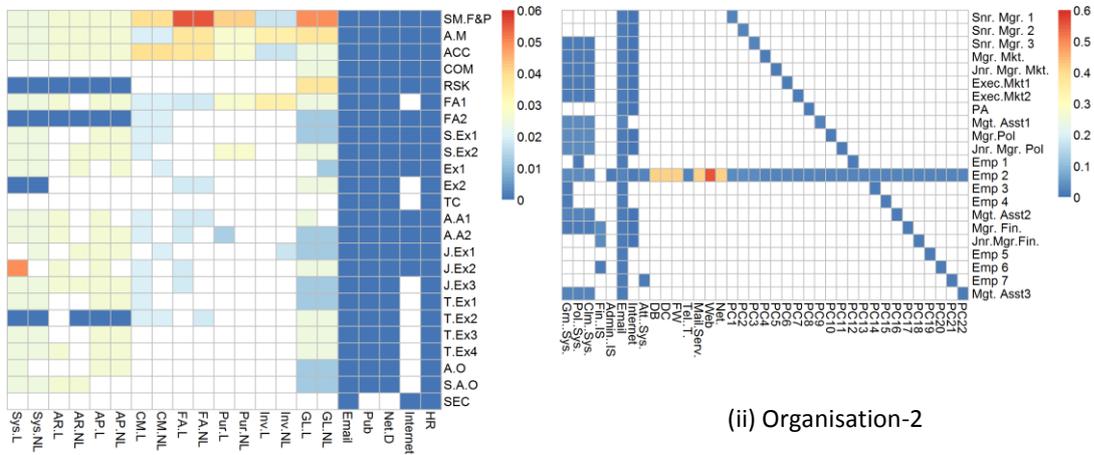


(iii) Organisation - 3

Figure 6-29: Top-five EKR(a) risk values of the agents in organisations 1,2 and 3.

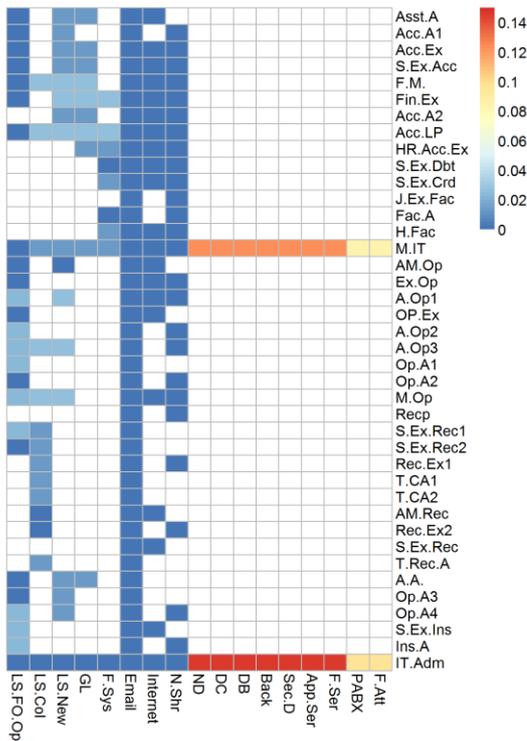
The resource access authorisations that carry high risks due to agents having exclusive knowledge with respect to a resource can be analysed using the  $EKR(a_i, r_j)$  metric. Heat-maps in Figure 6-30 depict the risks due to agents having exclusive knowledge to utilise resources of Organisations 1, 2 and 3. Rows represent agents while columns represent resources. Cell colours represent the  $EKR(a_i, r_j)$  risk scores of resource authorisations, where the highest risks are indicated by red and lowest risks are indicated by dark blue (refer the legend for a numerical comparison. Note that the scales differ in three organisations and colours cannot be used to compare risks across them). White cells indicate that the corresponding agent is not authorised to access the given resource. The network diagrams in Figure 6-31, which represent the Agent  $\rightarrow$  Resource, Agent  $\rightarrow$  Knowledge and Resource  $\rightarrow$  Knowledge networks of the three organisations, also highlight the resource access authorisations that receive high  $EKR(a_i, r_j)$  risks. Blue spheres in the network diagrams represent agents, triangles represent resources and squares represent knowledge. Resource access links with high  $EKR(a_i, r_j)$  scores are indicated by thicker and

darker links. Agent and Resource nodes have also been sized proportionately to the highest  $EKR(a_i, r_j)$  metric score they are associated with.



(i) Organisation-1

(ii) Organisation-2



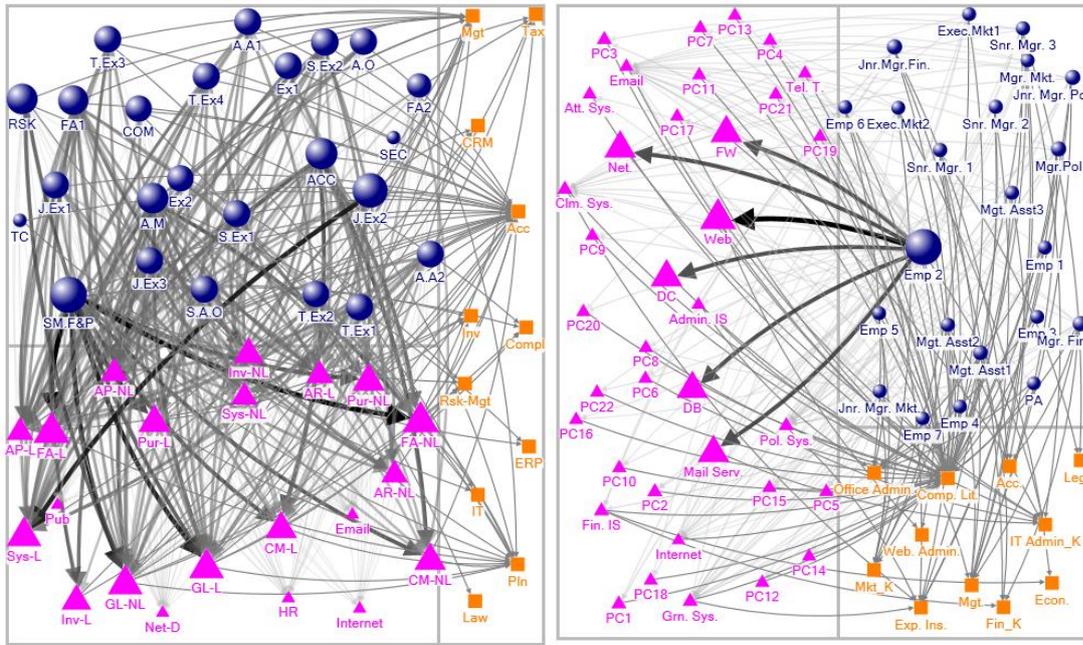
(iii) Organisation – 3

Figure 6-30: Heat-map representations of the risks due to agents having exclusive knowledge to utilise resources of Organisations 1, 2 and 3. Rows represent agents while columns represent resources. Cell colours represent the  $EKR(a_i, r_j)$  risk scores of resource authorisations where the highest risks are indicated by red and lowest risks are indicated by dark blue (refer the legend for a numerical comparison). Note that the scales differ in three organisations and colours cannot be used to compare risks across them). White cells indicate that the corresponding agent is not authorised to access the given resource.

As illustrated in Figure 6-30(i), many access authorisations with significant  $EKR(a_i, r_j)$  risks in Organisation-1 are associated with agents *SM.F&P*, *A.M*, *ACC*, *FA1*, and *S.Ex2*. These agents also receive the top-five  $EKR(a_i)$  metric scores in the same organisation. At the same time, there are many access authorisations with non-zero risk scores in Organisation-1. This can be clearly observed in the network diagram presented in Figure 6-31(i) where there are many thick, dark resource access links indicating higher risk scores associated with them. In contrast to Organisation-1, most resource access authorisations in Organisations 2 and 3 receive very low  $EKR(a_i, r_j)$  risk scores as shown by many dark blue cells in Figure 6-30 (ii) and (iii). In Organisation-2, access authorisations with a high risk occur in relation to the agent *Emp 2* accessing network and security devices (*FW*, *Net.*, *DC*, *DB*, *Web* and *Mail Serv.*). This is further illustrated in the network diagram in Figure 6-31(ii) where the relevant links are conspicuous among the others. The same pattern can be observed for Organisation -3, where the two agents *M.IT* and *IT.Adm* are associated with the access authorisations receiving high  $EKR(a_i, r_j)$  metric scores. The access authorisations of Organisation 2 and 3 that receive high scores are illustrated in the sub-networks given in Figure 6-32, which show Agent  $\rightarrow$  Resource, Agent  $\rightarrow$  Knowledge and Resource  $\rightarrow$  Knowledge links. There are six resource access authorisations shown in Figure 6-32(i) - *Emp 2* $\rightarrow$ *FW*, *Emp 2* $\rightarrow$ *Net.*, *Emp 2* $\rightarrow$ *DC*, *Emp 2* $\rightarrow$ *DB*, *Emp 2* $\rightarrow$ *Web* and *Emp 2* $\rightarrow$ *Mail Serv.* and their  $EKR(a_i, r_j)$  risk scores are shown on the links.

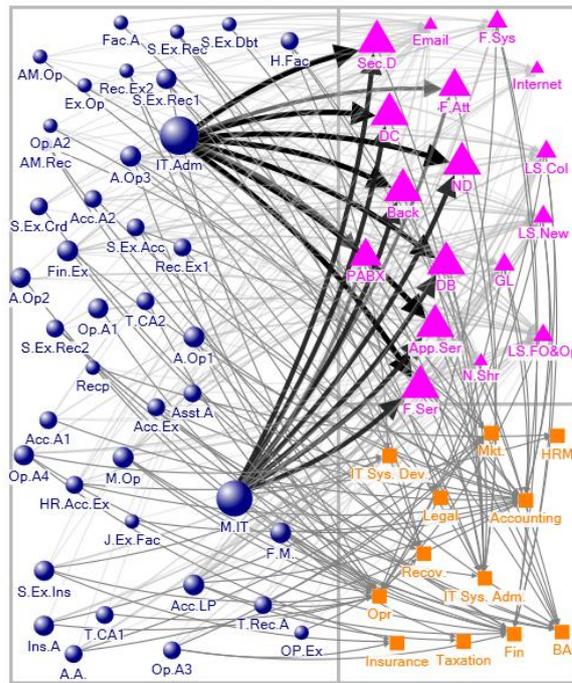
The six resources in the access relationships seen in Figure 6-32(i) require the knowledge - *IT Admin\_K* (IT systems administration) while the resource *Web* (Web server and company website) additionally requires the knowledge *Web. Admin* (website administration). There are two agents possessing the knowledge - *IT Admin\_K* while only *Emp 2* knows *Web. Admin*. Out of the resource access links, *Emp 2* $\rightarrow$ *Web* has a higher risk score (0.556) than the others (0.417). This is due to the fact that *Emp 2* has a greater proportion of agent-knowledge pairs required for *Web* than for the other five resources.

Similarly, Figure 6-32(ii) illustrates the resource access relationships that score the highest  $EKR(a_i, r_j)$  values in Organisation-3. Although four agents have the required knowledge - *IT Sys.Adm* (IT systems administration) to operate the resources shown in the diagram, only two are given access. The risk scores of access links originating from the agent - *IT.Adm* is slightly higher (0.146) than those originating from *M.IT* (0.125). This difference occurs since *IT.Adm* has a higher composite risk attribute value than that of *M.IT* ( $C_a(IT.Adm) > C_a(M.IT)$  since *IT.Adm* is an external contractor).



(i) Organisation-1

(ii) Organisation-2



(iii) Organisation – 3



Figure 6-31: Network diagrams representing Agent → Resource, Agent → Knowledge and Resource → Knowledge networks of the three organisations. Blue spheres represent agents, triangles represent resources and squares represent knowledge. Resource access links with high  $EKR(a_i, r_j)$  scores are indicated by thicker and darker links. Agent and Resource nodes have been sized proportionately to the highest  $EKR(a_i, r_j)$  metric score they are associated with.

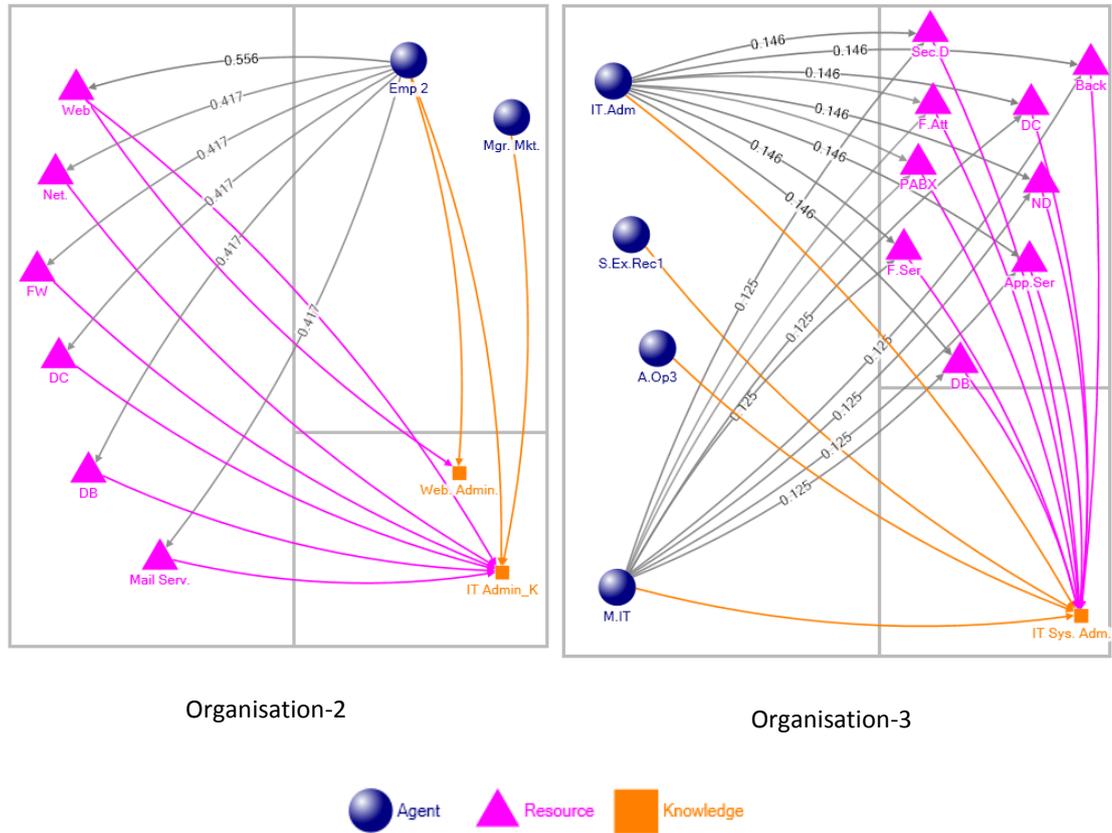


Figure 6-32: The sub-networks visualising the resource access relationships that score high  $EKR(a_i, r_j)$  scores in Organisations 2 and 3. The networks show Agent→Resource (indicated in grey), Agent→Knowledge (indicated in yellow) and Resource→Knowledge (indicated in pink) links. The  $EKR(a_i, r_j)$  metric score is stated on the resource access links.

### 6.4.2 Risks due to agents having exclusive knowledge to perform a task

Exclusive knowledge possessed by agents with respect to a task can lead to insider threat events. If such exclusive knowledge is used to carry out fraud, sabotage or theft of information, it will be difficult for an organisation to either prevent or detect such attempts. The EKT metrics defined in 5.5.2 enables the analysis and quantification of risks due to agents having exclusive knowledge related to tasks by considering three criteria – the extent to which agent holds exclusive knowledge related to a task, the intrinsic risk characteristics of an agent and the criticality of the task. The EKT metrics can be calculated per agent –  $EKT(a_i)$  and task assignment –  $EKT(a_i, t_p)$ . Figure 6-33 lists the agents who receive the top-ten  $EKT(a_i)$  values in the three organisations.

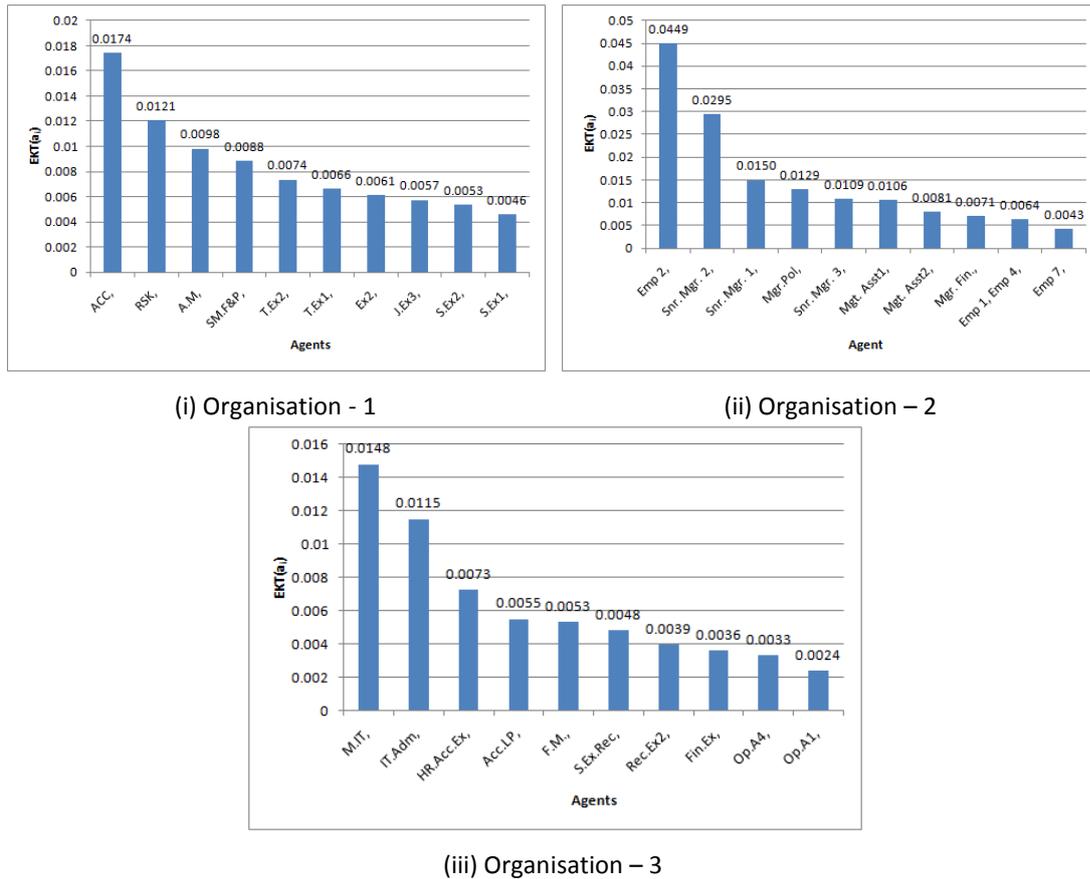
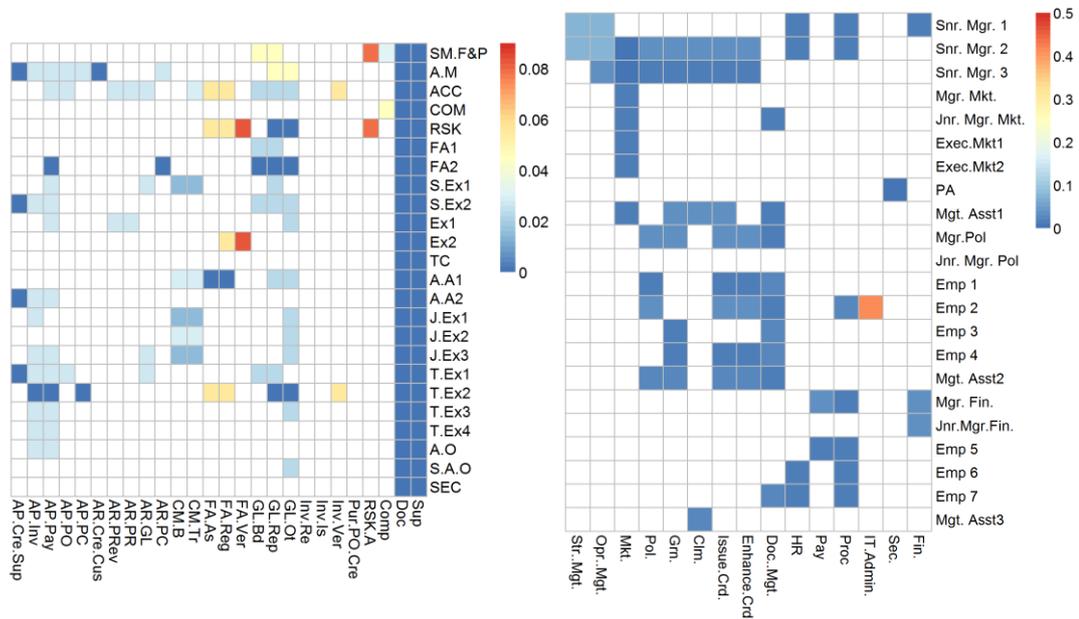


Figure 6-33: Top-ten EKT(a<sub>i</sub>) risk values of the agents in organisations 1,2 and 3.

In Organisation-1, agent – ACC receives the highest metric value. The EKT(a<sub>i</sub>) risk scores in Organisation-1 shows a gradual decrease from this agent to the lowest. On the other hand, two agents labelled – Emp 2 and Snr. Mgr. 2 in Organisation-2 receives distinctly high scores than the others in the same company. A similar pattern can be observed for Organisation-3, where the two agents – M.IT and IT.Adm score risk values that are significantly higher than their co-workers.

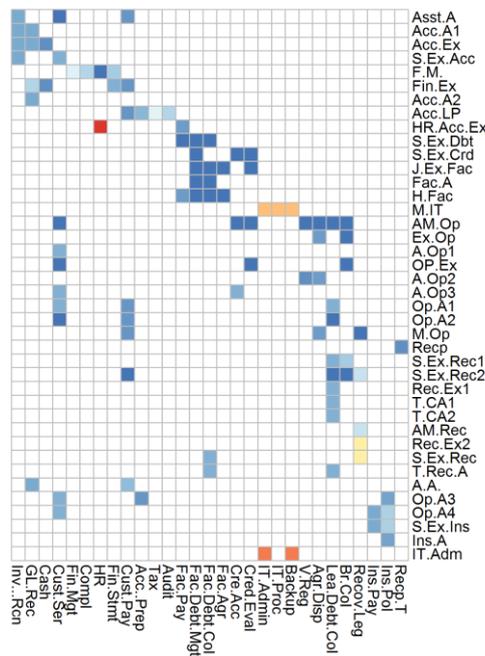
The EKT(a<sub>i</sub>,t<sub>p</sub>) metric enables the analysis of individual task assignments that cause high risks due to agents possessing exclusive knowledge related to them. Figure 6-34 shows heat-map representations of EKT(a<sub>i</sub>,t<sub>p</sub>) risks of the task assignments of three organisations. In the heat-maps, rows represent agents while columns represent tasks. Cell colours represent the EKT(a<sub>i</sub>,t<sub>p</sub>) risk scores of task assignments where the highest risks are indicated by red and lowest risks are indicated by dark blue (refer the legend for a numerical comparison). Note that the scales differ in three organisations and colours cannot be used to compare risks across them). White cells indicate that the corresponding agent is not assigned for the given task. The same results are depicted using network diagrams in Figure 6-35, which represent Agent → Task, Agent → Knowledge and Task → Knowledge networks

of the three organisations. In the network diagrams, blue spheres represent agents, diamonds represent tasks and squares represent knowledge. Task assignment links with high  $EKT(a_i, t_p)$  scores are indicated by thicker and darker links. Agent and task nodes have been sized proportionately to the highest  $EKT(a_i, t_p)$  metric score they are associated with.



(i) Organisation-1

(ii) Organisation-2



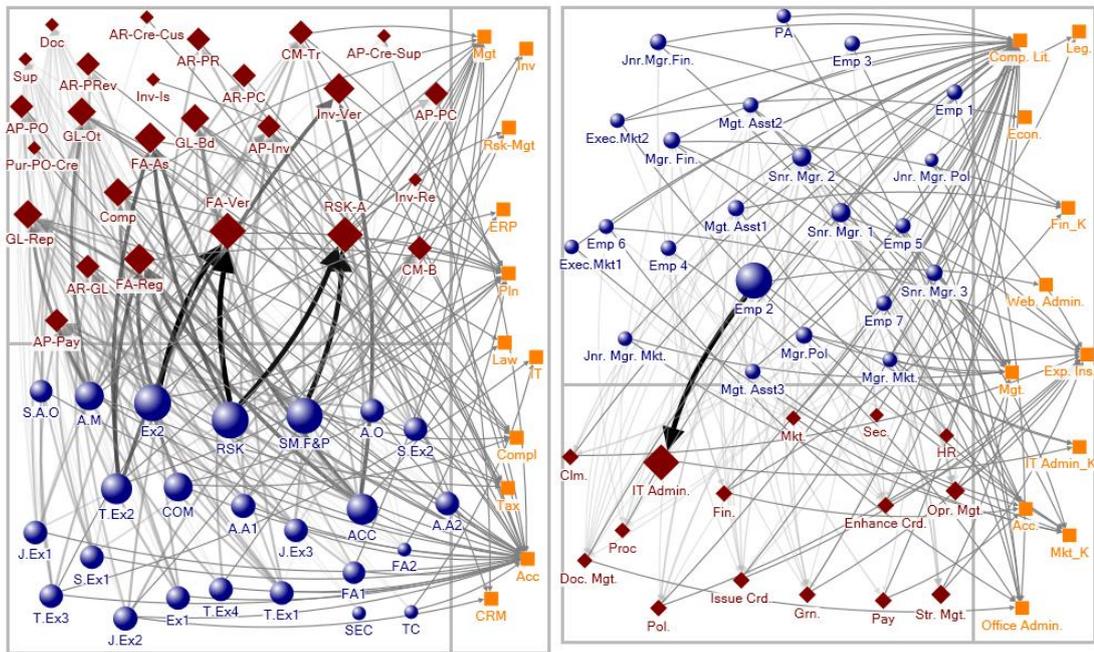
(iii) Organisation – 3

Figure 6-34: Heat-map representations of the risks due to agents having exclusive knowledge to perform tasks of Organisations 1, 2 and 3. Rows represent agents while columns represent tasks. Cell colours represent the  $EKT(a_i, t_p)$  risk scores of task assignments where the highest risks are indicated by red and lowest risks are indicated by dark blue (refer the legend for a numerical comparison). Note that the scales differ in three organisations and colours cannot be used to compare risks across them). White cells indicate that the corresponding agent is not assigned for the given task.

With regards to Organisation-1, Figure 6-34(i) shows that all the task assignments related to the agent – ACC, have non-zero  $EKT(a_i, t_p)$  risk values. Note that the same agent obtains the highest agent centric risk score –  $EKT(a_i)$  in the company. However, the task assignments that have the highest  $EKT(a_i, t_p)$  risk scores in Organisation-1 occur in relation to tasks *FA.Ver* and *RSK.A* as indicated by the red cells in corresponding columns of the heat-map. This can be also observed in the network in Figure 6-35(i), where the thicker and darker links terminate at the two resources. Figure 6-36(i) presents the refined sub-network, which only shows the task assignments that receive the highest metric values in Organisation-1. According to the figure, performing task - *FA-Ver* requires knowledge – *Pln*. and four agents possess this knowledge. On the other hand, the task –*RISK-A* requires three different types of knowledge – *Pln*, *Inv* and *Mgt*. The total number of agents having these three types of knowledge is much greater than four. Therefore, metric scores for the task assignments *SM.F&P*→*RSK-A* and *RSK*→*RSK-A* are lower (0.079) than that for the task assignments *RSK*→*FA-Ver* and *Ex2*→*FA-Ver* (0.083). Also note that the three agents *SM.F&P*, *RSK* and *Ex2* have the same composite risk attribute value and no metric variations occur due to intrinsic agent risk in this case.

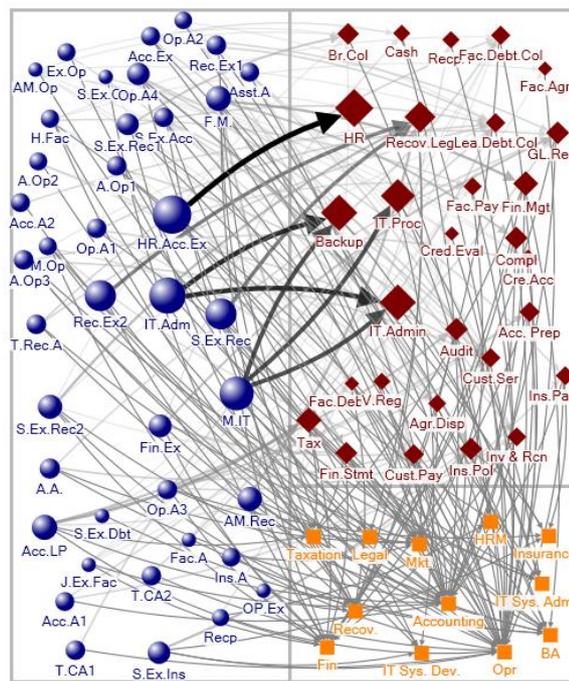
According to the heat-map in Figure 6-34(ii), task assignment - *Emp 2*→*IT Admin.* in Organisation-2 has a significantly higher risk when compared with other task assignments of the same company. This can also be observed in the network in Figure 6-35(ii). The refined sub-network in Figure 6-36(ii) confirms that the task *IT Admin.* (IT systems administration) requires knowledge – *IT Admin\_K*. There are only two agents possessing this knowledge in the organisation and out of them only *Emp 2* has been assigned for the task. The exclusivity of the knowledge required for the task - *IT Admin.* results in a very high metric value for the task assignment *Emp 2*→*IT Admin* in Organisation-2.

Figure 6-34(iii) represents a heat-map of  $EKT(a_i, t_p)$  risk scores of Organisation-3. According to the heat-map, task assignments *HR.Acc.Ex*→*HR*, *IT.Adm*→*IT.Admin*, *IT.Adm*→*Backup*, *M.IT*→*IT.Admin*, *M.IT*→*IT.Proc* and *M.IT*→*Backup* carry significant risks. The corresponding links are also highlighted in the network diagram in Figure 6-35(iii). According to the refined sub-network shown in Figure 6-36(iii), performing the task *HR* requires knowledge *HRM*. Since only two agents possess this knowledge, task assignment *HR.Acc.Ex*→*HR* receives the highest  $EKT(a_i, t_p)$  score in Organisation-3 (risk value of 0.167). The variation in the risk scores of the other task assignments occurs due to the higher composite agent risk attribute value of *IT.Adm*.



(i) Organisation-1

(ii) Organisation-2



Organisation – 3



Figure 6-35: Network diagrams representing Agent → Task, Agent → Knowledge and Task → Knowledge networks of the three organisations. Blue spheres represent agents, diamonds represent tasks and squares represent knowledge. Task assignment links with high  $EKT(a_i, t_p)$  scores are indicated by thicker and darker links. Agent and task nodes have been sized proportionately to the highest  $EKT(a_i, t_p)$  metric score they are associated with.

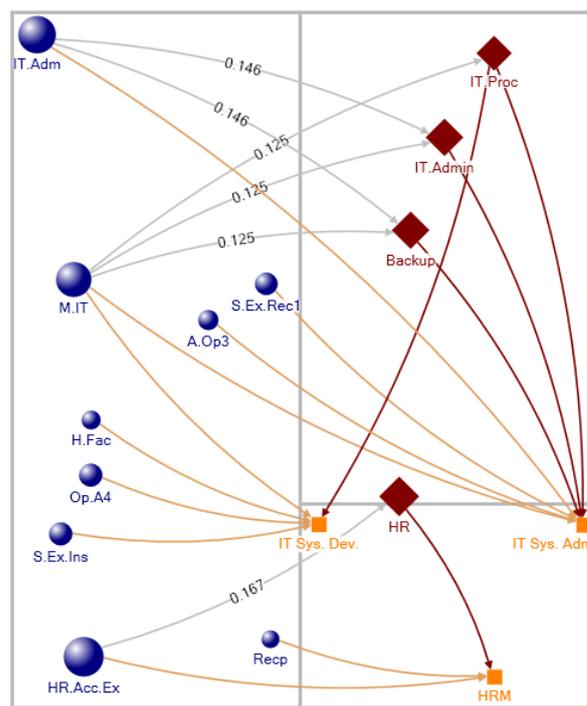
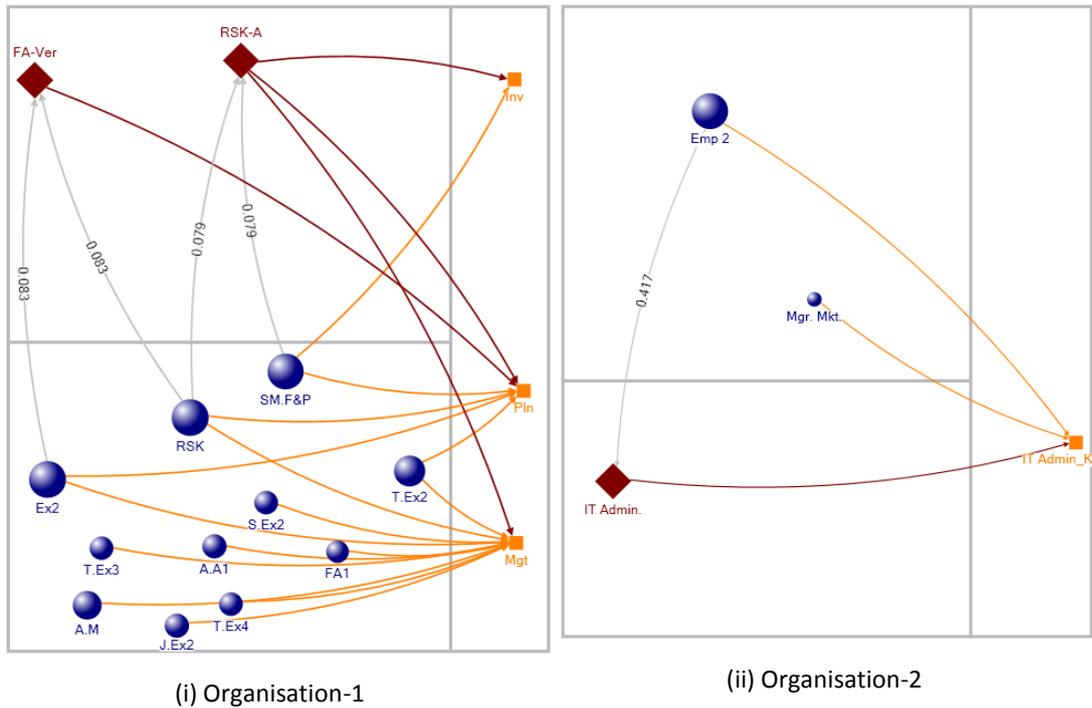


Figure 6-36: The sub-networks visualising the task assignments that score high  $EKT(a_i, t_p)$  scores in the three Organisations. The networks show Agent→Task (indicated in grey), Agent→Knowledge (indicated in yellow) and Task→Knowledge (indicated in brown) links. The  $EKT(a_i, t_p)$  metric scores are stated on the task assignment links.

## 6.5 Assessment of risks due to social relationships combined with resource authorisations or task assignments

Table 5-7 in chapter 5 lists five types of security risks that occur due to social relationships combined with the resource authorisations or task assignments in an organisation. The metrics developed to quantify these risks are also given in the same chapter. Since the metrics do not restrict the types of social relationships that can be used, analysts are free to select the types that are important in their organisational contexts. In this research, data on four types of social relationships have been collected creating four separate social networks per organisation. These four types of social networks are:

1. Formal Reporting Network: Network based on the formal organisational hierarchy (Who reports to whom?).
2. Advice Network: Network based on giving/receiving advice on work related matters. (Who advises whom?)
3. Information Exchange Network: Network based on people exchanging information with each other. (Who exchanges information with whom?)
4. Friendship Network: Network based on friendships between individuals. (Who is a friend of whom?)

These four types of social networks have different properties and applicability in relation to the metrics as summarised in Table 6-1.

The formal reporting network is based on the organisational hierarchy of the organisation. All links in this network can be included in the analysis since they are well documented with very high reliability assuming that the organisational chart of a company is up to date. Naturally, all links in the formal reporting network are directional and the direction is drawn from supervisor to subordinate. In terms of applicability in calculating different types of risks, the formal reporting relationships can be used as inputs to the IAC, TAR and TAT metrics. As pointed out in prior research (Astley and Sachdeva 1984; Brass 1984; Brass and Burkhardt 1993) hierarchical relationships are sources of power and influence. Therefore, they can be used to obtain indirect and transient access through social networks, which is the primary contributing factor for the risks assessed using the three metrics mentioned above. The importance of including the formal reporting

relationships are further emphasized by the real insider threat case numbers 29 and 37 listed in Table 4-1, where insiders have used their power and influence to obtain unauthorised access. On the other hand, there is no evidence to suggest that hierarchical relationships play any role in forming highly connected groups or cliques in organisations. Therefore, formal reporting relationships are not used in the calculation of ACR and ACT metrics.

Table 6-1: The properties and applicability of social networks to each risk type

		Type of Social Network			
		Formal Reporting	Advice	Information Exchange	Friendship
<b>Nature of relationship</b>		Formal only	Both formal and informal		Informal only
<b>Directionality</b>		Unidirectional		Bidirectional	
<b>Strength of links included</b>		All links included	Only strong links included in analysis		
<b>Applicability</b>	<b>Indirect access to resources (IAC)</b>	Applicable			
	<b>Transitive access to dependent resources (TAR)</b>	Applicable			
	<b>Transitive assignment of dependent tasks (TAT)</b>	Applicable			
	<b>Close group controlling a resource (ACR)</b>	Not Applicable		Applicable	
	<b>Close group performing a task (ACT)</b>	Not Applicable		Applicable	

Similar to the formal reporting networks, advice networks also contain unidirectional relationships (Gibbons 2004; Krackhardt 1990). In this research, directionality is drawn from the advisor to the person who is seeking advice. At the same time, work-related advice relationships can include both formal (as described in the organisational hierarchy) and informal ties. While agents can seek work-related advice from their supervisors, they are also free to consult other employees. Since the data on advice networks have been self-reported by the participants, data reliability must be ensured. In order to increase the reliability, only strong ties reflecting very regular advice seeking relationships have been included in metric calculations. According to Marsden (1990) social network data is more reliable in the case of strong ties as opposed to weak ones. Furthermore, previous research

(Granovetter 1983; Granovetter 1973; Krackhardt 1992; Nelson 1989) indicate that strong social relationships carry more power to influence decision making while weak ones are important in diffusion of information. Since the metrics developed in this research focus on aspects such as obtaining indirect and transient access instead of diffusion of information, only including strong social relationships is further justified. The research literature also provides some guidelines on the selection criteria for the strong links. According to the seminal paper by Granovetter (1973), strength of a social network link is a function of four factors – amount of time spent together (can be interpreted as frequency of interaction as well), emotional intensity of the connection, intimacy and reciprocity. Krackhardt (1992) defines a strong friendship (*philos* is the term used in his paper) as one which fulfils three conditions – there should be regular interaction among the agents, they must feel affection towards each other and they must have interacted for a considerable amount of time. Although there is no empirical evidence to suggest that the same guidelines apply for investigations focusing on socio-technical aspects of information systems security, similar criteria have been adopted in this research. Thus a strong advice relationship is defined as a one where either party has indicated it as his primary advice relationship or reflecting at least regular (weekly or more frequently) advice related interaction. Moreover, the advice relationship must be acknowledged by the other party at least in a weak sense (interaction less regular than weekly). In terms of applicability, advice relationships can be used as inputs for calculating the IAC, TAR and TAT metrics since advice networks are sources of power, especially under normal operational conditions of an organisation as pointed out by Krackhardt (1992). This also implies that they are not applicable in the calculation of the ACR and ACT metrics as in the case of formal reporting networks.

The third type of social relationship data collected creates the information exchange networks. Previous research suggests that information exchange can be both formal and informal (Haythornthwaite 1996), which is also the stance taken in this research. Also, researchers have recognised the opportunities for information exchange provided by multiple modes of communication (Haythornthwaite and Wellman 1998). Since the data collected in this research include multiple information exchange modes and the directionality of some of them can be ambiguous (for example, face-to-face meetings or discussions), information exchange is modelled as an undirected relationship. As in the case of advice networks, only strong information exchange links are included for reliability and relevance. A strong link in this case is defined as a reported exchange of information between two agents with a weekly frequency or better that is corroborated by a

reciprocated link of any frequency. Prior research suggests that information exchange relationships facilitate collaboration (Haythornthwaite and Wellman 1998; Cho et al. 2007) as well as power and influence (Brass and Burkhardt 1993). Therefore, in addition to the three metrics - IAC, TAR, TAT, information exchange networks can also be used to calculate ACR and ACT scores.

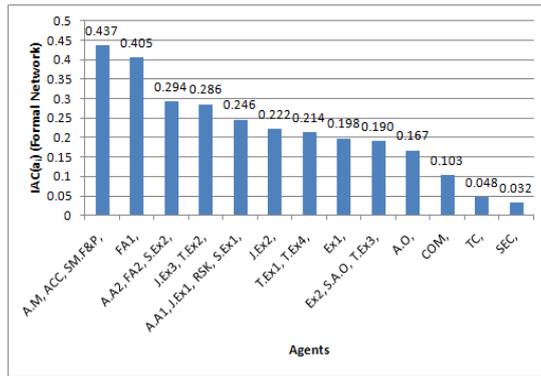
The fourth type of social network data collected creates the friendship networks. Friendship networks are always informal since they are not mandated by the organisations (Wiseman 1986). As in the case of advice and information networks this research only considers strong friendship associations in order to maintain reliability and relevance. Strong friendship links will be stable associations providing more power and influence over the individuals participating in them. A strong friendship in this research is defined as a relationship where either party identifies the other as one of his better or closest friends. As an additional condition, a strong friendship must be a reciprocated one at least in a weak sense (agent reciprocating must at least like the other party). In terms of the directionality, some researchers have considered friendship ties as directional (Gibbons 2004; Haythornthwaite and Wellman 1998) while others have treated them as undirected (Lincoln and Jon 1979). Their choice is motivated by their research objectives. Since this research focus on strong friendships, it is assumed that they are stable and mutual. As a result, friendship links are treated as undirected in the analysis. There is evidence from previous research that in addition to mutuality, friendship relationships can be sources of power and influence (Brass 1984; Gibbons 2004). Hence, similarly to the information exchange relationships, friendship links are used in the calculation of all five metrics – IAC, TAR, TAT, ACR and ACT.

The next five sub-topics presents the results of the assessment of socio-technical risks that occur due to social relationships combined with the resource authorisations or task assignments in an organisation.

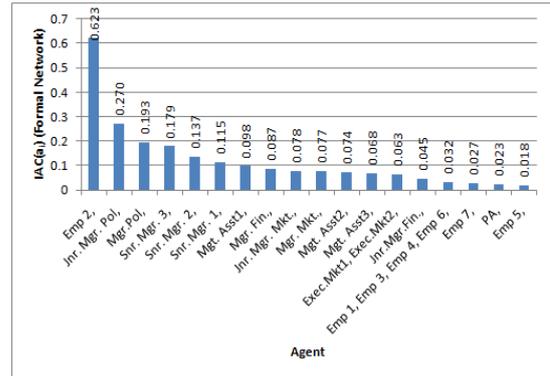
## **6.5.2 Risks due to agents having indirect access to information resources**

### **Indirect access through the formal reporting structure of organisations**

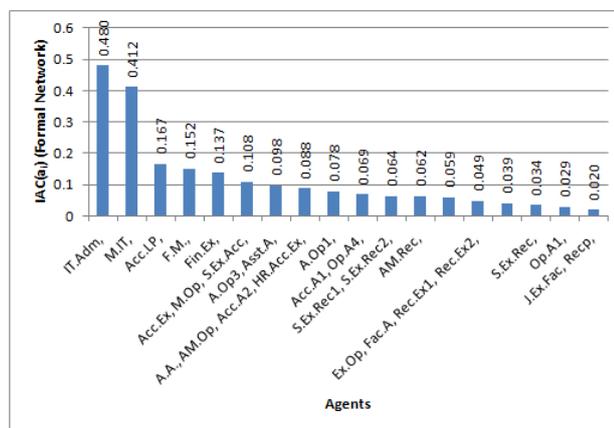
An agents' overall capability to access information resources either through direct authorisation or by utilising the social networks can be quantified using the IAC metric. Figure 6-37 presents the  $IAC(a_i)$  values of the agents in the three organisations calculated using the formal reporting structure.



(i) Organisation - 1



(ii) Organisation - 2



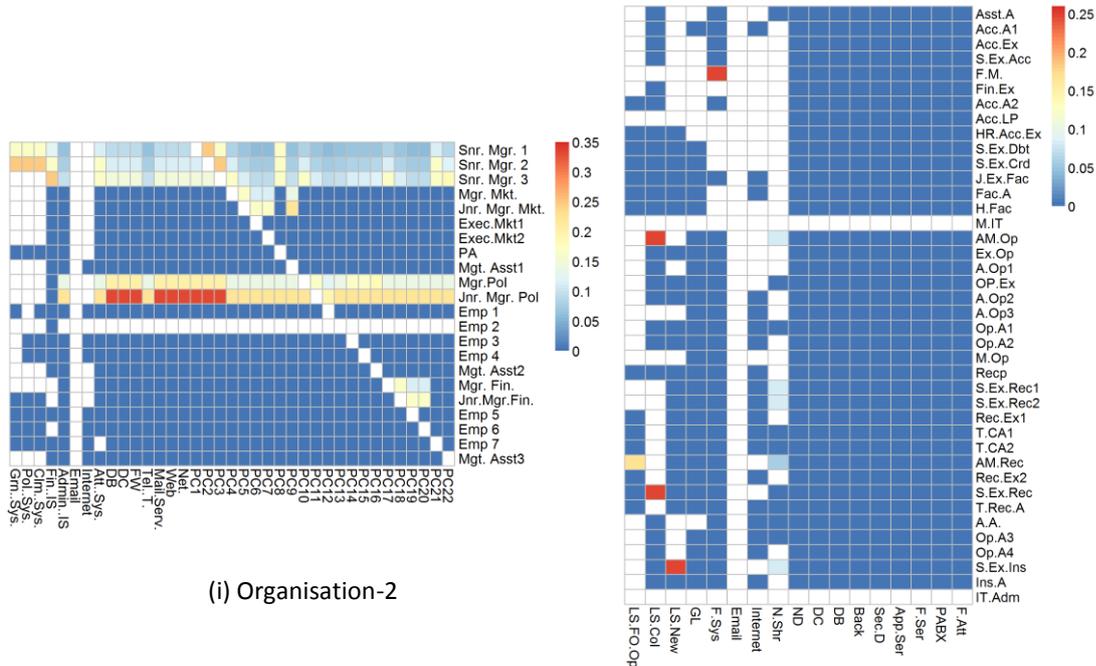
(iii) Organisation - 3

Figure 6-37: IAC(a<sub>i</sub>) metric scores of the agents in three organisations calculated using the formal reporting relationships

In all three organisations the agents who receive the highest metric scores have direct access to many information resources. Since the shortest possible path to an information resource occurs when an agent has direct access to it, people having numerous direct authorisations tend to receive high risk scores. In fact, in Organisation-1 no agent obtains indirect access to information resources through the formal organisational relationships and the metric values purely reflect the authorisations granted to the agents.

The access capabilities of agents with respect to each resource can be quantified using the IAC(a<sub>i</sub>, r<sub>j</sub>) metric. Figure 6-38 provides heat-map representations of IAC(a<sub>i</sub>, r<sub>j</sub>) risk scores for all agent resource combinations of the three organisations. In the heat-maps, dark blue cells reflect cells with either zero or very low risk scores while the red cells reflect high scores (refer the legend for a numerical comparison). White cells indicate agents having

direct access to the corresponding information resources. From Figure 6-38(i), it is clear that the three agents - *Snr. Mgr. 1*, *Snr. Mgr. 2* and *Snr. Mgr. 3* have indirect access to many resources. However, this can be expected through the formal reporting links of a hierarchical organisation since the three agents occupy senior management positions having authority over many employees.



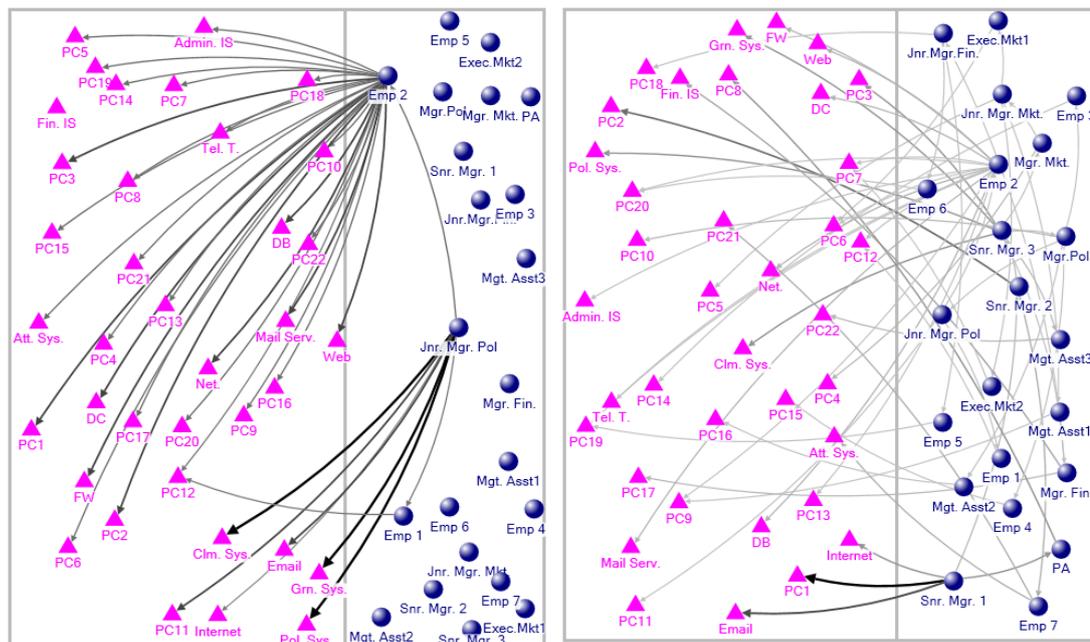
(i) Organisation-2

(ii) Organisation-3

Figure 6-38: Heat-map representations of the  $IAC(a_i, r_j)$  scores of all agent, resource combinations in Organisations 2 and 3 calculated considering the formal reporting relationships. Rows represent agents while columns represent information resources. The cell colour reflects the metric score where dark blue represents very low scores and red represents high scores. White cells indicate agents having direct authorisations to access the corresponding resources.

On the other hand, highest indirect access risks (indicated by red and orange cells in Figure 6-38 (i)) in Organisation-2 are associated with the agent labelled – *Jnr. Mgr. Pol.* Figure 6-39(i) depicts the shortest resource access pathways of the agent - *Jnr. Mgr. Pol.* The figure shows that in addition to six directly accessible resources, this agent has indirect access to many others through the agent - *Emp 2*. Since these indirect access pathways are very short, they receive high metric scores. Furthermore, the intermediate agent - *Emp 2* has been flagged for intrinsic risk characteristics resulting in a higher composite agent risk value. In contrast to *Jnr. Mgr. Pol.* information access pathways of *Snr. Mgr. 1* are more complicated and longer as illustrated in Figure 6-39 (ii). The pathways of the latter also involve many more agents. Owing to longer access paths, the  $IAC(a_i, r_j)$  risk scores

corresponding to the agent *Snr. Mgr. 1* have lower risk values (Note that the corresponding row has cells with colours indicating lower risk values). Despite the longer paths, *Snr. Mgr. 1* has indirect access to all information resources while there is no pathway through the formal reporting structure of the organisation for *Jnr. Mgr. Pol.* to access the resource *Fin. IS* as indicated in Figure 6-39 (Also note the dark blue cell in the row corresponding to *Jnr. Mgr. Pol.* in the heat-map). Figure 6-38(ii) indicates that there are fewer indirect access opportunities through the formal reporting structure of the Organisation-3.



(i) Sub-network of agent *Jnr. Mgr. Pol*

(ii) Sub-network of agent *Snr. Mgr. 1*

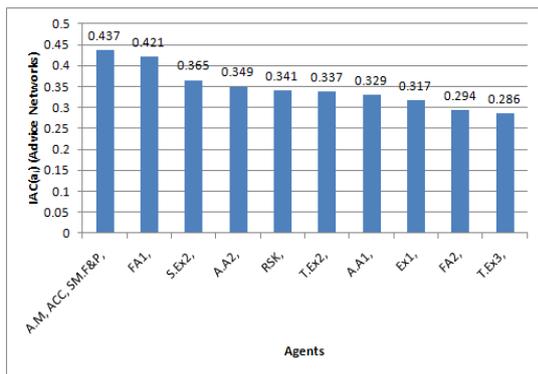
Legend: ● Agent ▲ Resource

Figure 6-39: Sub-networks illustrating the shortest resource access pathways of agents - *Jnr. Mgr. Pol* and *Snr. Mgr. 1* in Organisation-2. Blue spheres represent agents and triangles represent information resources. The diagrams only show resource access (agent → resource) and formal reporting (agent → agent) links that are part of the shortest information access pathways of the focal agents.

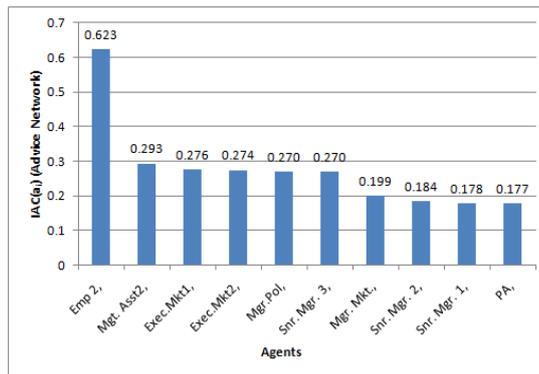
**Indirect access through the advice relationships in organisations**

Agents who receive the top ten IAC(a<sub>i</sub>) scores in the three organisations (calculated using the advice networks) are given in Figure 6-40. Similar to the IAC(a<sub>i</sub>) metric scores calculated using the formal reporting structure, agents having direct access to many information resources score high values. This can be further confirmed using the heat-maps in Figure

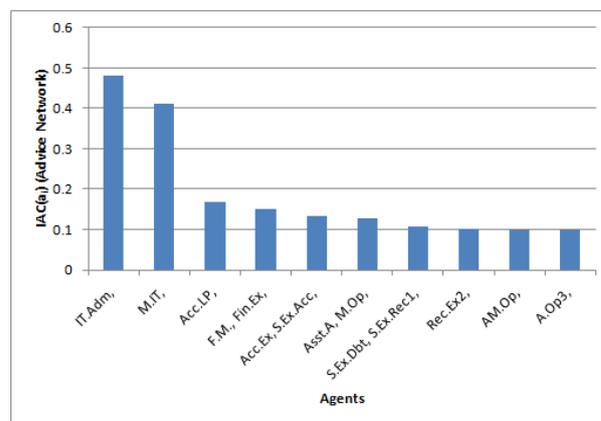
6-41, where direct authorisations appear as white cells. The agents scoring high IAC(a<sub>i</sub>) metric scores - *A.M*, *ACC*, *SM.F&P* and *FA1* in Organisation-1; *Emp 2* in Organisation-2; and *IT.Adm* and *M.IT* in Organisation-3 have many white cells in the corresponding rows of the heat-maps. Therefore, the agents who obtain most indirect access through the advice networks are the ones receiving moderate IAC(a<sub>i</sub>) scores. As indicated by the presence of many red and orange coloured cells in the heat-maps in Figure 6-41, many agents have high potential for indirect access in all three organisations.



(i) Organisation - 1



(ii) Organisation – 2

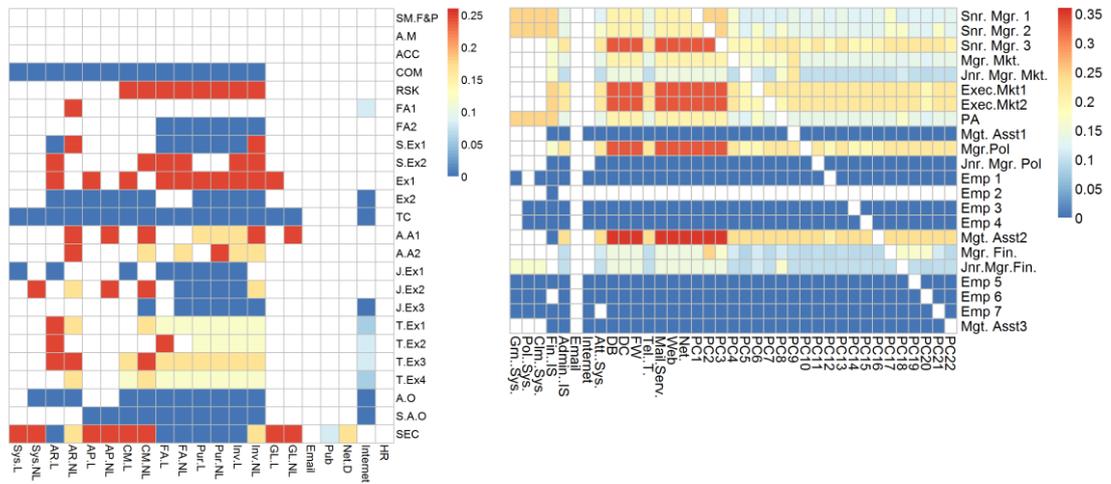


(iii) Organisation – 3

Figure 6-40: Agents receiving the top-ten IAC(a<sub>i</sub>) metric scores in the three organisations (calculated using advice relationships)

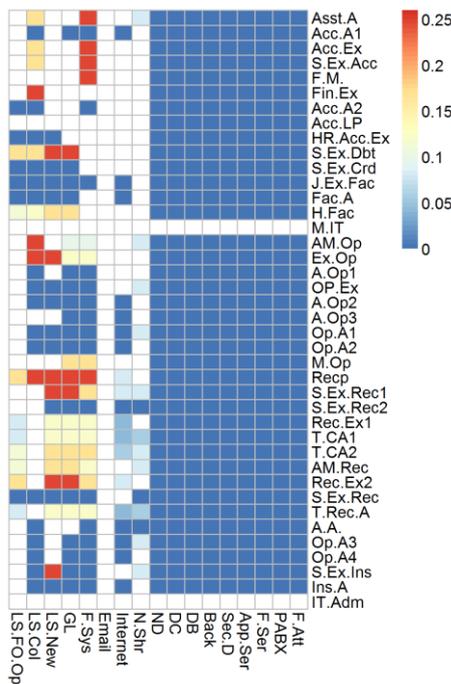
Out of these, Figure 6-42 illustrates the access pathways of three prominent agents – *Ex 1* in Organisation-1, *Mgt. Asst 2* in Organisation-2 and *Recp* in Organisation-3. According to Figure 6-42(i), agent – *Ex 1* can obtain access to all information resources not authorised for him through five other agents linked by advice relationships. Agent *Mgt. Asst 2* in

Organisation-2 obtains indirect access to information resources mainly through *Emp 2* as illustrated in Figure 6-42(ii).



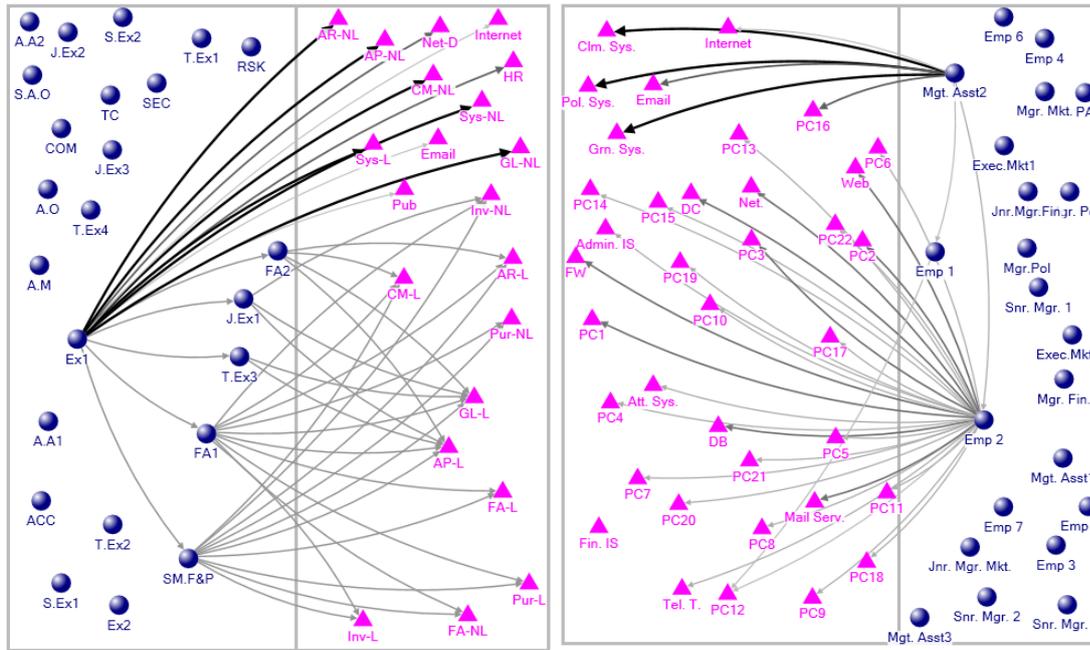
(i) Organisation - 1

(ii) Organisation – 2



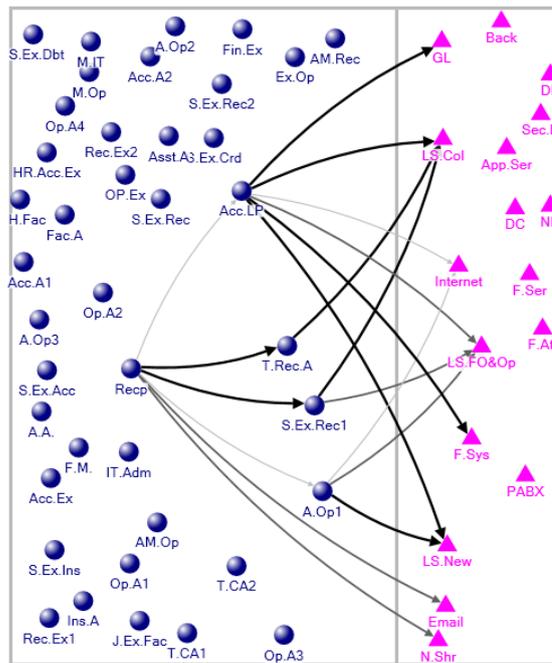
(iii) Organisation – 3

Figure 6-41: Heat-map representations of the  $IAC(a_i, r_j)$  scores of all agent, resource combinations in three organisations calculated considering the advice relationships. Rows represent agents while columns represent information resources. The cell colour reflects the metric score where dark blue represents very low scores and red represents high scores. White cells indicate agents having direct authorisations to access the corresponding resources.



(i) Agent *Ex 1* in Organisation-1

(ii) Agent *Mgt. Asst2* in Organisation-2



(iii) Agent *Recp* in Organisation – 3

Legend: ● Agent ▲ Resource

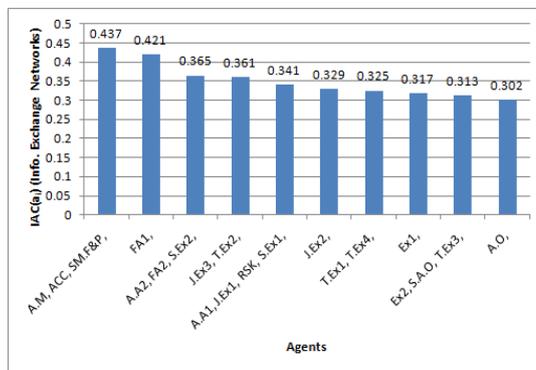
Figure 6-42: Sub-networks illustrating the shortest resource access pathways of three agents who have high indirect access potential through the advice networks. The diagrams only show resource access (agent → resource) and advice (agent → agent) links that are part of the shortest information access pathways of the focal agents.

Indirect access risks in Organisation-3 are not widespread in comparison to the other two as evident from the heat-map consisting mainly of blue cells. In Organisation-3, the two agents (*M.IT* and *IT.Adm*) who have access to majority of the critical information resources

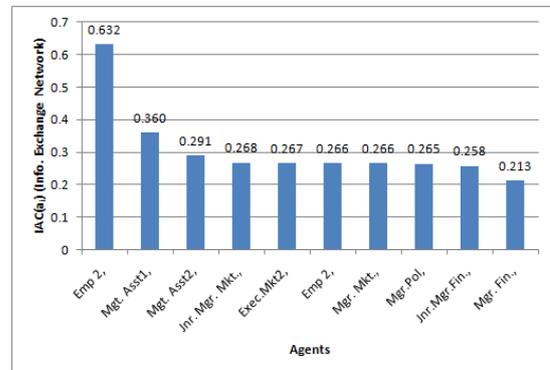
(network devices and servers) do not receive advice (in a strong sense as described earlier) from other agents. Therefore, other agents do not receive indirect access to these critical resources through the advice networks of Organisation-3. Figure 6-42(iii) illustrates the shortest access paths of the agent – *Recp* in Organisation-3. As shown in the figure, there are many resources that the agent cannot obtain indirect access utilising the advice relationships.

**Indirect access through the information exchange networks**

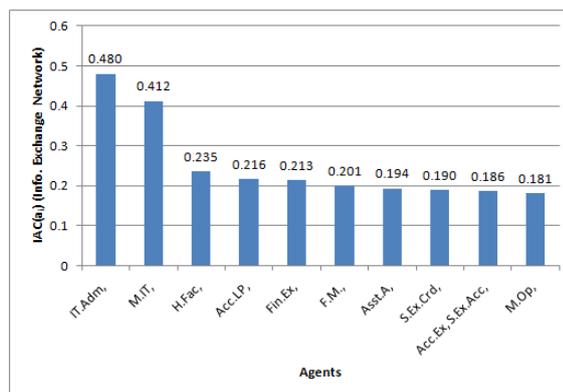
Figure 6-43 presents the  $IAC(a_i)$  values of the agents receiving the top-ten metric scores calculated using the information exchange networks. As in the case of formal reporting and advice relationships, the agents having direct access to many resources score the highest metric values.



(i) Organisation - 1



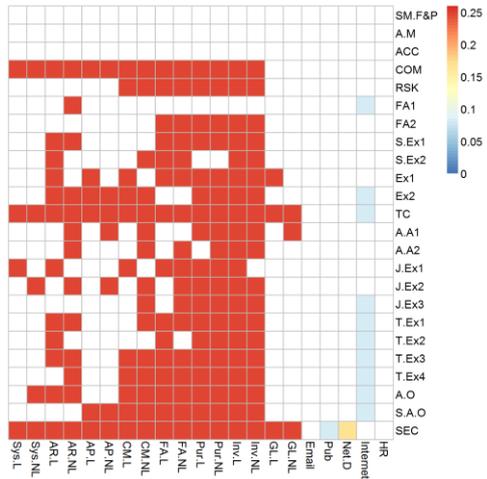
(ii) Organisation – 2



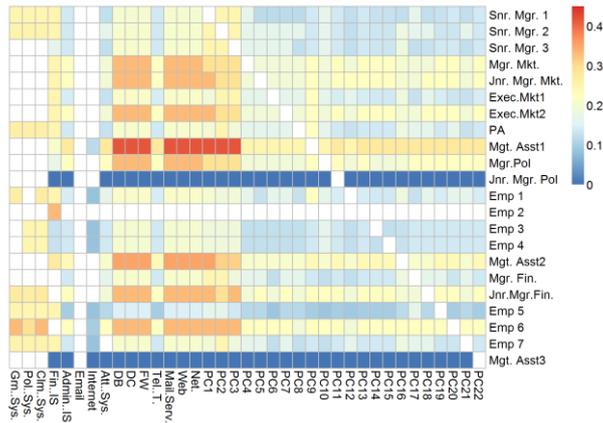
(iii) Organisation – 3

Figure 6-43: Agents receiving the top-ten  $IAC(a_i)$  metric scores in the three organisations (calculated using the information exchange relationships)

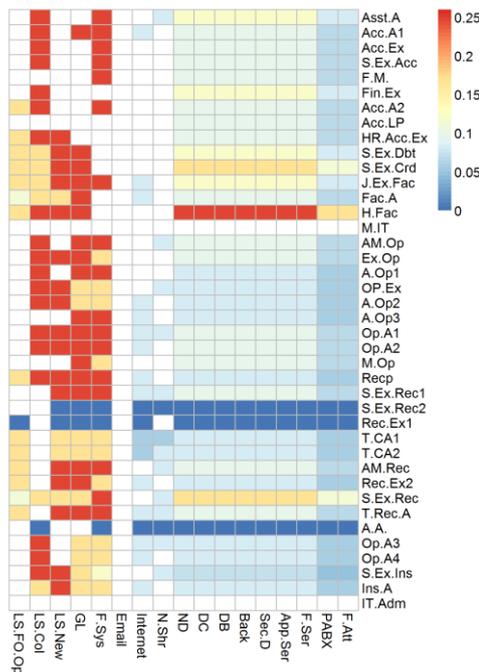
Figure 6-44 presents heat-map representations of the indirect access risks of the three organisations. In the heat-maps, rows represent agents while columns represent information resources. The cell colour reflects the metric score where dark blue represents very low scores and red represents high scores.



(i) Organisation - 1



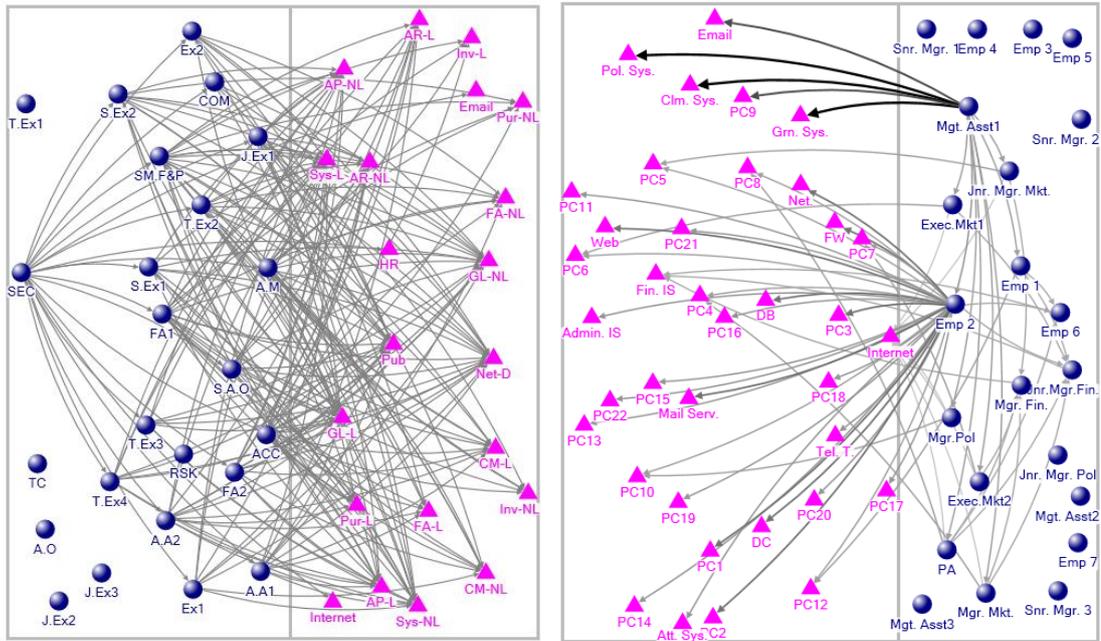
(ii) Organisation – 2



(iii) Organisation – 3

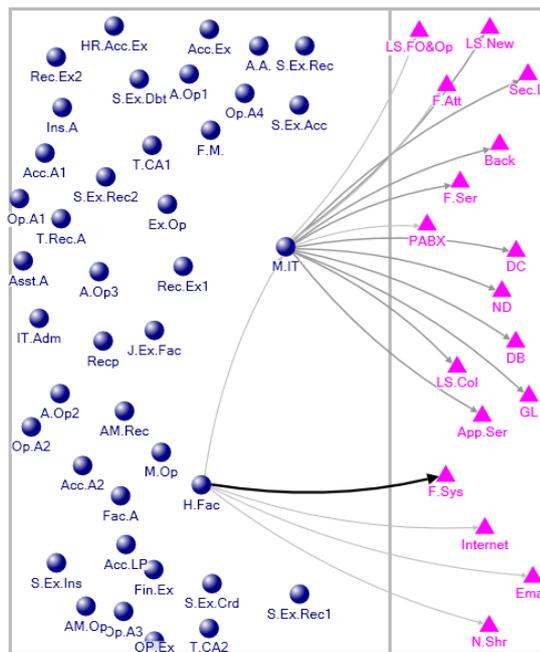
Figure 6-44: Heat-map representations of the  $IAC(a_i,r_j)$  scores of all agent, resource combinations in three organisations calculated considering the information exchange relationships. Rows represent agents while columns represent information resources. The cell colour reflects the metric score where dark blue represents very low scores and red represents high scores. White cells indicate agents having direct authorisations to access the corresponding resources.

Figure 6-45 illustrates the shortest access paths of three agents with high indirect resource access potential. Prevalence of red cells in Figure 6-44(i) indicate that all agents in Organisation-1 has high potential for indirect access to almost all the resources they do not possess direct authorisations. The reason for high indirect access risk scores is the availability of multiple short paths through the information exchange network of the organisation. Figure 6-45(i) illustrate the multiple short access paths of the information exchange network available for the agent – SEC.



(i) Agent SEC in Organisation-1

(ii) Agent Mgt. Asst1 in Organisation-2



(iii) Agent H.Fac in Organisation – 3

Legend: ● Agent ▲ Resource

Figure 6-45: Sub-networks illustrating the shortest resource access pathways of three agents who have high indirect access potential through the information exchange networks. The diagrams only show resource access (agent → resource) and advice (agent → agent) links that are part of the shortest information access pathways of the focal agents.

According to the heat-map in Figure 6-44(ii), many agents have indirect access to information resources through the information exchange network of Organisation-2. Out of them, indirect access capabilities of *Mgt. Asst1* are conspicuous. The access pathways of

this agent through the information exchange network are illustrated in Figure 6-45 (ii). The majority of the short indirect access paths of *Mgt. Asst1* occur through the agent - *Emp 2*, who is the systems administrator in Organisation-2. Unlike in the case of advice networks, information exchange relationships of Organisation-3 provide pathways for many employees to obtain indirect access to all information resources as evident from the heat-map in Figure 6-44(iii). The reason for the difference can be seen in the shortest paths of agent – *H.Fac* illustrated in Figure 6-45(iii). In contrast to the advice network, the ego node here has a link to one of the two agents (*M.IT*) having direct access to critical information resources.

**Indirect access through the friendship networks**

Figure 6-46 depicts the  $IAC(a_i)$  metric scores of the agents who receive the top-ten values in the three organisations through the friendship networks. Similar to the previously described social networks, agents having direct access to more resources score the highest  $IAC(a_i)$  metric values. The heat-maps representing  $IAC(a_i, r_j)$  metric scores for all agent resource combinations of the three organisations are given in Figure 6-47.

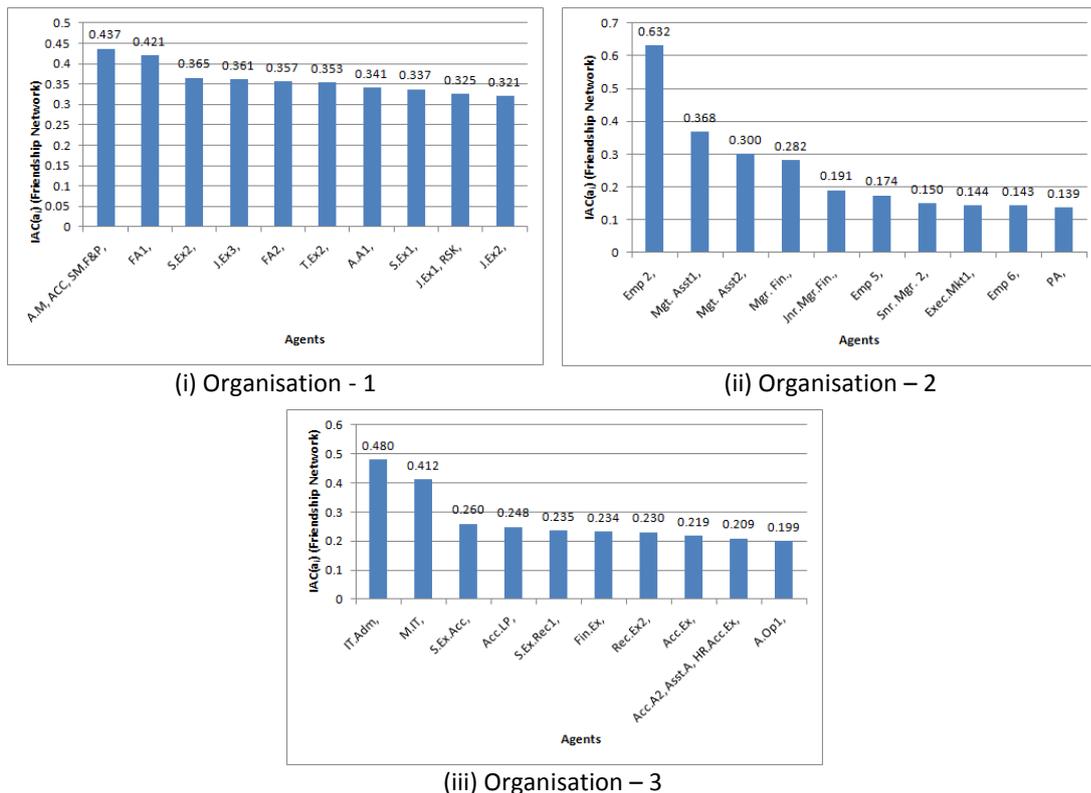


Figure 6-46: Agents receiving the top-ten  $IAC(a_i)$  metric scores in the three organisations (calculated using the friendship links between agents)



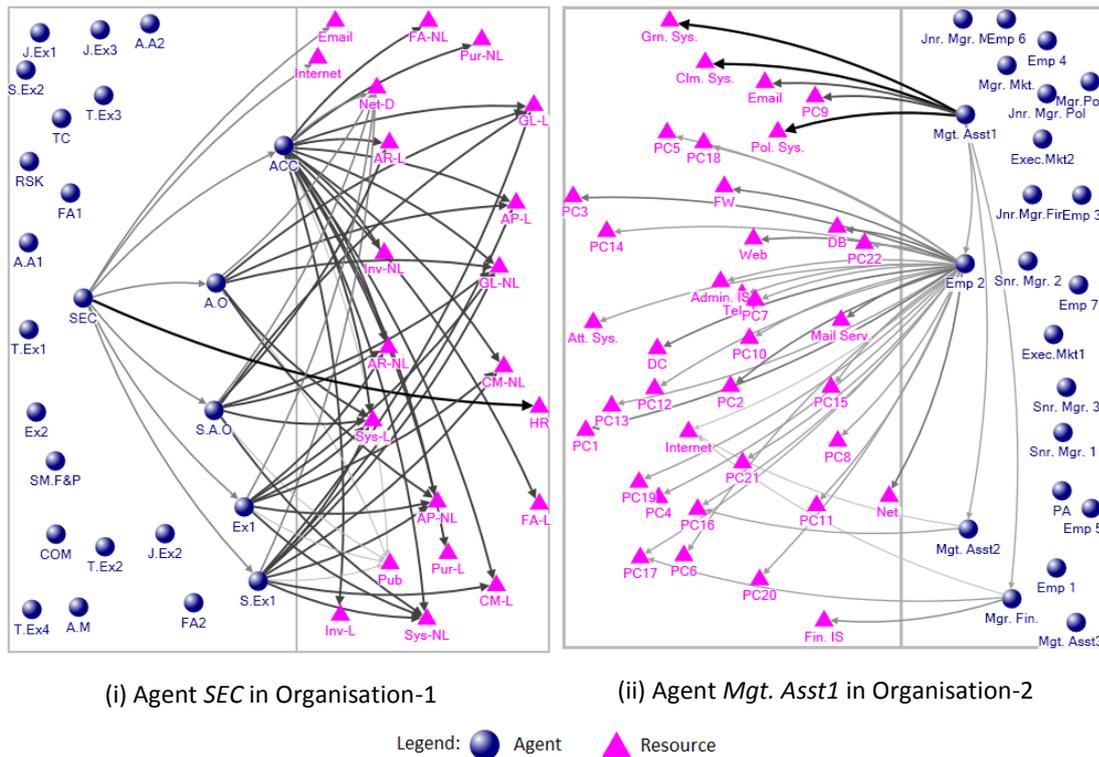


Figure 6-48: Sub-networks illustrating the shortest resource access pathways of two agents who have high indirect access potential through the information exchange networks. Blue spheres represent agents and triangles represent information resources. The diagrams only show resource access (agent → resource) and advice (agent → agent) links that are part of the shortest information access pathways of the focal agents.

In the heat-maps in Figure 6-47, rows represent agents while columns represent information resources. High indirect access risks are indicated by red shades while very low risks are indicated by dark blue (refer the scales given). White cells indicate that the agent has direct authorisations for the corresponding resources. According to Figure 6-47(i), all agents except *COM* and *A.A2* has potential for indirect access through the friendship links. In contrast to this, the information exchange network described earlier provides possibilities for all agents to indirectly access all information resources. Figure 6-48(i) illustrates the shortest access paths of agent- *SEC* in Organisation-1. There are fewer short access paths for this agent via the friendship links than through the information exchange network (cf. Figure 6-45 (i)). According to the heat-maps in Figure 6-47, there are fewer indirect access possibilities through the friendship network of Organisation-2 when compared with the other two organisations. Figure 6-48(ii) illustrates the shortest access paths available for the agent *Mgt. Asst1* in Organisation-2 via the friendship network. As in the case of information exchange networks, majority of the shortest paths occur through *Emp 2*. Another trend visible in the two heat-maps (Figure 6-48(ii) and (iii)) for organisations 1 and 2 is that fewer agents occupying managerial positions have notable

indirect access capabilities through friendship links. For example, managers - *Snr. Mgr.1*, *Snr.Mgr.3*, *Mgr.Mkt.*, and *Mgr. Pol* in Organisation-2 and *F.M*, *H.Fac* and *M.OP* in Organisation-3 have very low indirect access capabilities through the friendship networks.

### **6.5.3 Risks due to agents having transitive access to dependent information resources**

Sometimes, even when agents are not authorised to access two dependent information resources, they can still obtain transitive access through the social networks as described in section 5.6.2. TAR metrics can be used to assess such risks due to transitive access to dependent information resources. The next four sub-topics present the results of the risk assessment carried out using the TAR metrics.

#### **Transitive access to dependent resources through formal reporting structure of organisations**

There are no paths for agents to obtain transitive access to dependent resources in Organisation-1 and all agents receive a  $TAR(a_i)$  risk score of zero. In Organisation-2 agent – *Jnr. Mgr. Pol* receives a metric score of 0.00026 while in Organisation-3 agents - *F.M.* and *AM.Rec* receives risk scores of 0.00017 and  $7.33 \times 10^{-5}$  respectively. All other agents in these two organisations receive a risk metric of zero via the formal reporting structure. The  $TAR(a_i, r_j)$  metric quantifies the transitive access risks per agent- resource combination. Again all agent-resource combinations in Organisation-1 receive a risk score of zero. The agent-resource combinations – *Jnr. Mgr. Pol* → *Net.*, *Jnr. Mgr. Pol* → *DB* and *Jnr. Mgr. Pol* → *Mail Serv.* in Organisation-2 and *F.M.* → *F. Sys* and *AM.Rec* → *LS.FO&Op* in Organisation-3 receive non-zero  $TAR(a_i, r_j)$  values as illustrated in Figure 6-49.

#### **Transitive access to dependent resources through advice relationships**

Bar-charts in Figure 6-50 gives the  $TAR(a_i)$  scores of the agents receiving non-zero values in the three organisations calculated using the advice networks. According to the results, majority of the agents in all three organisations have  $TAR(a_i)$  values of zero although more agents carry the risk via the advice networks than through the formal reporting structures of the organisations.

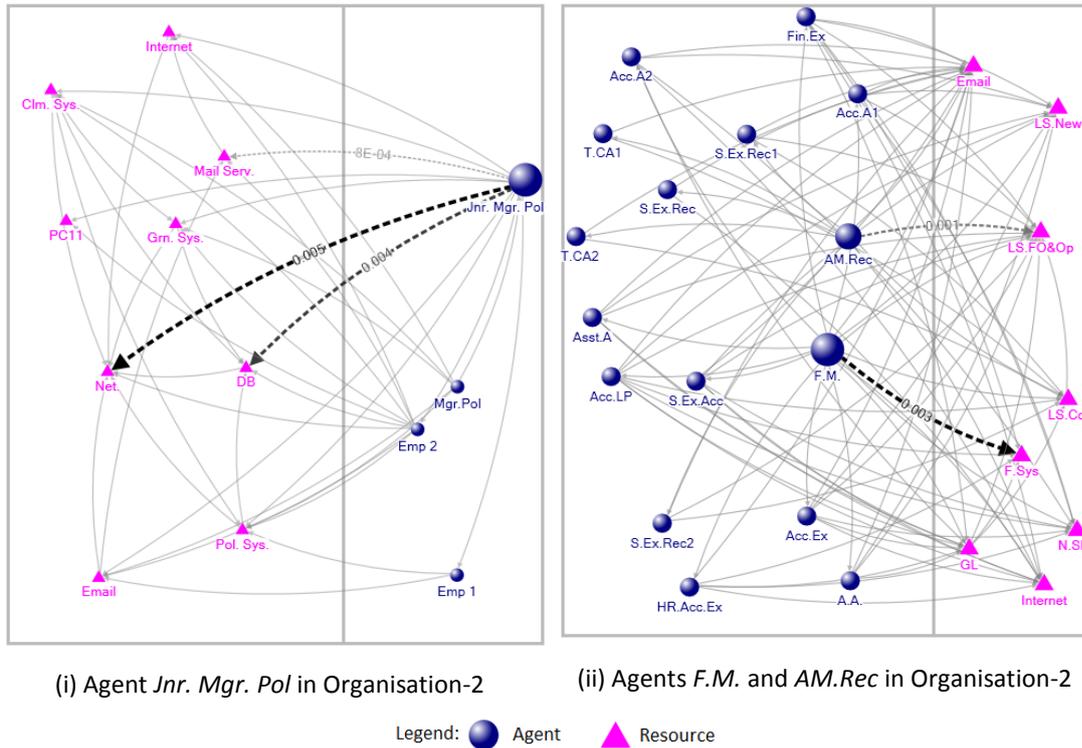
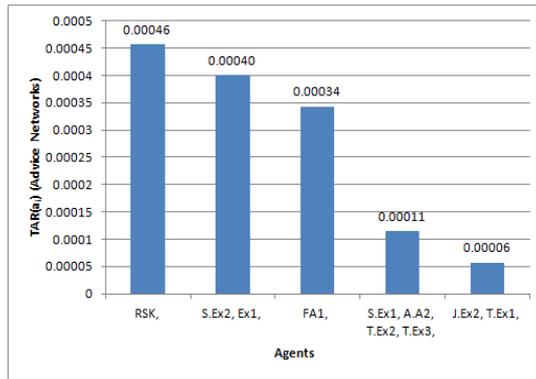
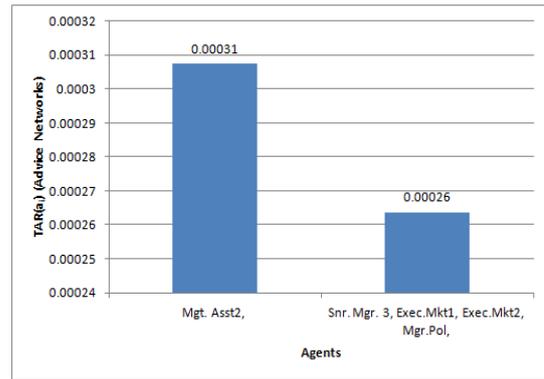


Figure 6-49: Sub-networks illustrating the transitive access to dependent resource risks via the formal reporting networks of Organisations 2 and 3. Only agents who score a non-zero  $TAR(a_i)$  score, their associated agents and resources are shown in the diagrams. The networks illustrate agent  $\rightarrow$  agent, agent  $\rightarrow$  resource and resource  $\rightarrow$  resource links. The transitive access links are shown in dotted lines along with the  $TAR(a_i, r_j)$  score as a link labels. Only agent -*Jnr. Mgr. Pol* in Organisation-2 and agents -*F.M.* and *AM.Rec* in Organisation-3 have transitive access to dependent resource risks.

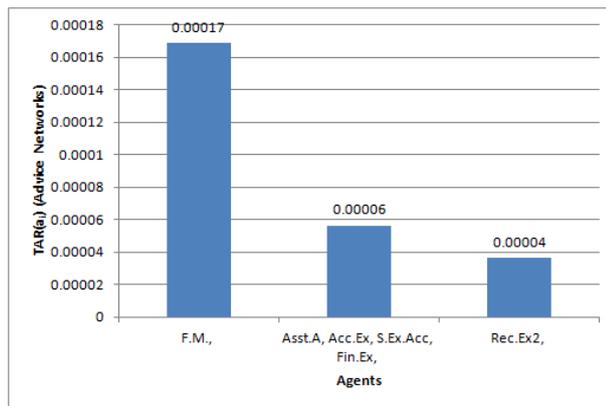
Heat-maps in Figure 6-51 represent the transitive access to dependent resource risks ( $TAR(a_i, r_j)$  scores) for all possible agent-resource combinations of Organisations 1 and 2. In Organisation-3, only *F.M.*  $\rightarrow$  *F.Sys* receive a significant score of 0.0029 out of six agent-resource combinations obtaining non-zero risk values. In Organisation-1, a significant risk occurs due to agent - *FA1* obtaining transitive access to resource *AR.NL* as shown in Figure 6-51(i).  $TAR$  risks can be demonstrated using an example taken from Organisation-2 illustrated in Figure 6-52. As shown in the figure, agent - *Mgt. Asst2* can obtain access to resource *DB* (indicated by the dotted line) utilising his advice relationship with agent *Emp 2* (*Mgt. Asst2* advises *Emp 2*) although he does not have a direct authorisation for the resource. However, this potential for transitive access creates a risk since *Mgt. Asst2* can directly access three other resources (*Pol. Sys*, *Clm. Sys* and *Grn. Sys*) that depend on resource - *DB*. Therefore, even if the organisation does not explicitly authorise a given agent to access dependent information resources, sometimes the controls can be bypassed by manipulating the social network.



(i) Organisation - 1



(ii) Organisation - 2



(iii) Organisation - 3

Figure 6-50: Agents receiving non-zero TAR(a<sub>i</sub>) metric scores in the three organisations (calculated using the advice relationships between agents)

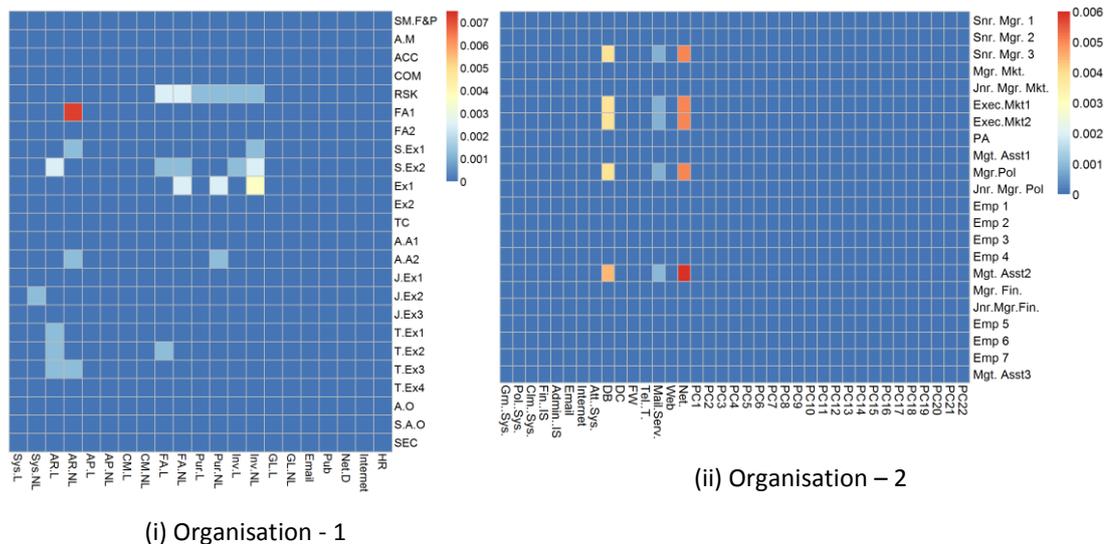


Figure 6-51: Heat-map representations of the TAR(a<sub>i</sub>, r<sub>j</sub>) scores of all agent, resource combinations in organisations 1 and 2 calculated considering the advice relationships. Rows represent agents while columns represent information resources. The cell colour reflects the metric score where dark blue represents very low scores and red represents high scores.

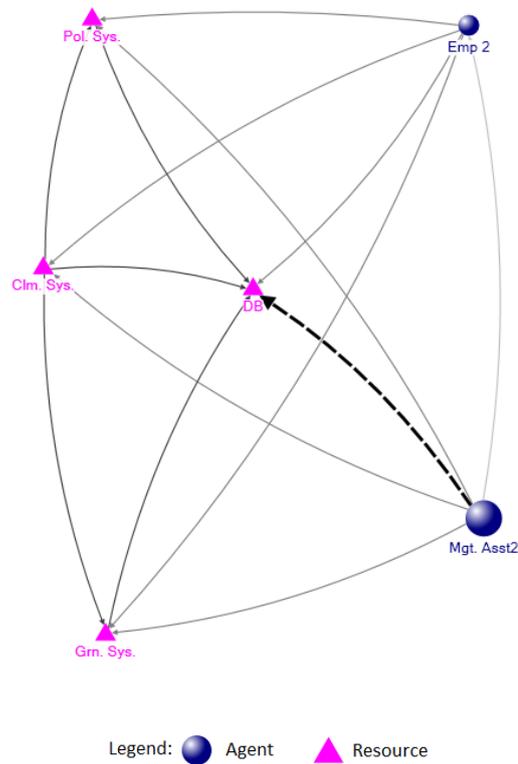


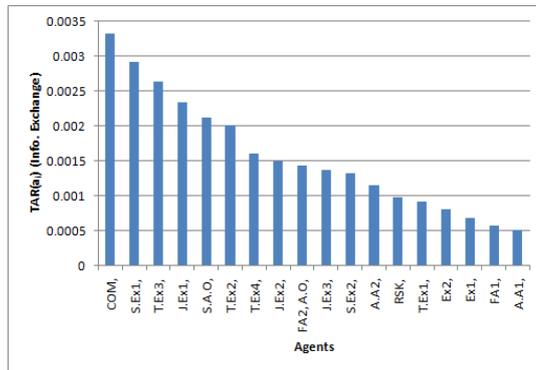
Figure 6-52: Example from Organisation-2 illustrating the transitive access to dependent information resources. Diagram shows the transitive access possibility of *Mgt. Asst2* in relation to *DB* (shown as a dotted line).

**Transitive access to dependent resources through the information exchange networks**

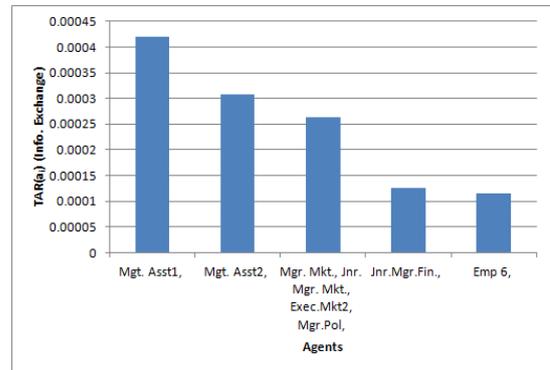
Bar-charts in Figure 6-53 depict the  $TAR(a_i)$  scores of the agents receiving non-zero values in the three organisations, calculated using the information exchange networks. When compared with the  $TAR(a_i)$  scores, calculated using the formal reporting and advice networks, more agents receive non-zero values through the information exchange networks.

Figure 6-54 presents heat-maps depicting  $TAR(a_i, r_j)$  scores of all agent-resource combinations in the three organisations calculated using the information exchange networks. According to the heat-maps, the highest risks in organisations 1, 2 and 3 occur due to transitive access possibilities to  $J.Ex1 \rightarrow Sys-L$ ,  $Mgt. Asst1 \rightarrow Net.$ , and  $HR.Acc.Ex \rightarrow LS.FO\&Op$  respectively. There is no visible pattern for the occurrence of transitive access to dependent resource risks in Organisation – 1. On the other hand, according to the heat-map in Figure 6-54 (ii), high risk scores in Organisation – 2 occur in relation to resources –

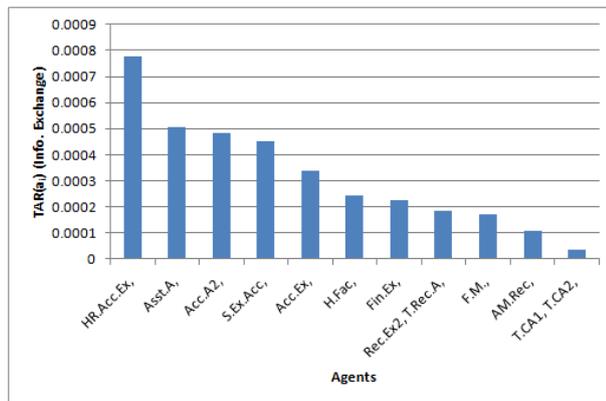
DB, Mail Serv. and Net. High risk scores in Organisation – 3 occur in relation to resources - LS.FO&Op, LS. Col. and F. Sys as well as the agent – H.Fac.



(i) Organisation - 1

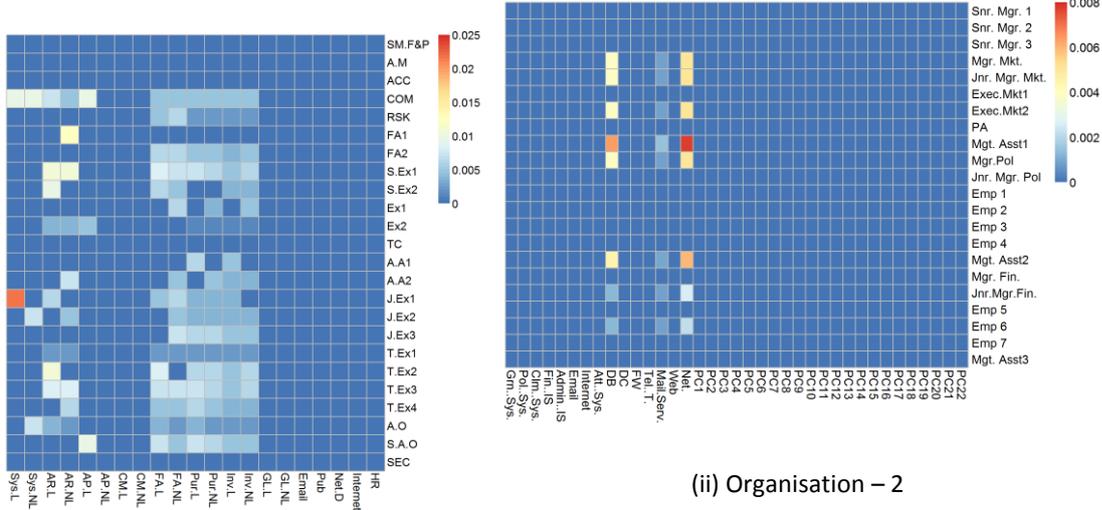


(ii) Organisation – 2



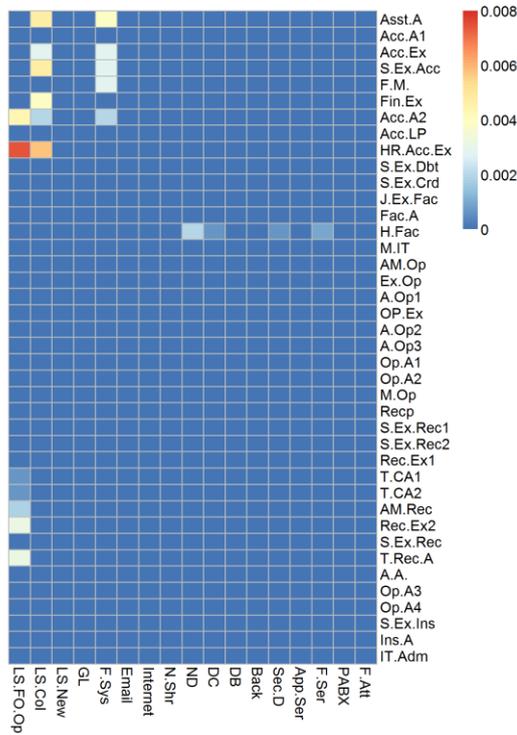
(iii) Organisation – 3

Figure 6-53: Agents receiving non-zero TAR(a<sub>i</sub>) metric scores in the three organisations (calculated using the information exchange relationships between agents)



(i) Organisation - 1

(ii) Organisation – 2

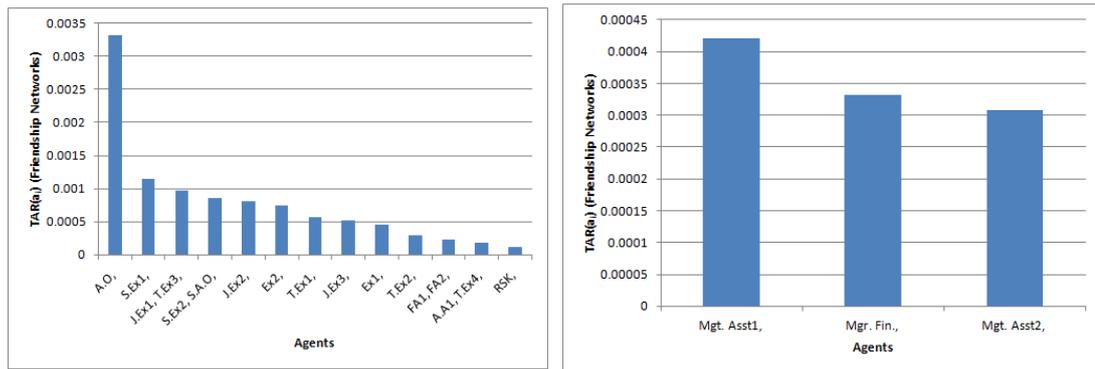


Organisation - 3

Figure 6-54: Heat-map representations of the  $TAR(a_i, r_j)$  scores of all agent, resource combinations in three organisations calculated considering the information exchange relationships. Rows represent agents while columns represent information resources. The cell colour reflects the metric score where dark blue represents very low scores and red represents high scores.

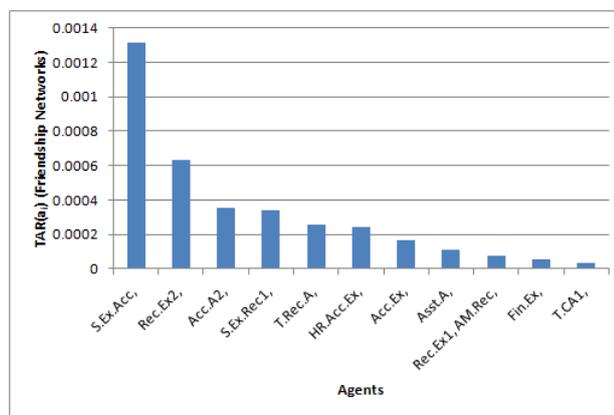
**Transitive access to dependent resources through the friendship networks**

Bar-charts in Figure 6-55 depict the  $TAR(a_i)$  scores of the agents receiving non-zero values in the three organisations calculated using the friendship networks. Although the number of agents receiving non-zero the  $TAR(a_i)$  scores are similar for both friendship and information exchange networks of organisations 1 and 3, very few agents in Organisation–2 receive non-zero risk scores through the friendship network.



(i) Organisation - 1

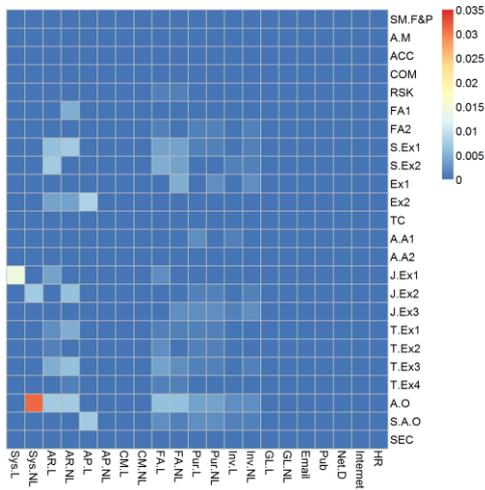
(ii) Organisation – 2



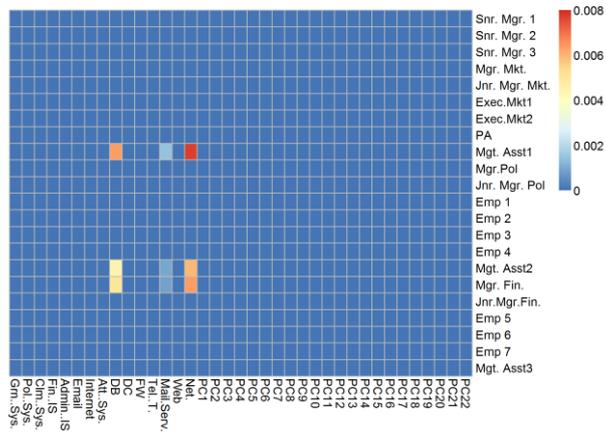
(iii) Organisation – 3

Figure 6-55: Agents receiving non-zero  $TAR(a_i)$  metric scores in the three organisations (calculated using the friendship networks in organisations)

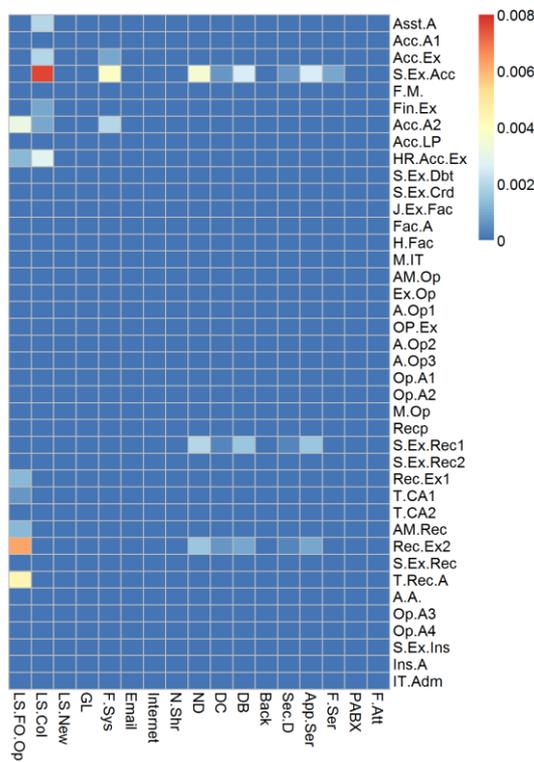
Figure 6-56 presents heat-maps depicting  $TAR(a_i, r_j)$  scores of all agent-resource combinations in the three organisations calculated using the friendship networks. In Organisation – 1, the only significant  $TAR(a_i, r_j)$  risk score occurs due to the transitive access relationship  $A.O. \rightarrow Sys. NL$ . The high metric values in Organisation – 2 occur in relation to the resources – *Net.* and *DB*. In Organisation – 3, the highest  $TAR(a_i, r_j)$  risk score occurs due to the transitive access relationship  $S.Ex.Acc \rightarrow LS.Col$ .



(i) Organisation - 1



(ii) Organisation - 2



Organisation - 3

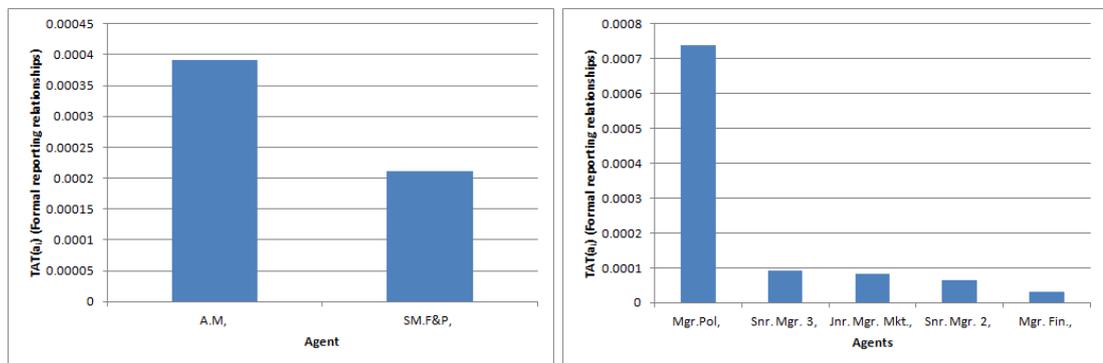
Figure 6-56: Heat-map representations of the  $TAR(a_i, r_j)$  scores of all agent, resource combinations in three organisations calculated considering the friendship networks. Rows represent agents while columns represent information resources. The cell colour reflects the metric score where dark blue represents very low scores and red represents high scores.

### 6.5.4 Risks due to agents obtaining transitive assignment to dependent tasks

Even when agents are not assigned to dependent tasks in an organisation, they can obtain transitive assignments to tasks through their social networks as described in section 5.6.3. Such a transitive task assignment could violate the principle of separation of duty. TAT metrics defined in section 5.6.3 can be used to assess transitive task assignment risks and the next four sub-topics present the results of that analysis.

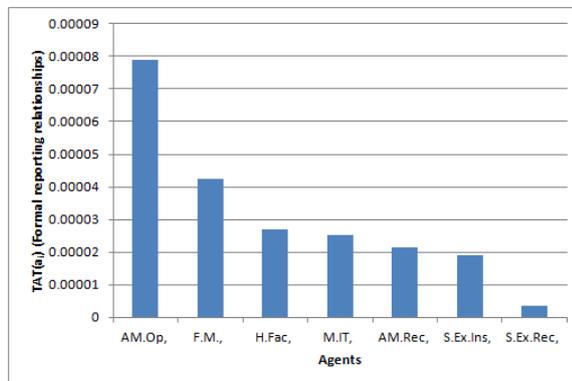
#### Transitive assignment of dependent tasks through the formal reporting structure of organisations

Figure 6-57 present the  $TAT(a_i)$  scores of the agents receiving non-zero metric values in the three organisations calculated using the formal reporting structures. In Organisation-1, only two agents obtain non-zero metric scores. As illustrated in Figure 6-58(i), there are several transitive task assignments that result in non-zero  $TAT(a_i, t_p)$  scores associated with these two agents. Agent – *Mgr. Pol* in Organisation-2 obtain a significantly higher  $TAT(a_i)$  score when compared with the others in the same organisation. The heat-map in Figure 6-58(ii) demonstrate that the transitive task assignments with the highest  $TAT(a_i, t_p)$  risk scores in Organisation-2 are associated with the agent - *Mgr. Pol*.



(i) Organisation - 1

(ii) Organisation – 2



(iii) Organisation – 3

Figure 6-57: Agents receiving non-zero  $TAT(a_i)$  metric scores in the three organisations (calculated using the formal reporting relationships)



**Transitive assignment of dependent tasks through advice relationships**

Figure 6-59 illustrate the  $TAT(a_i)$  scores of the agents in three organisations calculated using the advice relationships. As in the case of  $TAT(a_i)$  the risk scores calculated using the formal reporting structures, only few agents score non-zero risk scores via the advice networks. Three agents – ACC, A.M, and SM.F&P score significantly higher  $TAT(a_i)$  scores when compared with the others in Organisation-1. As shown in the heat-map in Figure 6-60(i), most transitive task assignments with high  $TAT(a_i, t_p)$  scores in Organisation-1 occur in relation to these three agents. In Organisation-2, two agents – Mgr. Pol and Snr. Mgr. 3 score significantly higher  $TAT(a_i)$  scores than others. Heat-map in Figure 6-60(ii) shows that majority of the high-risk transitive task assignments in Organisation-2 are associated with these two agents. In Organisation-3, agent – AM.Op receives a significantly higher  $TAT(a_i)$  value than others. In all three organisations, same agents tend to score high  $TAT(a_i)$  metric values through both formal reporting and advice networks. For example, agents – A.M and SM.F&P are the only ones in Organisation-1 obtaining non-zero metric scores through the formal reporting network and the same agents score the second and third highest values through the advice network. Similarly, agent Mgr. Pol in Organisation-2 and agent – AM.Op in Organisation-3 score the highest metric values in their organisations through both formal reporting and advice networks.

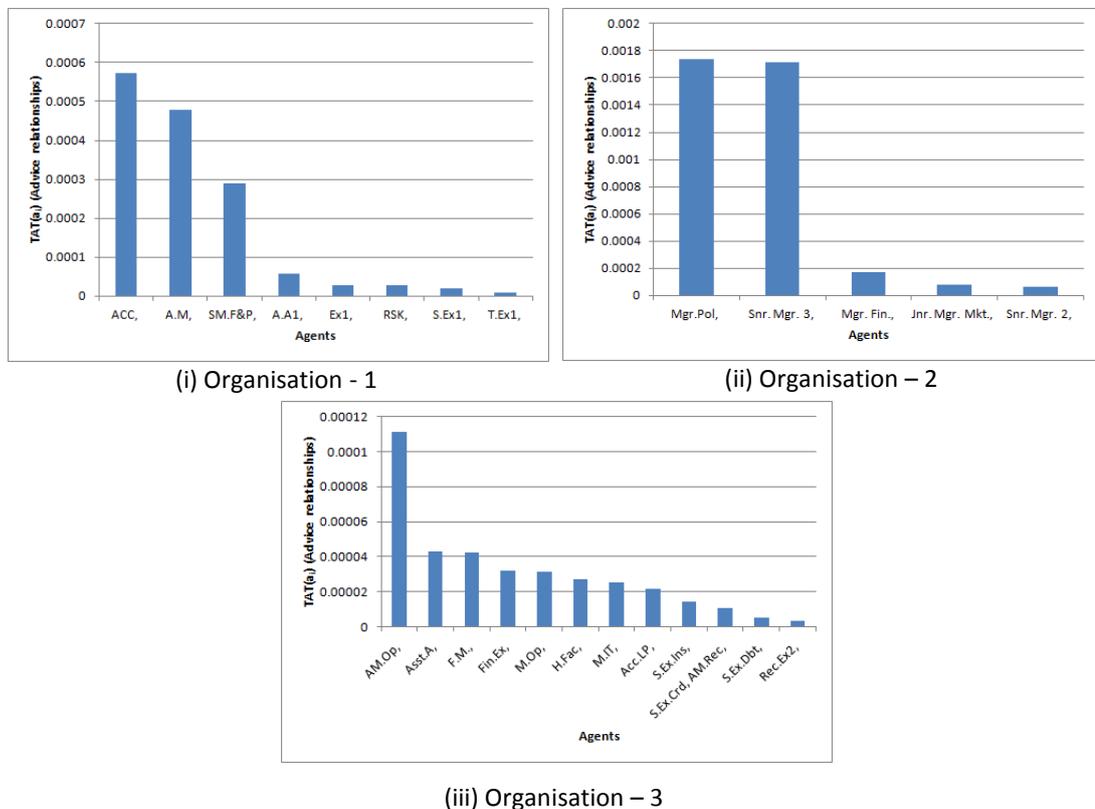
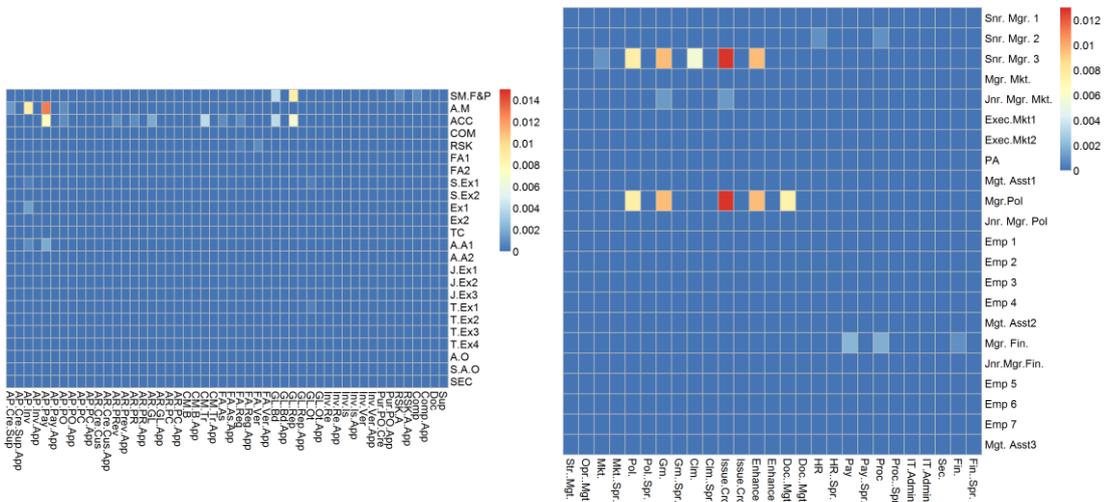
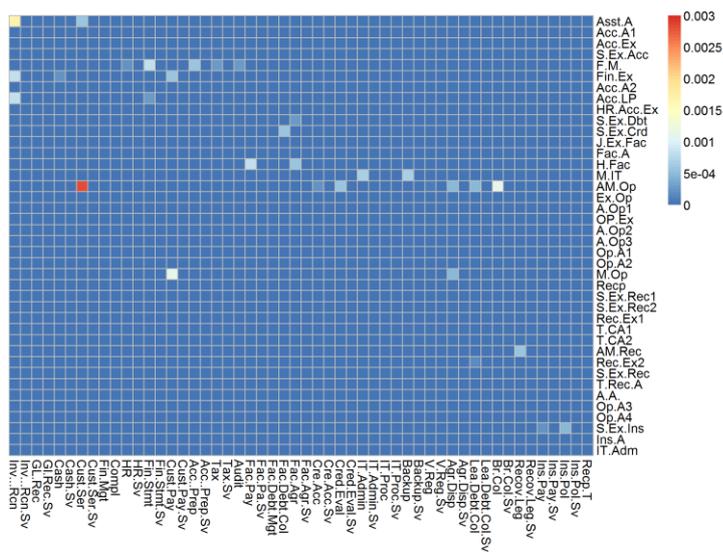


Figure 6-59: Agents receiving non-zero  $TAT(a_i)$  metric scores in the three organisations (calculated using the advice relationships)



(i) Organisation - 1

(ii) Organisation – 2

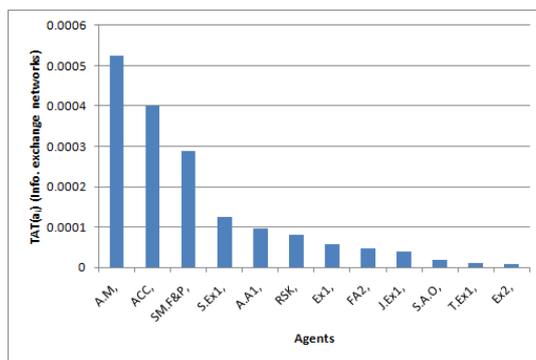


Organisation -3

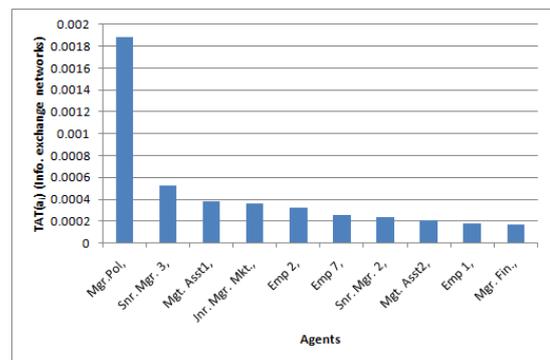
Figure 6-60: Heat-map representations of the TAT( $a_i, t_p$ ) scores of all agent, task combinations in three organisations calculated considering advice networks. Rows represent agents while columns represent tasks. The cell colour reflects the metric score where dark blue represents very low scores and red represents high scores.

**Transitive assignment of dependent tasks through information exchange networks**

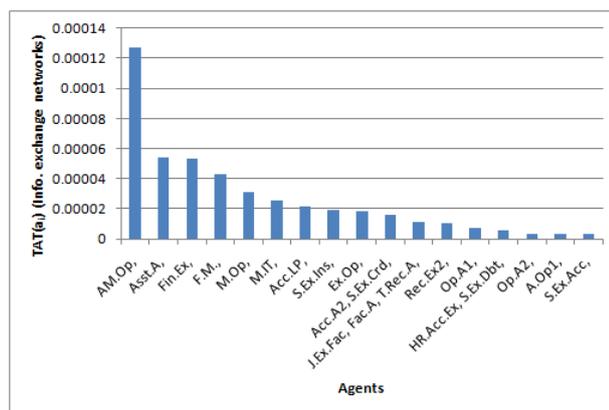
Figure 6-61 presents the  $TAT(a_i)$  scores of the agents who obtain non-zero values using the information exchange networks of the organisations. The same agents who score high risk values through the formal reporting and advice networks receive high metric scores through the information exchange network as well. In Organisation-1 agents *A.M.*, *ACC* and *SM.F&P* receive significantly high  $TAT(a_i)$  values. Agent – *Mgr. Pol* in Organisation-2 and agent – *AM.Op* in Organisation-3 also obtain high scores when compared with others in their organisations. However, more agents receive non-zero  $TAT(a_i)$  values through the information exchange networks than through the advice networks. Figure 6-62 depict the heat-map representations of the  $TAT(a_i, t_p)$  scores of all agent, task combinations in the three organisations. In the heat-maps, red colour cells indicate the transitive task assignments that cause the highest dependent task assignment risks in each organisation.



(i) Organisation – 1

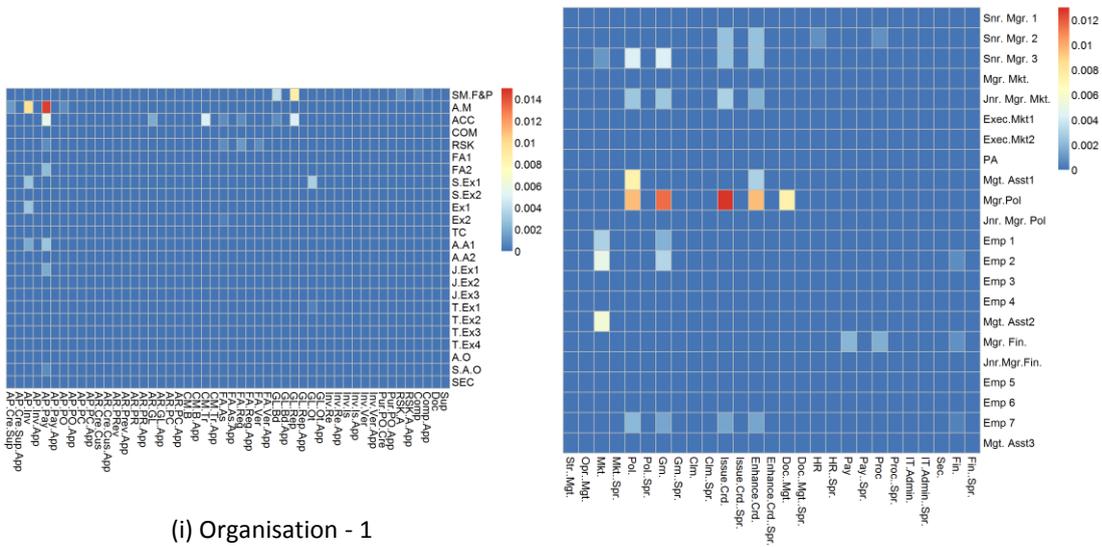


(ii) Organisation – 2



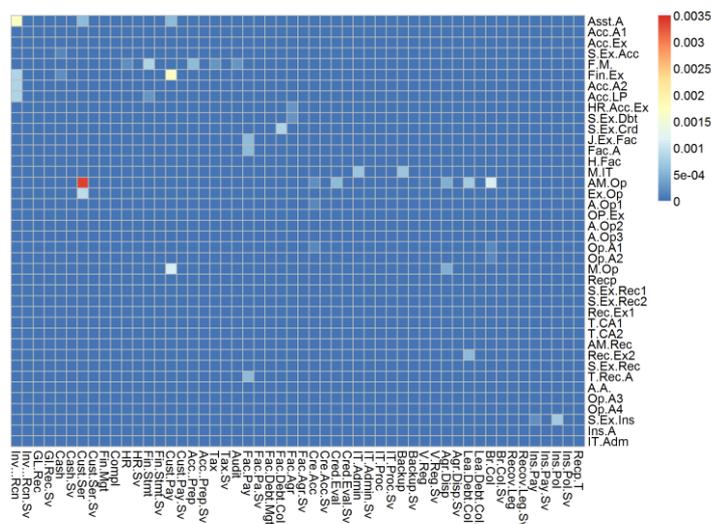
(iii) Organisation – 3

Figure 6-61: Agents receiving non-zero  $TAT(a_i)$  metric scores in the three organisations (calculated using the information exchange networks)



(i) Organisation - 1

(ii) Organisation - 2



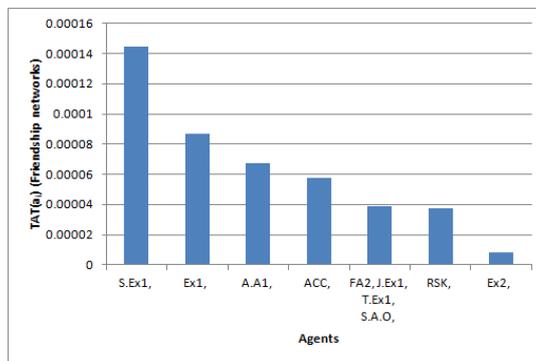
Organisation - 3

Figure 6-62: Heat-map representations of the  $TAT(a_i, t_p)$  scores of all agent, task combinations in three organisations calculated considering information exchange networks. Rows represent agents while columns represent tasks. The cell colour reflects the metric score where dark blue represents very low scores and red represents high scores.

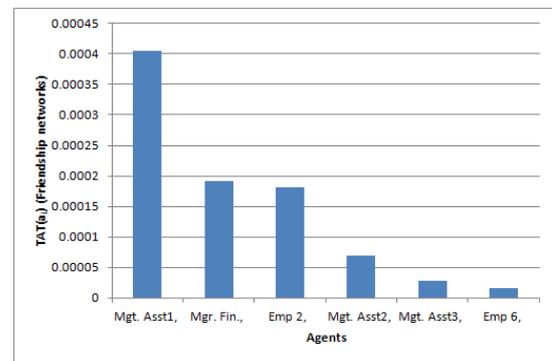
**Transitive assignment of dependent tasks through friendship networks**

Figure 6-63 presents the  $TAT(a_i)$  scores of the agents who score non-zero values in the three organisations calculated using the friendship networks. When compared with  $TAT(a_i)$

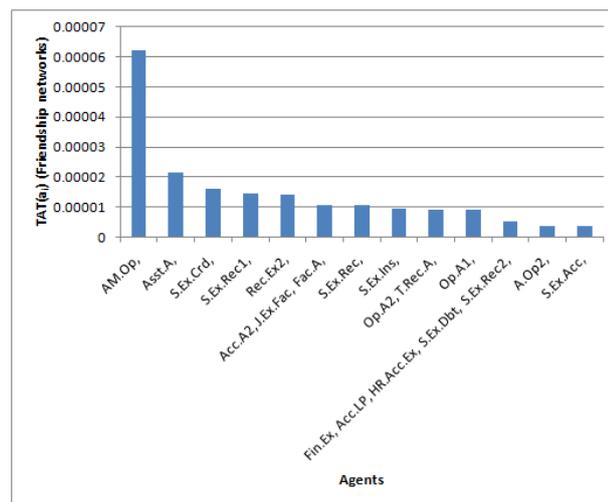
results obtained using the other three social networks, a different set of agents receive high metric scores through the friendship networks of Organisations 1 and 2. In Organisation-1 agent – *S.Ex1* obtains the highest score while *Mgt. Asst1* obtains the highest score in Organisation-2. The three agents - *A.M.*, *ACC* and *SM.F&P*, who receive high  $TAT(a_i)$  values in Organisation-1, through the other social networks, receive metric scores of zero through the friendship network. Similarly, the agent – *Mgr. Pol* in Organisation-2 also receive a  $TAT(a_i)$  metric score of zero via the friendship network. The only exception to this trend is the agent - *AM.Op* in Organisation-3, who scores the highest metric values through all four social networks. In general, agents who receive high  $TAT(a_i)$  metric scores through the formal reporting, advice and information exchange networks occupy managerial positions in their organisations while agents receiving high metric scores through the friendship network are non-managerial staff members.



(i) Organisation - 1



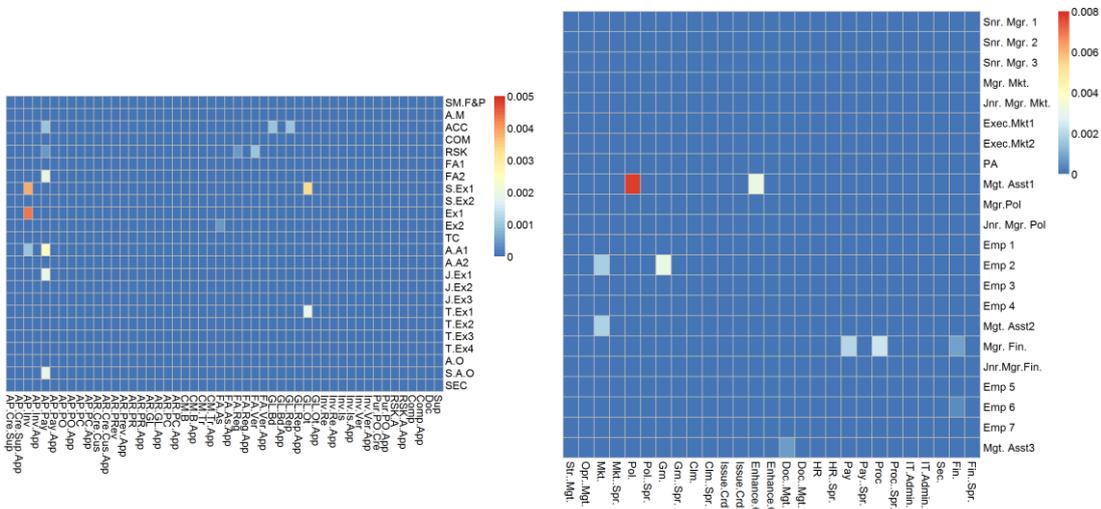
(ii) Organisation – 2



(iii) Organisation – 3

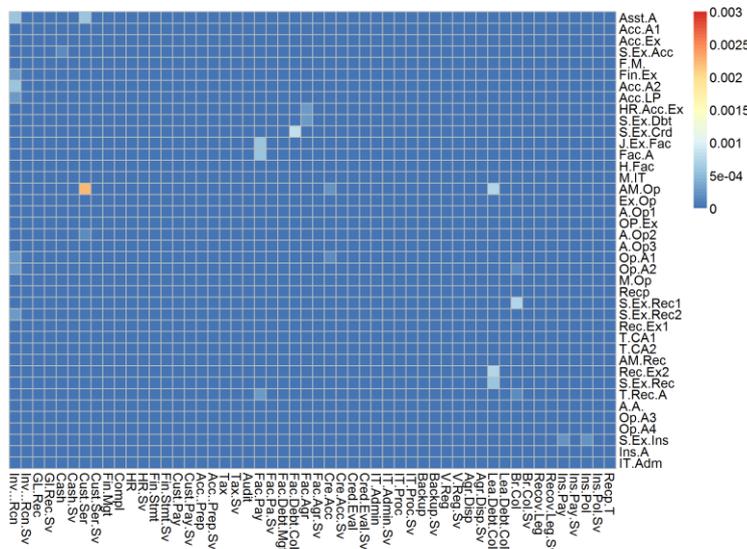
Figure 6-63: Agents receiving non-zero  $TAT(a_i)$  metric scores in the three organisations (calculated using the friendship networks)

Figure 6-64 depicts the heat-map representations of the  $TAT(a_i, t_p)$  scores of all agent, task combinations in the three organisations via the friendship networks.



(i) Organisation - 1

(ii) Organisation – 2



Organisation -3

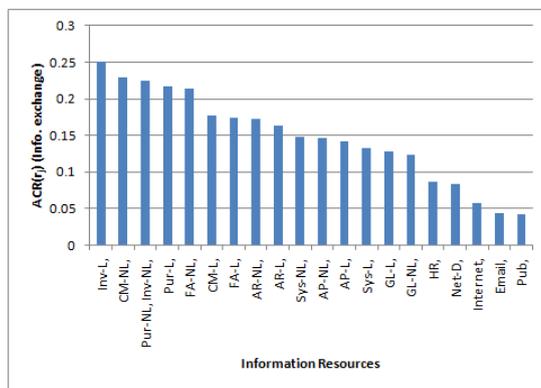
Figure 6-64: Heat-map representations of the  $TAT(a_i, t_p)$  scores of all agent, task combinations in three organisations calculated considering friendship networks. Rows represent agents while columns represent tasks. The cell colour reflects the metric score where dark blue represents very low scores and red represents high scores.

### 6.5.5 Risks due to closely associated group of agents controlling a resource

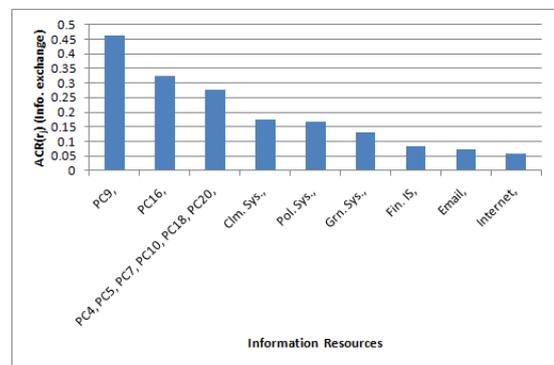
When a closely associated group of agents have control over an information resource, it could lead to collusion resulting in an increased risk of insider threat events. The ACR (Agent Clustering for Resource) metric, defined in section 5.6.4, can be used to quantify such risks. The next two sub-topics present the results of the risk assessment carried out using the ACR metric, which only has a resource centric definition.

#### Agent clustering for a resource due to information exchange networks

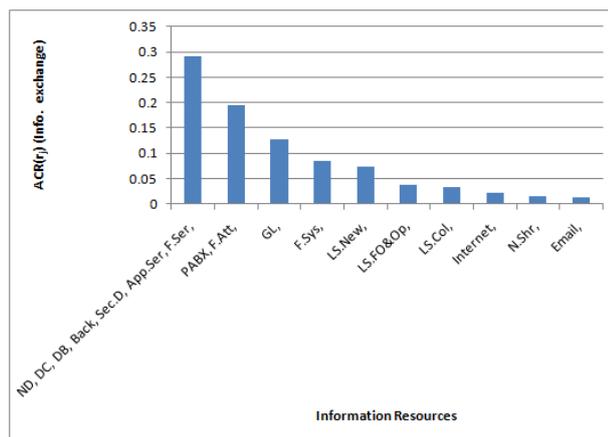
Figure 6-65 presents the  $ACR(r_j)$  scores of the information resources that score non-zero metric values in the three organisations calculated using the information exchange networks.



(i) Organisation - 1



(ii) Organisation - 2

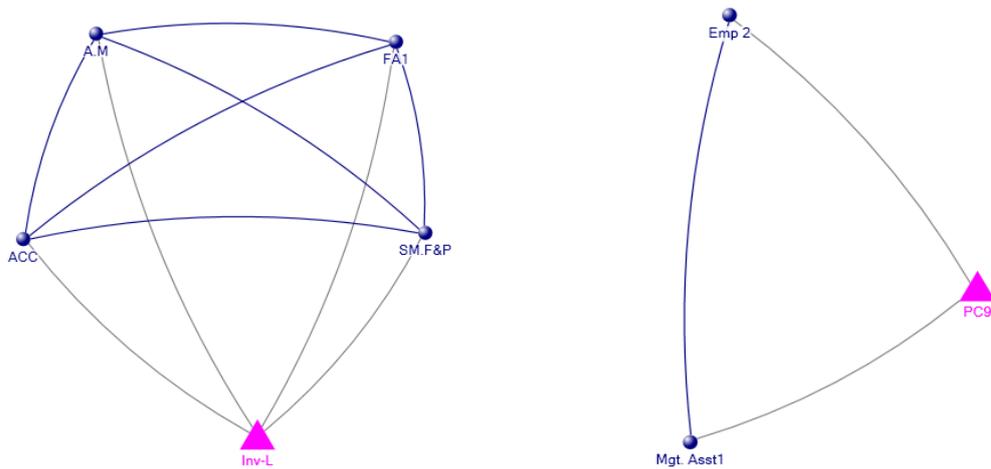


(iii) Organisation - 3

Figure 6-65: Information resources receiving non-zero  $ACR(r_j)$  metric scores in the three organisations (calculated using the information exchange networks)

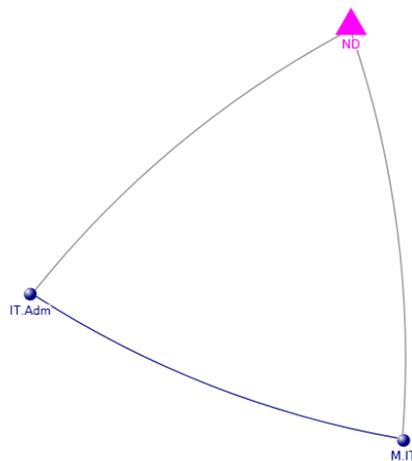
The resources receiving very low  $ACR(r_j)$  risk scores in all three organisations are ones accessible to many agents. These low-scoring resources include email systems, Internet

access and other commonly shared information resources. On the other hand, information resources obtaining high  $ACR(r_j)$  scores are the ones accessible by relatively few people. Figure 6-66 illustrates sub-networks consisting of resource access and information exchange links related to three resources that score high  $ACR(r_j)$  values.



(i) Information resource *Inv-L* in Organisation-1

(ii) Information resource *PC9* in Organisation-2



(iii) Information resource *ND* in Organisation – 3

Legend: ● Agent ▲ Resource

Figure 6-66: Sub-networks illustrating resource access and information exchange links related to three resources that score high  $ACR(r_j)$  values. Blue spheres represent agents and triangles represent information resources. The grey lines show resource access (agent → resource) while blue lines indicate information exchange (agent → agent) links.

As shown in Figure 6-66(i), the resource *Inv-L* in Organisation-1 has four agents accessing it and all four are connected to each other via information exchange relationships. Information resources *PC9* and *ND* (in organisations 2 and 3 respectively) have only two connected agents accessing them.

**Agent clustering for a resource due to friendship networks**

Figure 6-67 illustrates the  $ACR(r_j)$  scores of the information resources that score non-zero metric values in the three organisations calculated using the friendship networks. When compared with the metric values obtained using the information exchange network, the results obtained using the friendship network of Organisation-1 take lower values. The same trend can be observed in Organisation-3 while there is no significant difference in the case of Organisation-2. Furthermore, four information resources in Organisation-2 – *PC9*, *PC16*, *PC17* and *Fin. IS* score significantly high metric scores when compared with other resources in the three organisations. Similar to the results obtained using information exchange relationships, friendship network produces relatively low  $ACR(r_j)$  scores for resources accessed by many agents. Figure 6-68 illustrates sub-networks consisting of resource access and information exchange links related to three resources that score high  $ACR(r_j)$  values.

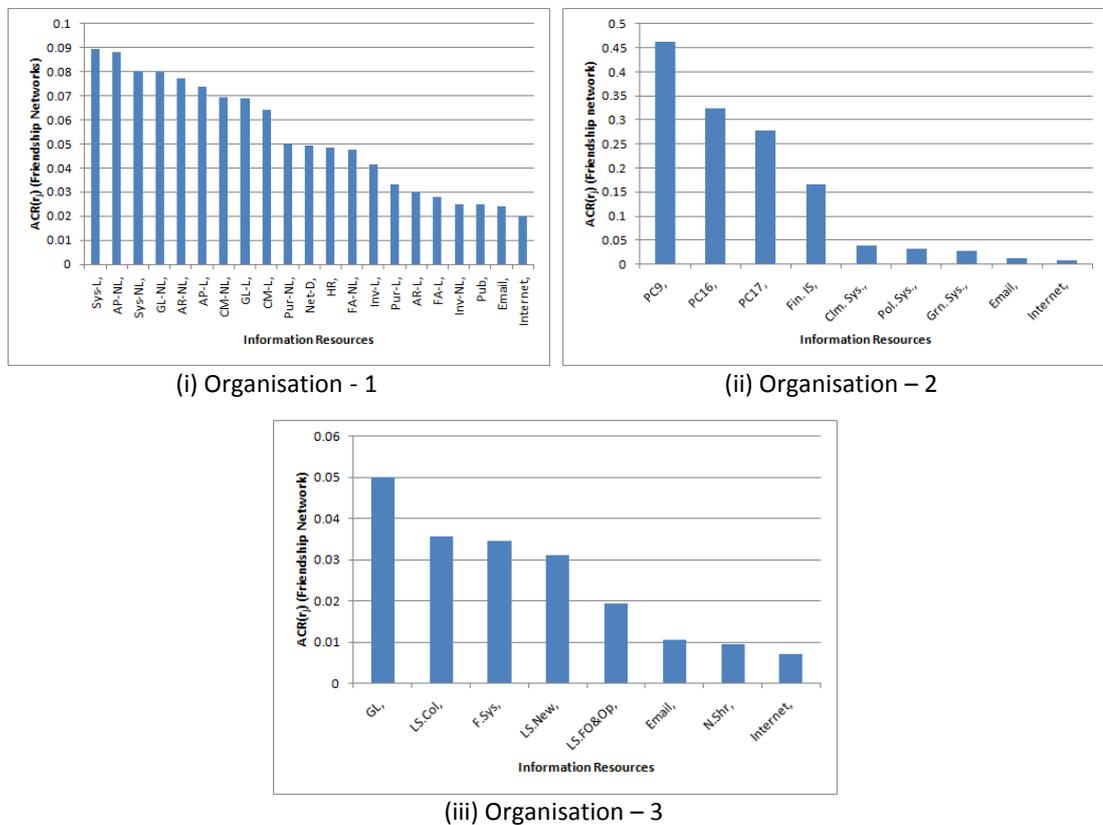
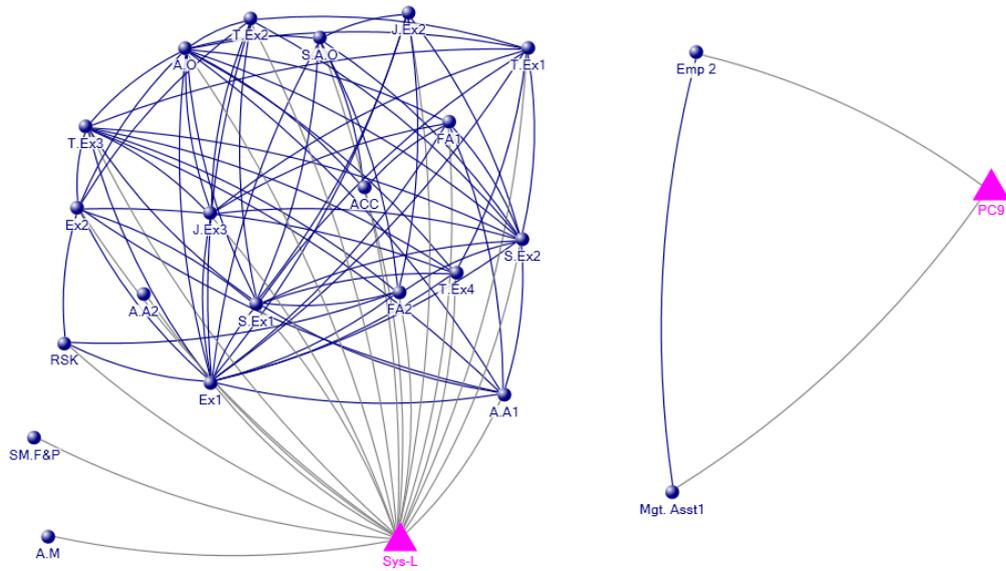
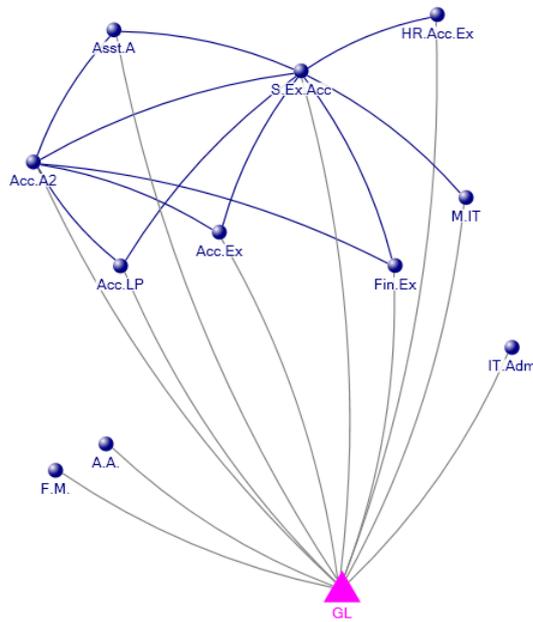


Figure 6-67 : Information resources receiving non-zero  $ACR(r_j)$  metric scores in the three organisations (calculated using the friendship networks)



(i) Information resource *Sys-L* in Organisation-1      (ii) Information resource *PC9* in Organisation-2



(iii) Information resource *GL* in Organisation – 3

Legend: ● Agent      ▲ Resource

Figure 6-68: Sub-networks illustrating resource access and friendship links related to three resources that score high  $ACR(r_j)$  values. Blue spheres represent agents and triangles represent information resources. The grey lines show resource access (agent  $\rightarrow$  resource) while blue lines indicate friendship (agent  $\rightarrow$  agent) links.

As shown in Figure 6-68(i), information resource *Sys-L* in Organisation-1 is accessible by twenty (20) agents out of which only three are isolates in the group. All other agents in the group are highly connected to each other. This result is a deviation from the observed pattern where resources accessible by a large number of agents have low  $ACR(r_j)$  scores. In Organisation-2, information resource *PC9* scores the highest risk value since two agents authorised to access this resource are linked by a friendship bond. Furthermore, the two authorised agents have been flagged for intrinsic risk properties and have higher composite agent risk ( $C_a$ ) values. The friendship links between agents accessing information resource *GL* in Organisation-3 is shown in Figure 6-68(iii). Although resource *GL* receives the highest metric score in Organisation-3, agents authorised to access this resource have relatively few friendship links between them when compared with the resources in the other two organisations. Furthermore, Organisation-3 record the lowest  $ACR(r_j)$  metric scores out of the three organisations indicating that the agent clustering around resources via the friendship network is not significant there.

### 6.5.6 Risks due to a closely associated group of agents performing a task

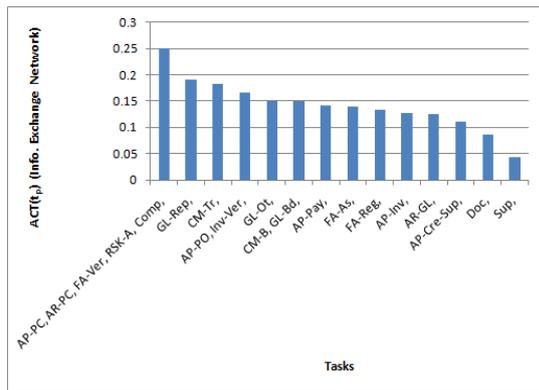
Similar to closely associated group of agents controlling a resource, a closely associated group of agents performing a task can also lead to collusion and increase the risk of insider threats. The ACT (Agent Clustering for Task) metric defined in section 5.6.4 can be used to quantify such risks. The next two sub-topics present the results of the risk assessment carried out using the ACT metric, which only has a task centric definition.

#### Agent clustering for a task due to information exchange networks

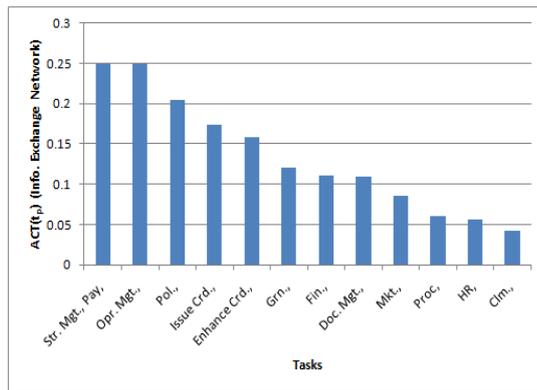
Figure 6-69 presents the  $ACT(t_p)$  risk scores of the tasks that receive non-zero risk values in the three organisations calculated using the information exchange relationships. According to the bar chart in Figure 6-69(i), five tasks receive the highest  $ACT(t_p)$  metric score in Organisation-1. All five tasks are performed by a pair of agents connected through an information exchange relationship resulting in a high metric score. Figure 6-70(i) depicts the agents assigned for the task receiving the second highest metric score - *GL-Rep* in Organisation-1 and information exchange links between the assigned agents. From the figure, it is clear that the eleven agents assigned for the task are highly connected via the information exchange links.

In Organisation-2, tasks – *Str. Mgt.*, *Pay* and *Opr. Mgt.* receive the highest metric values. Figure 6-70(ii) illustrates the agents assigned for the task *Opr. Mgt.* and information

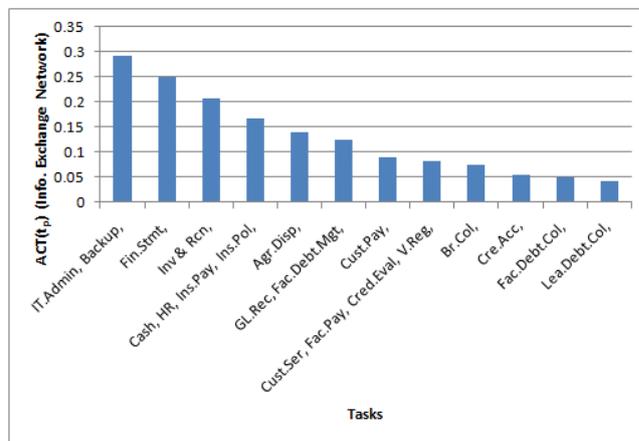
exchange relationships between them. Three agents are assigned for this task and all three are connected with each other. In Organisation-3, the three tasks obtaining the highest ACT( $t_p$ ) score are performed by a pair of agents linked through an information exchange relationship. Figure 6-70(iii) shows the agents assigned for the task receiving the fourth highest score (*Inv & Rcn*) and relationships between those agents. As shown in the diagram only one out of all possible links are missing in the group of agents performing the task - *Inv and Rcn*.



(i) Organisation - 1

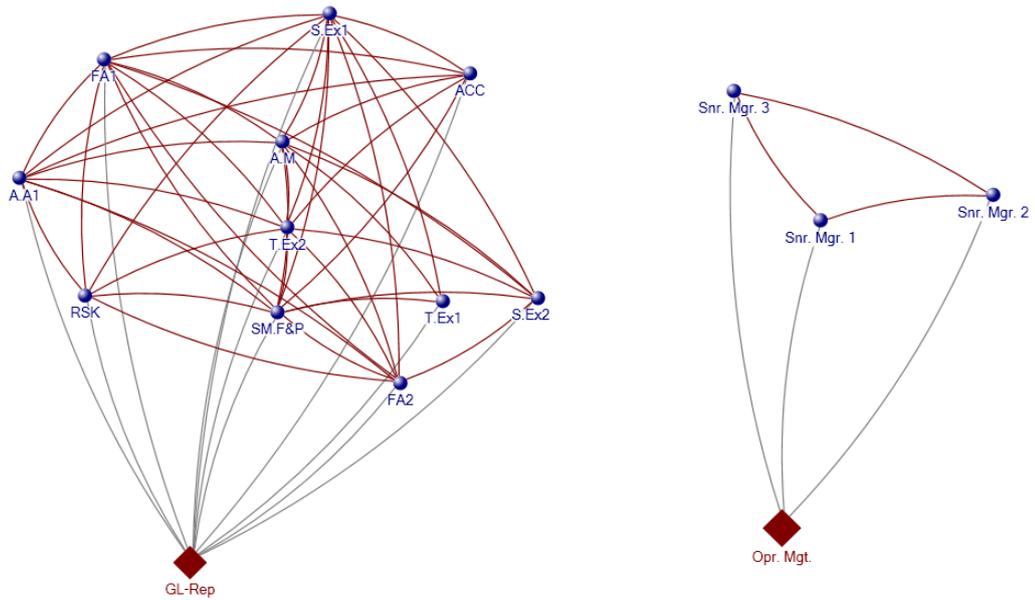


(ii) Organisation - 2



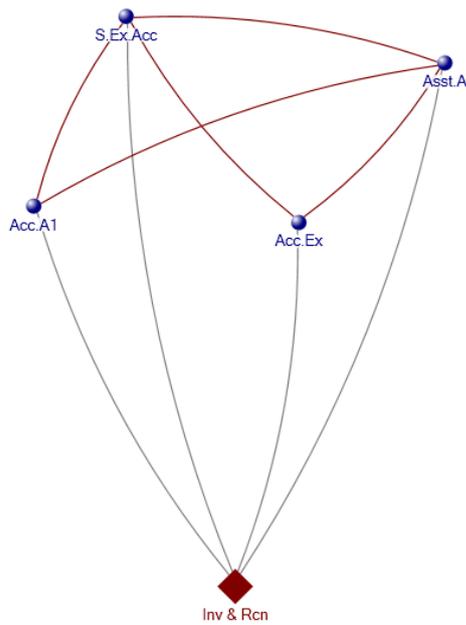
(iii) Organisation - 3

Figure 6-69: Tasks receiving non-zero ACT( $t_p$ ) metric scores in the three organisations (calculated using the information exchange networks)



(i) Task *GL-Rep* in Organisation-1

(ii) Task *Opr. Mgt.* in Organisation-2



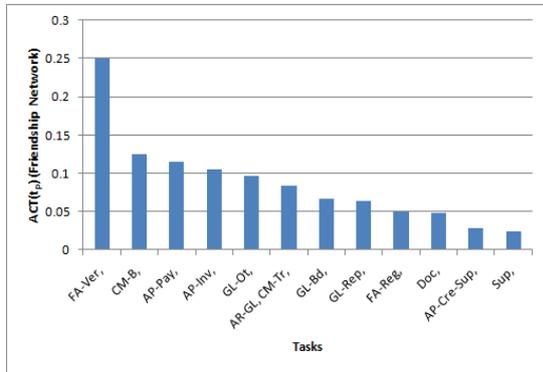
(iii) Task *Inv & Rcn.* in Organisation – 3



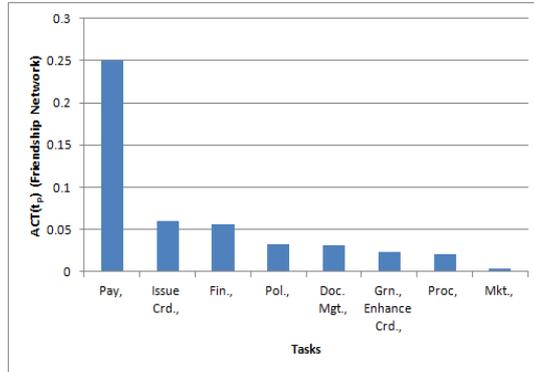
Figure 6-70: Sub-networks illustrating task assignment and information exchange links related to three tasks that score high  $ACT(t_p)$  values. Blue spheres represent agents and diamonds represent tasks. The grey lines show task assignment (agent  $\rightarrow$  task) while brown lines indicate information exchange (agent  $\rightarrow$  agent) links.

**Agent clustering for a task due to friendship networks**

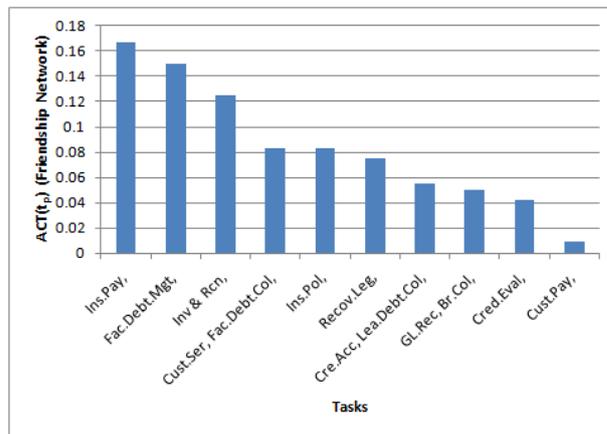
Figure 6-71 presents the  $ACT(t_p)$  risk scores of the tasks that receive a non-zero metric value calculated using the friendship links.



(i) Organisation - 1



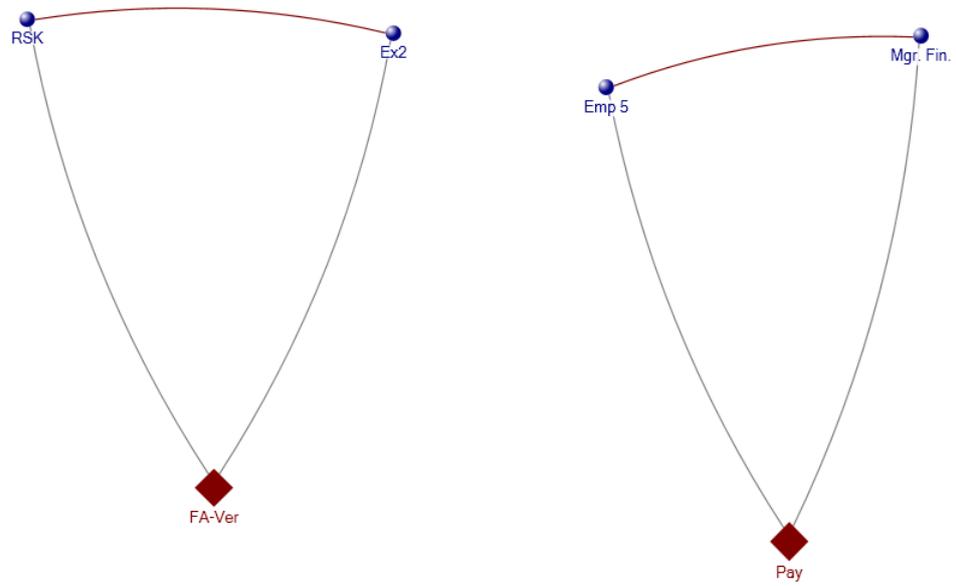
(ii) Organisation - 2



(iii) Organisation - 3

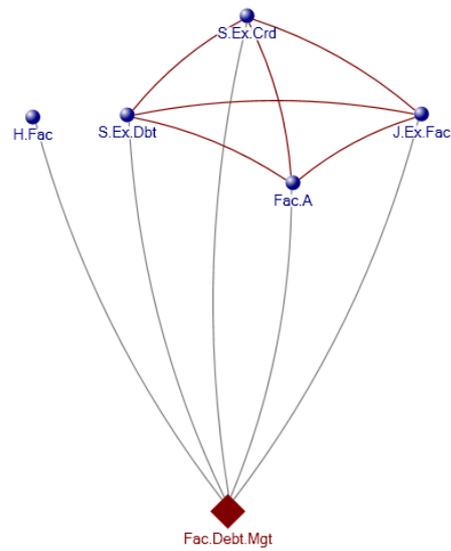
Figure 6-71: Tasks receiving non-zero  $ACT(t_p)$  metric scores in the three organisations (calculated using the friendship networks)

In all three organisations, the highest  $ACT(t_p)$  metric score occur due to a pair of agents, who are linked by a friendship link, controlling a task. Figure 6-72 (i) and (ii) illustrate the tasks that receive the highest metric scores in Organisation 1 and 2 and the relationships between the assigned agents while Figure 6-72 (iii) illustrate the same for the task receiving the second highest metric score in Organisation-3.



(i) Task *FA-Ver* in Organisation-1

(ii) Task *Pay* in Organisation-2



(iii) Task *Fac.Debt.Mgt.* in Organisation – 3



Figure 6-72: Sub-networks illustrating task assignment and friendship links related to three tasks that score high  $ACT(t_p)$  values. Blue spheres represent agents and diamonds represent tasks. The grey lines show task assignment (agent  $\rightarrow$  task) while brown lines indicate friendship (agent  $\rightarrow$  agent) links.

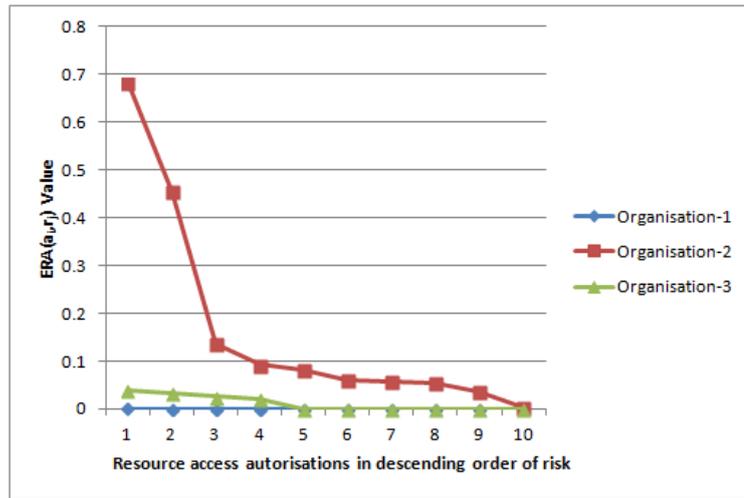
## 6.6 Summary and Discussion of the Results

### 6.6.1 Risks occurring due to resource access authorisations

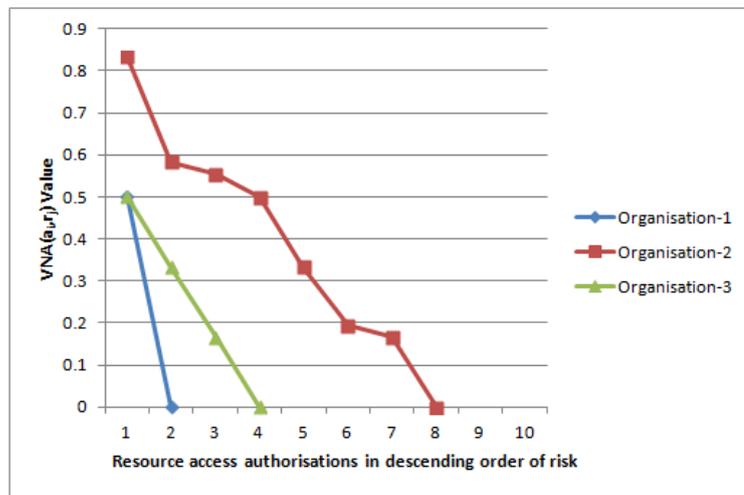
Four types of risks have been assessed under this category – agents having exclusive access to resources (risk assessed using ERA metrics), agents having exclusive administrative access to resources (risk assessed using EAA metrics), agents having access to resources not required for their tasks (risk assessed using VNA metrics) and agents having access to dependent information resources (risk assessed using the ADR metrics).

According to the results obtained for the three organisations, only a small proportion of agents carry high exclusive access risks. These high risks predominantly occur due to employees trusted with system administration duties having exclusive access to critical hardware systems of the organisations. Note that organisational units analysed in this research are relatively small ones (less than 50 agents) with one or two employees responsible for system administration duties. In the absence of system administrators in the data collected, as in the case of Organisation-1, managers usually receive high exclusive access risk scores.

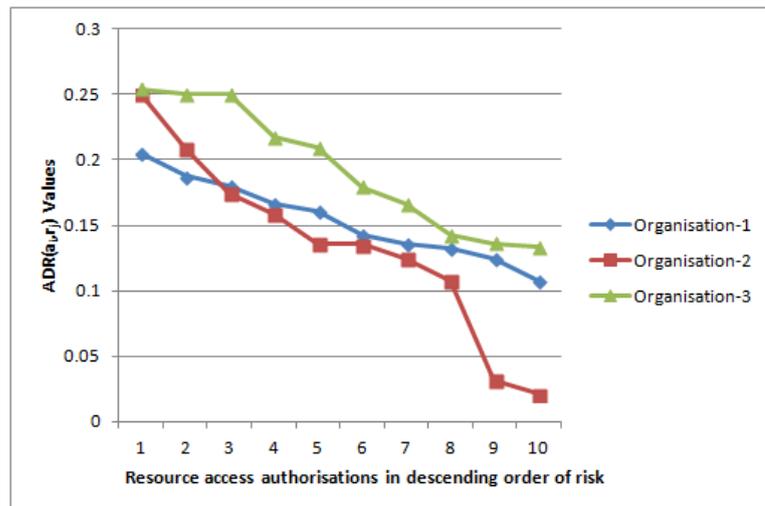
Figure 6-73(i) presents the  $ERA(a_i, r_j)$  risk scores of the top-ten resource access authorisations (in terms of the risk values) of the three organisations. How factors such as the number of agents accessing a resource, intrinsic risk properties of agents and resource criticalities affect the exclusive access risk scores can be demonstrated by comparing the  $ERA(a_i, r_j)$  metric scores of these resource access authorisations. As shown in Figure 6-73(i), the top-two risk values of Organisation-2 are very high when compared to other risk scores. These two points represent a single administrator having exclusive access to critical hardware resources. Furthermore, higher intrinsic risk value assigned to this employee also increases the metric value. In Organisation-3, there are at least two agents authorised for a resource and no agent has higher intrinsic risk values assigned to them. As a result, the  $ERA(a_i, r_j)$  risk values of the access authorisations take much lower values in Organisation-3. In the case of Organisation-1, there are at least four agents authorised to access a resource and no one has been assigned higher intrinsic risk values. Therefore, the risk scores of the access authorisations of Organisation-1 are almost negligible when compared with the other two organisations.



(i) Top-ten ERA(a<sub>i</sub>, r<sub>j</sub>) scores



(ii) Top-ten VNA(a<sub>i</sub>, r<sub>j</sub>) scores



(iii) Top-ten in ADR(a<sub>i</sub>, r<sub>j</sub>) scores

Figure 6-73: The risk score variations among resource access authorisations (agent → resource) receiving the top-ten risk values for the three metrics – (i) ERA(a<sub>i</sub>, r<sub>j</sub>), (ii) VNA(a<sub>i</sub>, r<sub>j</sub>) and (iii) ADR(a<sub>i</sub>, r<sub>j</sub>). Note that more than one resource access authorisation can have the same metric value.

In some cases, several agents can be authorised to access a resource but only one might have exclusive privileged (administrative) access rights. The EAA metrics quantify risks due to exclusive privileged access. According to the EAA metric results, agents who have exclusive access to a resource are usually authorised for privileged level of access to the same resource. For example, the same agents score the highest ERA( $a_i$ ) and EAA( $a_i$ ) metric scores in the three organisations.

Organisations should authorise agents to access information resources only if they are required for their job functions. Agents having excessive resource access authorisations violate the principle of least privilege and VNA metrics are used to assess such risks. According to the VNA( $a_i$ ) (agent centric) risk values, agents with excessive access authorisations are typically junior level managers or non-managerial staff. Most employees in Organisation-1 have access to at least one resource not required for their task. The excessive access risks are less common in the other two organisations. It must be noted that out of the three organisations, only the first one had well documented organisational tasks and processes. Therefore, granularity of the task assignments and the resource requirements of tasks were much better in the case of Organisation-1. This increased granularity could be a reason for the prevalence of need to access violations in Organisation-1. A comparison of the top-ten VNA risk values of the three organisations are given in Figure 6-73(ii). Organisation-2 scores the highest risk value out of the three organisations since the agents involved in the corresponding access authorisations have a higher composite agent risk value. Therefore, it is important for the Organisation-2 to take steps to mitigate this increased risk.

A another type of risk arising due to resource access authorisations is allowing agents to access dependent information resources thereby creating chances for sabotage, fraud or theft of information. According to the results obtained using the ADR metrics, agents entrusted with information systems administration duties and senior managers score high dependent resource access risk values. These two are the same employee categories that score high exclusive access risk values. A comparison of the top-ten dependent resource access risk values of the three organisations are presented in Figure 6-73(iii). Unlike the other risks due to resource access authorisations, all three organisations have comparable risk values in the case of dependent resource access.

### 6.6.2 Mitigation of risks occurring due to resource access authorisations

The results of the analysis of resource access authorisations provide insights in to insider security risks faced by organisations and action should be taken to mitigate the identified risks. With regards to exclusive access to resources, there are several methods to reduce the resulting risk metric values. These include authorising additional agents to access a resource and reassigning access to an agent with a lower intrinsic risk value. The ownership and the custodianship of an information resource should not be assigned to the same individual. In order to mitigate exclusive privileged access risks organisations can deploy tools such as Privilege Account Management (PAM) (Allan 2013). Furthermore, supervision, monitoring and configuration management controls should be introduced to control privileged access. For small organisations, like the ones analysed in this research, it may not be possible to have a group of system administrators sharing access to information resources. In such cases outsourcing some of the information systems administration and security functions may mitigate risks due to administrators having exclusive access although it has to be carried out after careful assessment of risks due to outsourcing. As an example, in Organisation-2, despite having administrative access to hardware systems, systems administrator does not have privileged access to the core business software systems which are managed by a third party service provider. If the administrator had access to these systems, it would have increased the exclusive privileged access risks of the organisation further.

Mitigating risks due to agents having access to resources not required for their tasks is straightforward since organisations can simply revoke excessive authorisations. In some cases, organisations might grant temporary authorisations for certain agents. Such temporary authorisations must be revoked once the task is fulfilled. Organisations must also ensure that previous access authorisations of an agent is revoked when he is reassigned to a new role to prevent a phenomenon known as “access creep” (Carpenter and Walls 2011), where an agent accumulates access authorisations to different systems over a period of time.

Risks occurring due to an agent having access to two dependent information resources should be mitigated by allowing a single agent to access only one of the dependent resources. It will be equivalent to implementing dual control (Ward and Smith 2002) where any task requiring both information resources should only be carried out with the collaboration of two or more agents.

### 6.6.3 Risks occurring due to task assignments

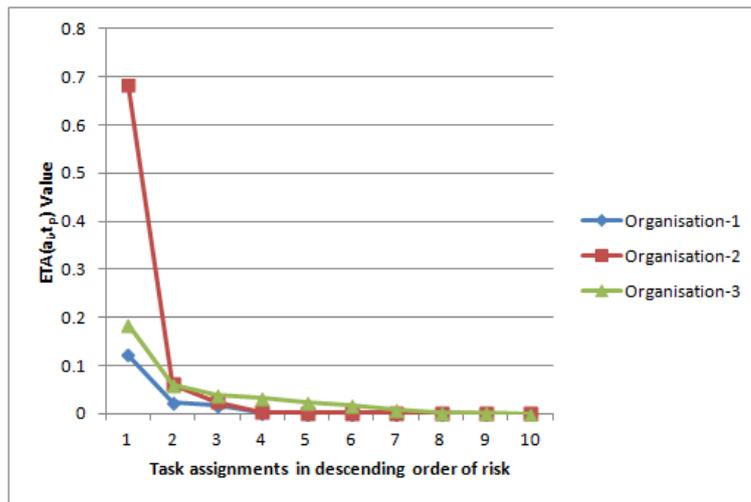
Two types of risks have been assessed under this category – agents exclusively performing tasks (risk assessed using the ETA metrics) and agents performing dependent tasks (risk assessed using the ADT metrics). According to the results, only a small percentage of tasks in each organisation are performed exclusively. However, there are some critical tasks in that score high exclusive task assignment risk values. Examples include *RSK-A* (risk assessment) and *Comp.* (compliance) in Organisation-1, *IT. Admin* (IT systems administration) in Organisation-2, *Fin. Mgt.* (financial management), *Compl.* (compliance), *Tax* (taxation), *Audit* (internal audit), *IT. Proc* (IT systems acquisition, recommendation and procurement) and *IT.Admin* (IT systems administration) in Organisation-3. In an agent perspective, employees dealing with IT system administration tasks and managers have the most number of exclusive task assignments. This task assignment pattern creates serious insider risks in organisations, especially considering the fact that the same categories of agents also have exclusive access to information resources as pointed out previously. Figure 6-74(i) compares the top-ten exclusive task assignment risk values of the three organisations. According to the graph, there is one strikingly high risk value in Organisation-2. This value occurs due to agent - *Emp2*, who has a high composite risk attribute value, performing task - *IT Admin* exclusively. The risk is significant since the agent has been flagged for concerning behaviour (resulting in the high composite agent risk) and the task being performed by the agent (IT systems administration) is a critical one.

As in the case of exclusive task assignments only a small percentage of agents have access to dependent tasks. Although some agents with IT system administration roles are assigned to dependent tasks majority of the dependent task assignments are associated with regular employees. Task assignments of managers in the three organisations contribute very little toward this type of risk. Furthermore, dependent task assignment risks in Organisation-1 are much less severe than that of other two organisations as shown in Figure 6-74(ii).

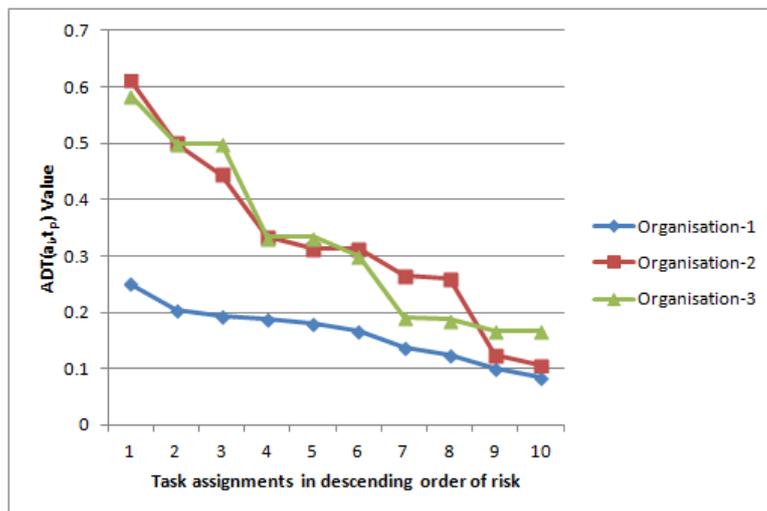
### 6.6.4 Mitigation of risks occurring due to task assignments

Risks occurring due to task assignments can be mitigated by the enforcement of separation of duty. Tasks that are performed exclusively by agents can be divided in to sub-tasks and a different agent can be assigned for each of the sub-tasks. Alternatively, an agent can be assigned to supervise the task. The same agent should not be assigned for

dependent tasks that can result in a conflict of interest. The simplest way to implement separation of duty is to enforce it as a static principle (static separation of duty) (Ferraiolo and Kuhn 1992; Sandhu et al. 1996) where an agent is not assigned to two conflicting tasks. However, if this requirement is too stringent organisations can implement the principle in a dynamic manner (dynamic separation of duty) (Simon and Zurko 1997; Sandhu, Ferraiolo, and Kuhn 2000), provided that organisational information systems are capable of such an implementation.



(i) Top-ten ETA ( $a_i, t_p$ ) scores



(ii) Top-ten ADT( $a_i, t_p$ ) scores

Figure 6-74: The risk score variations among task assignments (agent → task) receiving the top-ten risk values for the two metrics – (i)  $ETA(a_i, t_p)$  and (ii)  $ADT(a_i, t_p)$ . Note that more than one task assignment can have the same metric value.

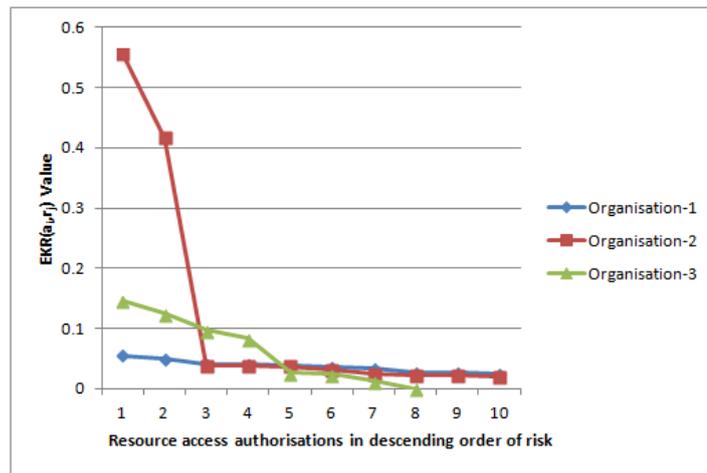
### **6.6.5 Risks occurring due to knowledge requirements**

Two types of risks are assessed under this category – agents having exclusive knowledge to operate a resource (risk assessed using EKR metrics) and agents having exclusive knowledge to perform a task (risk assessed using EKT metrics). According to the results, agents who perform IT system administration and managerial roles have high risks due to exclusive knowledge with regards to resources. The most severe of these risks occur due to IT systems administrators having exclusive knowledge to utilise critical hardware and software resources of organisations. Similarly, IT systems administrators having exclusive knowledge with regards to information systems administration and maintenance tasks is a major contributory factor for risks occurring under the knowledge requirements category. According to the graphs given in Figure 6-75, conspicuously high risk scores occur in Organisation-2 for both metrics. These conspicuous risk scores occur since the IT systems administrator of the organisation has been assigned a high composite risk attribute value due to the observation of agent's concerning behaviours.

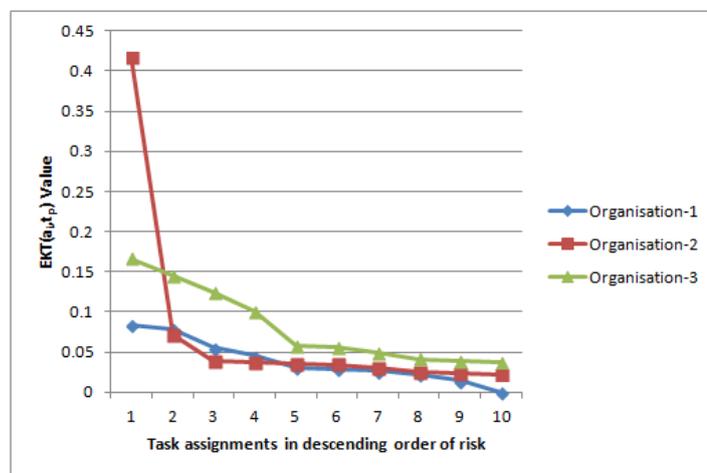
### **6.6.6 Mitigation of risks occurring due to knowledge requirements**

In order to mitigate risks occurring due to knowledge requirements multiple staff members must be trained to handle a given information resource or perform a specific task. Smaller organisations might have budgetary constraints that prevent them from providing specialised training to multiple staff members with regards to a task or an information resource. In such instances, providing in-house cross training may be a viable option. Moreover, enforcing administrative controls such as mandatory leave requirements enables organisations to train multiple staff members to handle tasks or resources that have specialised knowledge requirements.

In the three organisations, exclusive knowledge risks specially occur in relation to information systems administration. A malicious systems administrator can take advantage of this situation as described in case 1 and 4 in Table 4-1 to compromise information systems of the organisation. Under such circumstances organisation will not have the capability to detect, investigate, contain and recover from an insider threat event. Therefore, it is important for organisations to review their incident response capabilities in terms of information systems security. If the organisations lack in-house capabilities they must maintain regular contacts with organisations such as Computer Emergency Response Teams (CERT) to obtain their support during a security incident.



(i) Top-ten EKR (a<sub>i</sub>, r<sub>j</sub>) scores



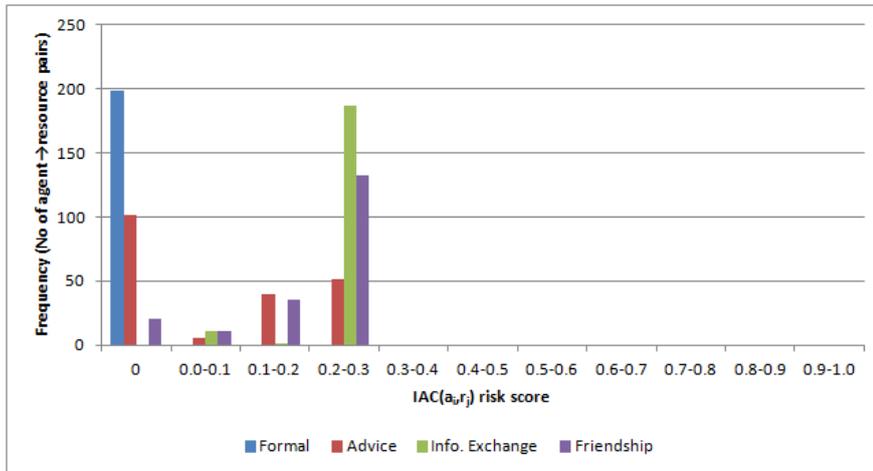
(ii) Top-ten EKT (a<sub>i</sub>, t<sub>p</sub>) scores

Figure 6-75: The variations in the top-ten risk values for the two metrics – (i) EKR(a<sub>i</sub>, r<sub>j</sub>) and (ii) EKT(a<sub>i</sub>, t<sub>p</sub>). Note that more than one resource access authorisation or task assignment can have the same metric value.

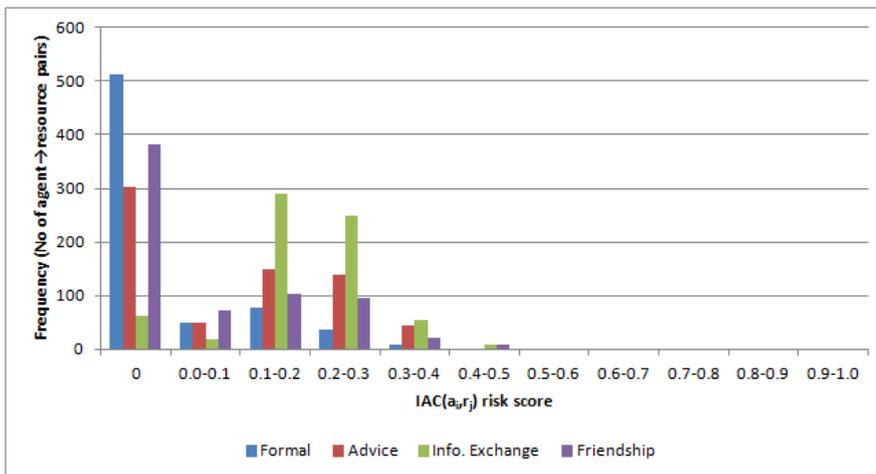
### 6.6.7 Risks occurring due to social relationships combined with resource authorisations or task assignments

Five types of risks were assessed under this category – agents having indirect access to resources through the social networks (risk assessed using the IAC metrics), agents having transitive access to dependent information resources (risk assessed using the TAR metrics), agents having transitive access to dependent tasks (risk assessed using the TAT metrics), a closely associated group of agents controlling a resource (risk assessed using ACR metrics) and a closely associated group of agents controlling a task (risk assessed using ACT metrics). Each of the risks were assessed repeatedly using four different social networks in each organisation – formal reporting structure, advice relationships, information exchange networks and friendship networks. Figure 6-76 presents the frequency of occurrence (number of *agent* → *resource* combinations) of the indirect access risk scores through the

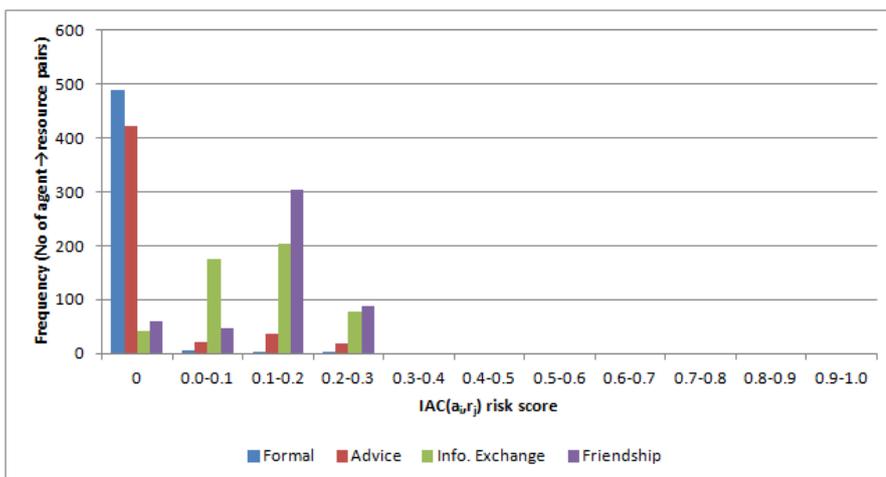
four social networks. Note that only  $agent(a_i) \rightarrow resource(r_j)$  combinations where the  $agent(a_i)$  cannot directly access the  $resource(r_j)$  have been counted.



(i) Organisation-1



(ii) Organisation-2



(iii) Organisation-3

Figure 6-76: The frequency of occurrence (number of agent  $\rightarrow$  resource combinations) of the  $IAC(a_i, r_j)$  risk scores through the four different types of social networks.

Only combinations where the agent ( $a_i$ ) cannot directly access the resource ( $r_j$ ) have been counted.

As evident from the bar charts in the Figure 6-76, no agent, resource combination receives an  $IAC(a_i, r_j)$  (i.e., indirect access risk) score above the range 0.4-0.5. According to the metric definition, an agent typically needs to have direct access to a resource to obtain values above this range. A risk value of zero indicates that an agent cannot access the relevant resource via the social network used. According to the bar-charts in Figure 6-76, many agent - resource combinations receive a risk score of zero via the formal reporting and advice networks. This trend is especially apparent for the formal reporting networks since only a very few non-zero risk scores occur through them. For example, in Organisation-1, no agent obtains indirect access to a resource through the formal reporting structure and corresponding  $IAC(a_i, r_j)$  risk values are zero. On the other hand, many non-zero  $IAC(a_i, r_j)$  risk scores occur through the information exchange and friendship networks.

There can be several reasons for the increased likelihood of indirect access through information exchange and friendship networks when compared to the other two social networks. First, this research models information exchange and friendship links as mutual (or reciprocated) where as formal reporting and advice networks are directional. Therefore, the hierarchical structure of formal reporting and advice networks only gives supervisors indirect access to resources held by subordinates and not vice versa. This severely limits the indirect access pathways through the formal reporting and advice networks. Furthermore, in the case of formal reporting networks, which create the highest number of zero  $IAC(a_i, r_j)$  metric values, supervisors are typically expected to have direct access to the information resources held by their subordinates. Second, unlike formal reporting networks, information exchange and friendship networks can link people from different departments and workgroups together, thereby creating indirect access pathways to resources controlled by people outside the department or a workgroup. This can result in many non-zero  $IAC(a_i, r_j)$  values through the information exchange and friendship networks.

Out of the  $IAC(a_i, r_j)$  values of the three organisations, depicted in Figure 6-76, the information exchange and friendship networks of Organisation-2 each produce nine values in the range of 0.4-0.5. These are the highest indirect access risk scores obtained across all three organisations. Figure 6-77 highlights nine of these indirect access pathways that occur through the friendship network of Organisation-2. All nine pathways relate to the potential of agent labelled *Mgt. Asst1* obtaining access to information resources with high sensitivity/criticality through the agent labelled *Emp 2*, who is the systems administrator. Both these agents have also been flagged for concerning behavioural characteristics

resulting in higher agent risk attribute values ( $C_a(a_i)$ ). Since all above factors are considered in the risk metric calculation, indirect access pathways highlighted in Figure 6-77 receive relatively high scores. Organisation-2 should be especially concerned about the potential for indirect access through these pathways.

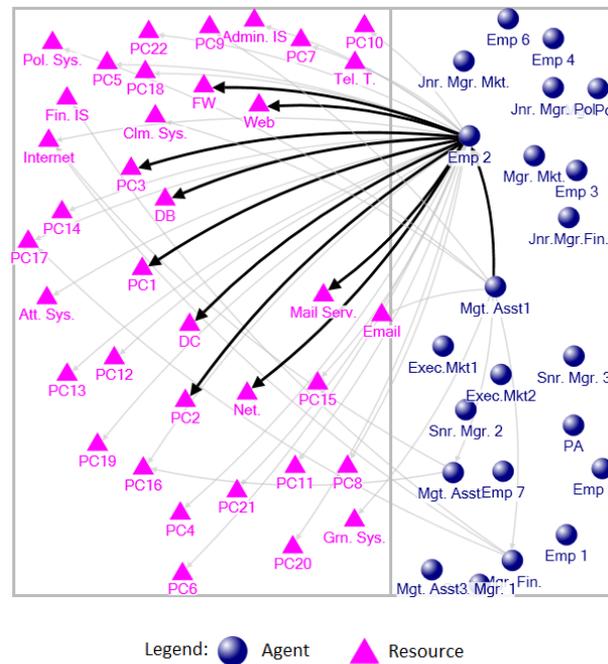
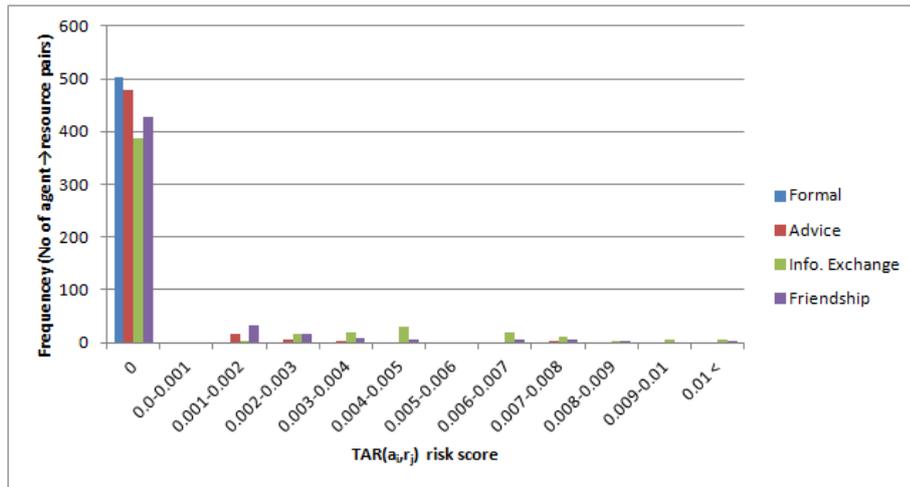
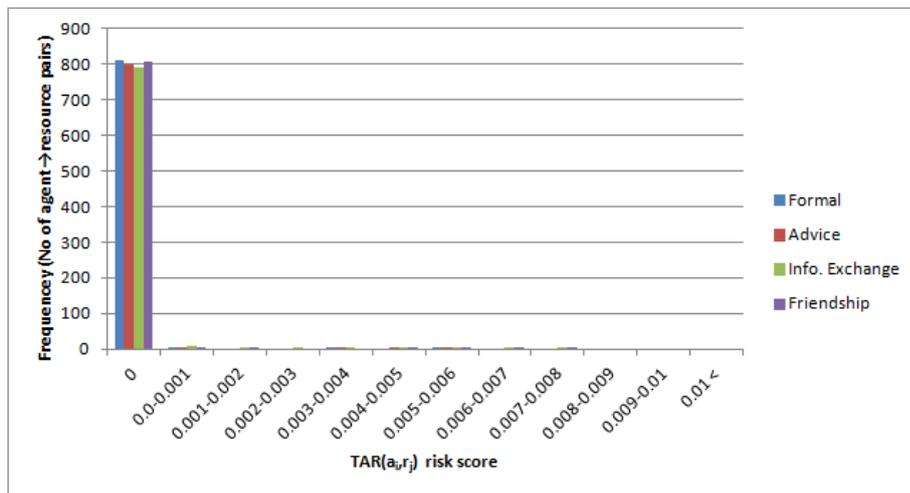


Figure 6-77: Indirect access pathways via the friendship network of Organisation-2 that result in highest risk scores.

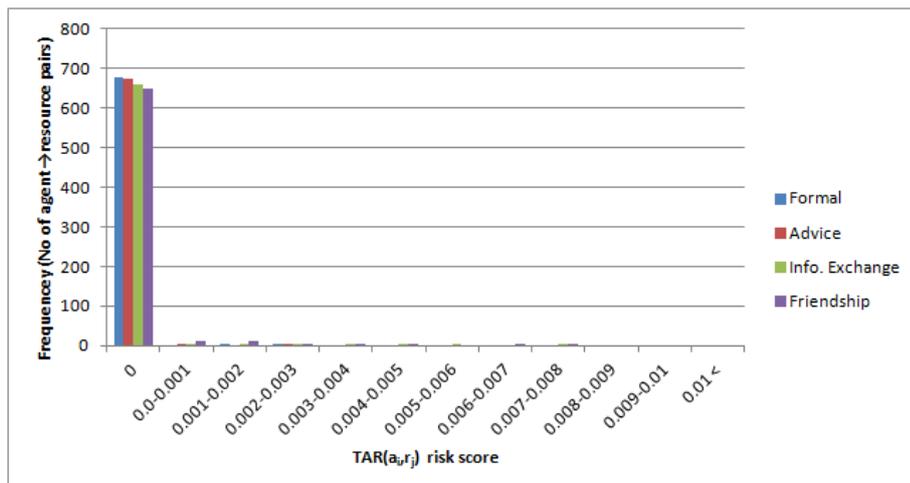
In terms of the risk of agents obtaining transitive access to dependent information resources, vast majority of the agent, resource combinations receive a zero risk value through all four types of social networks as illustrated in Figure 6-78 which presents the frequency of occurrence of  $TAR(a_i, r_j)$  values in the three organisations. However, there are a few considerably high risk scores that occur via the information exchange and friendship networks. For example, in Organisation-1, five transitive resource access possibilities receive risk scores over 0.01 via the information exchange network while another two receive similar scores via the friendship network. Organisations should pay attention to these transitive access possibilities with a high risk score when designing access control policies and procedures. Similar to the transitive access to dependent information resources, vast majority of the agent, task combinations in the three organisations receive metric scores of zero for risks due to transitive assignment to dependent tasks. Nevertheless, there are a few significant risk scores that require the attention of the organisations as described in section 6.5.4.



(i) Organisation-1



(ii) Organisation-2



(iii) Organisation-3

Figure 6-78: The frequency of occurrence (number of agent →resource combinations) of the TAR(a<sub>i</sub>,r<sub>j</sub>) risk scores through the four different types of social networks.

A closely associated group of agents controlling a resource is another type of socio-technical risk assessed in the three organisations. In terms of this risk, the general trend is that information resources accessible by many agents score lower  $ACR(r_j)$  metric scores while information resources accessible by two or few agents score larger metric values. The same trend is observed for the risk of closely associated group of agents controlling a task. The probability of agents being connected with each other decreases as the number of agents increase in a group. Therefore, this trend can be expected as a result of the  $ACR(r_j)$  and  $ACT(t_p)$  metric definitions.

### **6.6.8 Mitigating risks occurring due to social relationships combined with resource authorisations or task assignments**

Mitigating risks occurring due to social relationships combined with resource authorisations or task assignments are not as straightforward as mitigating other categories of risks since they do not directly violate security best practices. For example, an agent directly assigned to two dependent tasks violates the principle of separation of duty while the possibility of an agent obtaining transitive access to dependent resources through the social network does not violate any security principles. From the analysis of the three organisations, it is clear that major risks under this category occur through the information exchange networks, which contain both formal and informal relationships and friendship networks, which are completely informal. Organisations have limited leverage over such informal networks using conventional management strategies.

However, still there are many risk mitigation options available for organisations. According to McCulloh et al. (2013), formation and maintenance of social relationships are controlled by six primary social forces – prestige, reciprocity, homophily, proximity, transitivity and balance. Organisations can utilise or influence these social forces to control the structure of social interaction networks to an extent. In case of extremely high risks, organisations can reassign agents to different tasks or change their access authorisations. Changing the job role of an agent or assigning the agent to a different group or a department may change the information exchange and friendship relationships. However, organisations must be cautious in doing this since changes in the relationships can also introduce new types of risks. For example, changing the job roles of an employee can result in an increase in knowledge which in turn can pose new risks. Risk metrics can also be used to evaluate the reduction of the amount of risk due to such risk mitigation steps.

In the case of indirect access to information resources, some agents act as gatekeepers in many short access pathways. Organisations can provide information security awareness training for such employees to ensure that they are aware of the organisational policies as well as risks of information sharing. Information security policies and procedures of the organisations can also be modified to mitigate certain risks. The agents and resources obtaining high risk scores can also be targeted for increased monitoring.

Organisations must also be aware that optimising social relationship structures according to security requirements can be at odds with other organisational performance goals such as the speedy diffusion of knowledge, information and innovation. For example, limiting information exchange pathways might not only reduce security risks but it might also have an adverse effect on organisational performance. Therefore, organisations must strive to strike a balance between information security requirements and other organisational goals.

## 6.7 Chapter Summary

The objective of Chapter 6 is to discuss the results obtained by applying the risk assessment methodology to data collected from the three organisations introduced in Chapter 4. The information systems access security risks in the three organisations have been assessed using the thirteen metrics defined in Chapter 5. Each metric provides multiple perspectives of security risks such as agent centric, resource centric, access authorisation centric etc.

According to ISO/IEC 27005:2011 - *Information technology - Security techniques - Information security risk management standard* (International Organisation for Standardisation 2011) information systems security risk assessment consists of three activities. The first activity, called *risk identification*, deals with the identification of information resources, security threats faced by them, vulnerabilities in resources and existing controls. Identification of threats and vulnerabilities has been covered already in Chapter 5. The identification of information resources of the three organisations were carried out during the second data collection phase described in Chapter 4. Contents of this chapter primarily aligns with the other two risk assessment tasks specified in ISO/IEC 27005:2011 – *risk analysis* and *risk evaluation*.

The end goal of the *risk analysis* activity in ISO/IEC 27005:2011 is to produce estimates of risk levels either qualitatively or quantitatively. The results of the metric calculations provide quantitative risk values presented in this chapter fulfilling this goal. The *risk*

---

*evaluation* activity in ISO/IEC 27005:2011 is concerned with making risk mitigation decisions based on the risk values obtained during the risk analysis phase. The visualisations of risks presented in this chapter, using heat-maps and network diagrams, allow analysts to identify causes of the high risk values and to make risk mitigation decisions. Section 6.6 discusses common causes of high risk scores and possible actions that organisations could take in order to mitigate them. Therefore, it is clear that the information systems access risk assessment methodology developed in this research covers the entire risk assessment functionality specified in the ISO/IEC 27005:2011 standard.

## 7. Evaluation and Conclusions

This chapter first discusses the final evaluations of the research outcomes that were carried out using three case studies as well as a workshop conducted with the participation of security professionals. Then, the compatibility of the methodology with existing risk assessment standards and frameworks, conclusions made regarding the methodology and directions for future research are discussed. The progression of topics in the chapter is given in Figure 7-1.

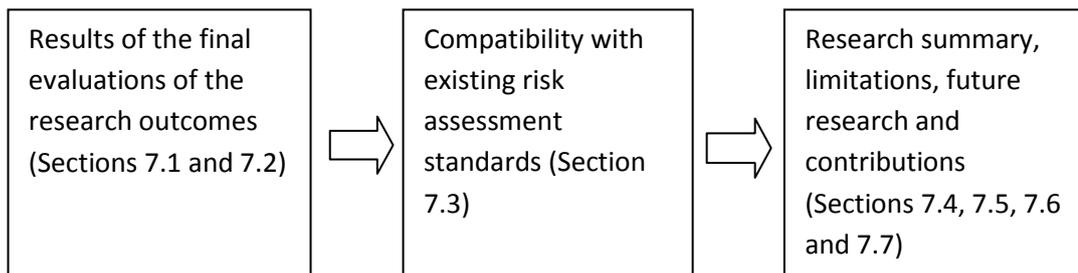


Figure 7-1: Arrangement of chapter sub-topics

### 7.1 Evaluation carried out by Information Security Professionals

As described in Section 4.3 of Chapter 4, artefacts developed in this research were evaluated during a workshop conducted with the participation of information security professionals by obtaining their responses to the questionnaire given in Appendix B. The questionnaire consisted of two types of questions – fixed choice and open-ended. The fixed-choice questions contained responses in a Likert-type (Likert 1932) scale while open-ended questions probe evaluators opinions further on the artefacts and possible improvements. A total of twenty-one (21) responses were obtained for the questionnaire.

The evaluation questionnaire obtained the evaluators' opinions on four separate aspects of the research outcomes. The first aspect evaluated the results produced by applying the methodology against the research objectives and the initial utility theory (Section 7.1.2). The other three aspects evaluated the risk assessment model (Section 7.1.3), method (Section 7.1.4) and metrics (Section 7.1.5) using criteria such as ease of use, validity and accuracy.

#### 7.1.1 Background of the Evaluators

All evaluators participated in the workshop had some background related to information systems security. Figure 7-2 presents the distribution of evaluators that participated from

each organisation sector while Figure 7-3 presents the number of evaluators that participated from organisations of different size (in terms of the number of employees). The majority of the evaluators (10) were from the Finance Sector Organisations while there were five and four people representing the ICT Services and Education Sectors respectively. One participant indicated that his organisation belonged to two sectors. It was important to have a majority from the Finance Sector since the data used for the analysis has been collected from the organisations belonging to the same sector. In terms of the organisation size, majority of the evaluators came from organisations with more than three hundred employees.

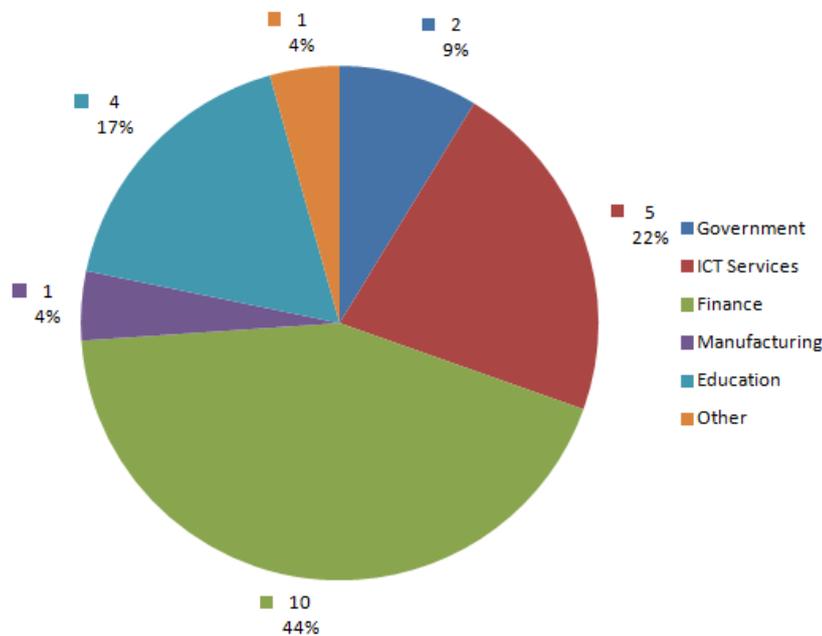


Figure 7-2: Distribution of evaluators participated from each organisation sector. Data labels show both the number of evaluators (number on top) and the percentage

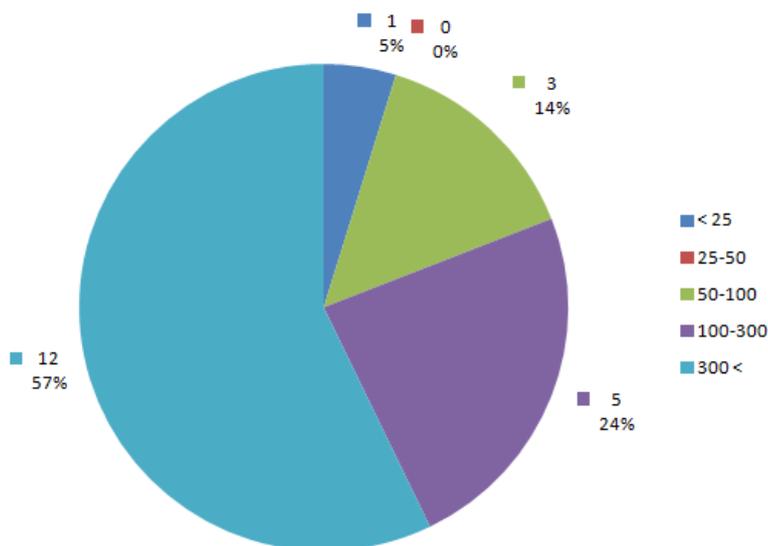


Figure 7-3: Number of evaluators from organisations of different size (based on the number of employees). Data labels show both the number of evaluators (number on top) and the percentage

Figure 7-4 shows the distribution of evaluators based on their job roles in organisations. Majority of the evaluators (13) are IT/Security Administrators. There were five Department Managers/Information Owners among the group. Three evaluators selected “other” category for their job role and all three indicated they are IT Security Auditors. The cumulative of the job roles is greater than the number of evaluators since some of them reported performing multiple job roles.

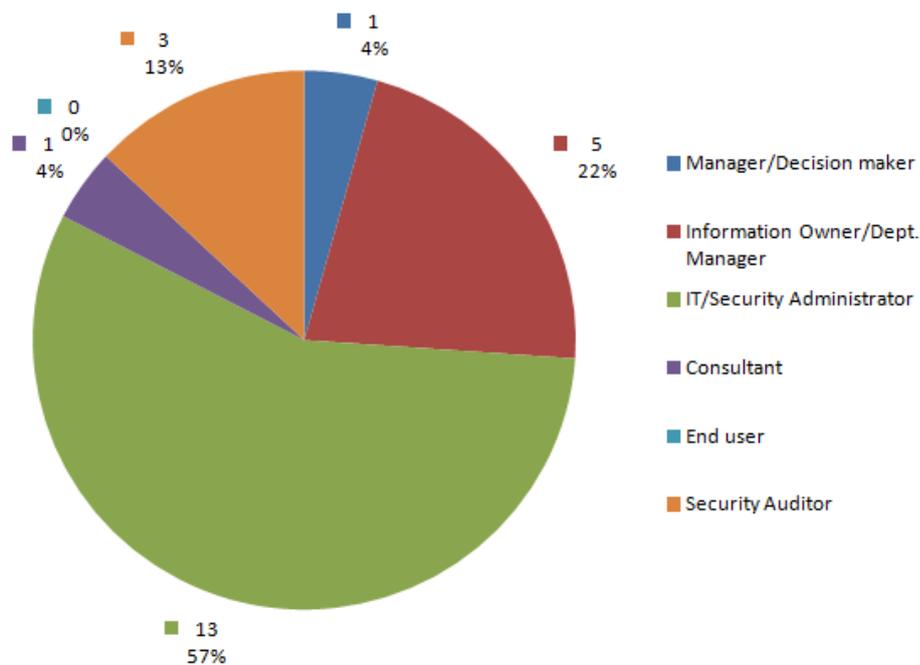


Figure 7-4: Job roles of evaluators in their organisations. Data labels show both the number of evaluators (number on top) and the percentage

### 7.1.2 Evaluation of the results produced by following the methodology

As stated in Chapter 3, the primary objective of the research is to develop a methodology (incorporating a risk assessment model, method and metrics) to assess security risks occurring due to organisational information systems access. The methodology is expected to provide necessary information for organisations to make access risk mitigation decisions thereby reducing the likelihood of insider security breaches. Furthermore, the initial utility theory is stated in Chapter 3 (page 68) as “*A socio-technical risk assessment methodology would help organisations to effectively assess information systems access risks that contribute to insider security breaches.*”

The results produced by applying the methodology must be evaluated against the research objectives and the utility theory. Therefore, the evaluators were asked three questions related to validity and usability of the results produced by the methodology. The three related evaluation criteria are stated below:

1. Usefulness of the results in the assessment of socio-technical access risks in organisations
2. Applicability of the results in improving the overall access risk awareness of the organisations
3. Effectiveness of the results in communicating access risks to the decision makers

The first two criteria evaluate the validity of the results while the last criterion is related to the usability.

**Criterion 1: Usefulness of the results in the assessment of socio-technical access risks in organisations**

In order to determine the usefulness of the results produced by the methodology in assessing of socio-technical access risks in organisations, the evaluators responded to the following question:

- *Do you think the results produced in the analysis are helpful in the assessment of socio-technical access risks in your organisation?*

The responses given for the above question are illustrated in Figure 7-5.

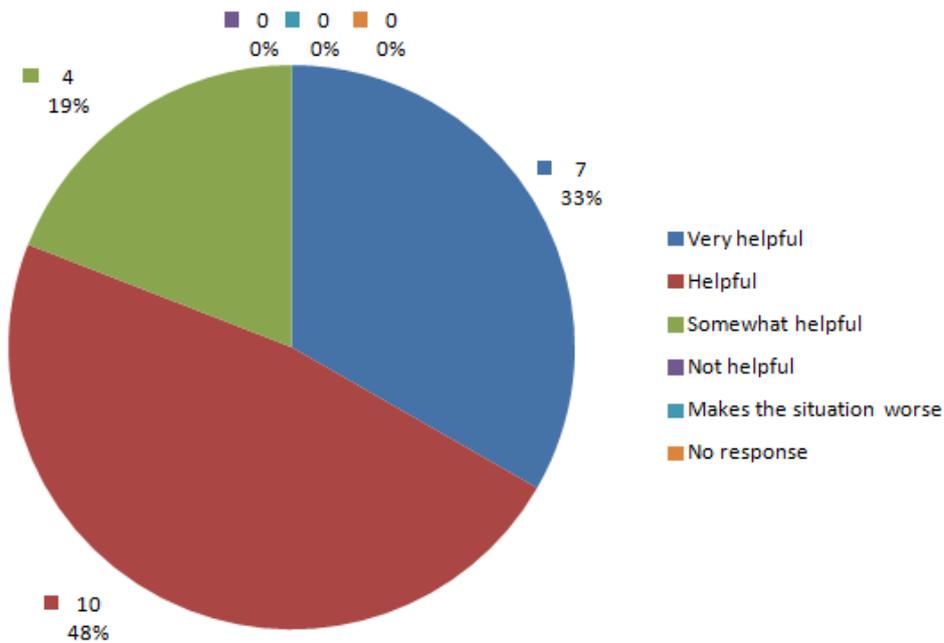


Figure 7-5: Evaluators’ opinions on the usefulness of the results in the assessment of socio-technical access risks in organisations. Data labels show both the number of evaluators (number on top) and the percentage

A great majority of the evaluators (81%) believe that the results produced by applying the methodology are either “very helpful” or “helpful” in the assessment of socio-technical access risks in organisations. The remaining evaluators (19%) feel that the results are “somewhat helpful” for the same purpose. Therefore, there is wide agreement among the evaluators that the results produced by the methodology are useful in assessing of socio-technical access risks in organisations.

### **Criterion 2: Applicability of the results in improving the overall access risk awareness of the organisations**

The evaluators answered the following question in order to determine the level of applicability of the results in improving the overall access risk awareness of the organisations:

- *Will the results improve overall access risk awareness of your organisation?*

The evaluators’ responses for the above question are illustrated in Figure 7-6.

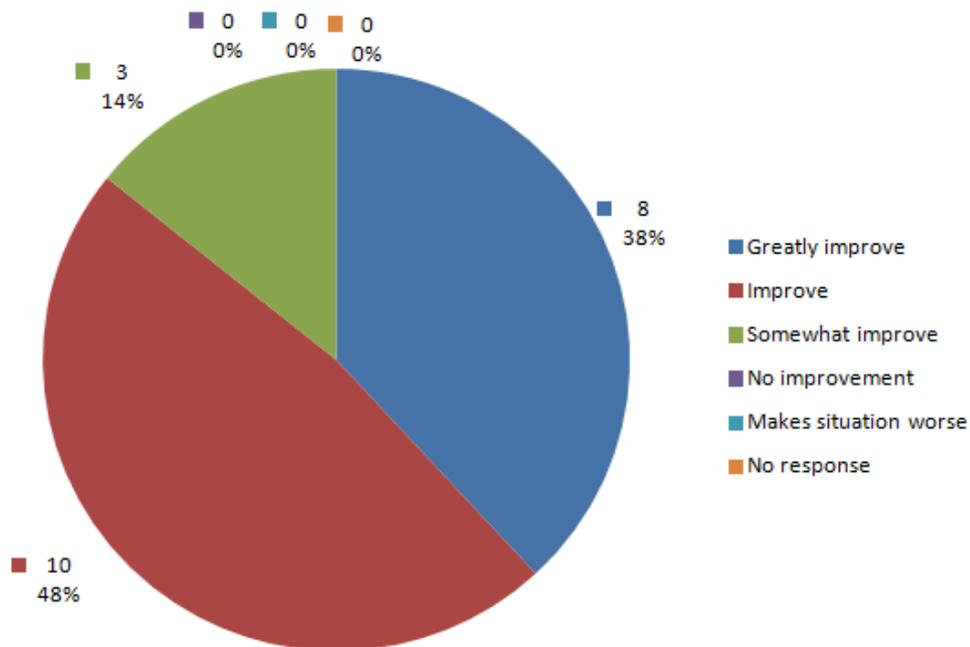


Figure 7-6: Evaluators’ opinions on the applicability of the results in improving the overall access risk awareness of the organisations. Data labels show both the number of evaluators (number on top) and the percentage

Most of the agents (86%) believe that the results produced by applying the methodology would either “greatly improve” or “improve” the overall access risk awareness of the

organisation. Rest of the evaluators (14%) feel that the results “somewhat improve” the risk awareness. Therefore, evaluators clearly agree that the risk assessment methodology provides applicable results that would increase the access risk awareness of organisations.

### Criterion 3: Effectiveness of the results in communicating access risks to the decision makers

The evaluators answered the following question in order to determine the effectiveness of the results in communicating access risks to the decision makers:

- *How effectively do the results produced by the metrics combined with the visualisations communicate the risks to the decision makers?*

The evaluators’ responses to the above question are illustrated in Figure 7-7.

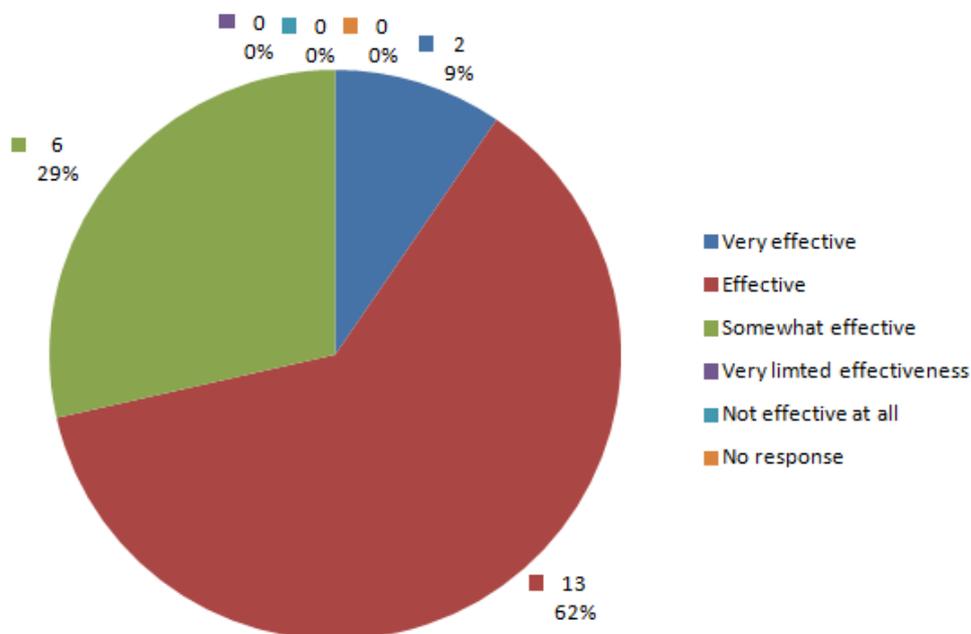


Figure 7-7: Evaluators’ opinions on the effectiveness of the results in communicating access risks to the decision makers. Data labels show both the number of evaluators (number on top) and the percentage

Majority of the evaluators (71%) believe that the result communicate access risks to the decision makers either “very effectively” or “effectively”. The rest of the evaluators (29%) feel that the results communicate access risks “somewhat effectively”. Although there is wide agreement among the evaluators on the effectiveness of the results in communicating access risks to the decision makers, a lesser number of them are convinced when compared with the Evaluation Criteria 1 and 2.

### 7.1.3 Evaluation of the risk assessment model

Two main criteria were used to evaluate the risk assessment model and its elements presented in Section 5.2. The second criterion can be further sub-divided as given below:

1. The ability of the model to represent important socio-technical interactions.
2. Ease of instantiating the model.
  - a. Time taken to collect the necessary data required to instantiate the model.
  - b. Ease of instantiating the model using the software developed in this research.

Since the first criterion measures the model representation against the actual socio-technical access interactions, it evaluates the validity and completeness of the model. The second criterion deals with the ease of use of the model in relation to its instantiation.

#### Criterion 1: The ability of the model to represent important socio-technical interactions

In order to evaluate the risk assessment model based on how well it represents the important socio-technical interactions of organisations, the following question was asked from the evaluators:

- *In your opinion, how well does the network model represent important socio-technical access interactions in your organisation?*

The responses obtained for this question are illustrated in Figure 7-8

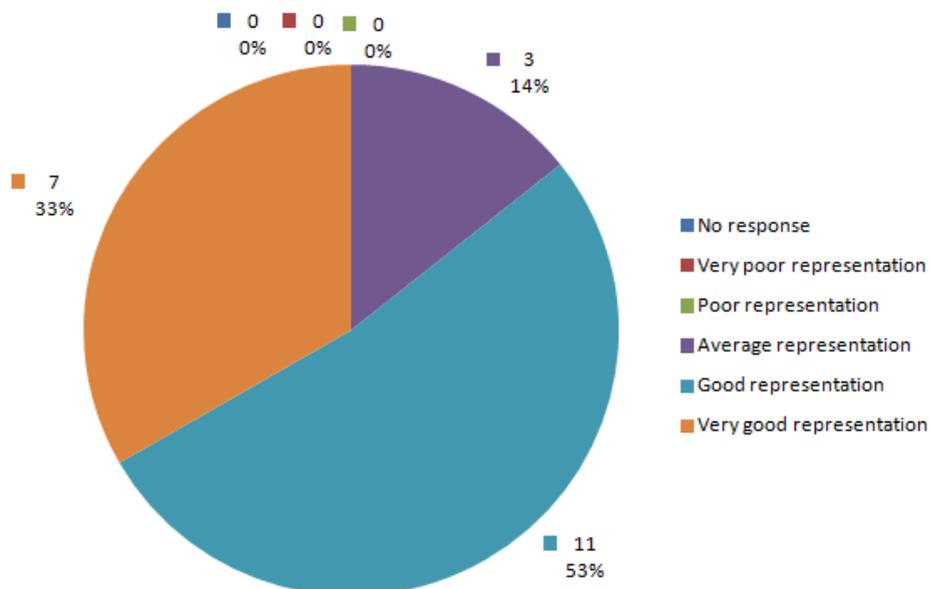


Figure 7-8: Evaluators' opinions on how well the risk assessment model represents important socio-technical interactions in organisations. Data labels show both the number of evaluators (number on top) and the percentage

According to the responses, 18 out of the 21 evaluators (86%) agree that the risk assessment model provide either a good or a very good representation of the important socio-technical access interactions. Only three evaluators believe that the representation is average while no one feels that the representation is poor.

### Criterion 2(a): Time taken to collect the necessary data required to instantiate the model

Instantiating the risk assessment model consists of two activities – first, collecting necessary data and then using that data to populate the model with the aid of software tools. Both these activities affect the ease of use of the model. In relation to the first activity, the following question was asked to gauge the evaluators' opinions on the time taken to collect the necessary data. Note that evaluators didn't actually collect the data. In fact they used anonymised data provided by the researcher. Therefore, the answers reflect estimates provided by the evaluators.

- *How long did it take/will it take for you to collect the data required to populate the model using the resources available to you in your organisation?*

The responses obtained for this question are illustrated in Figure 7-9.

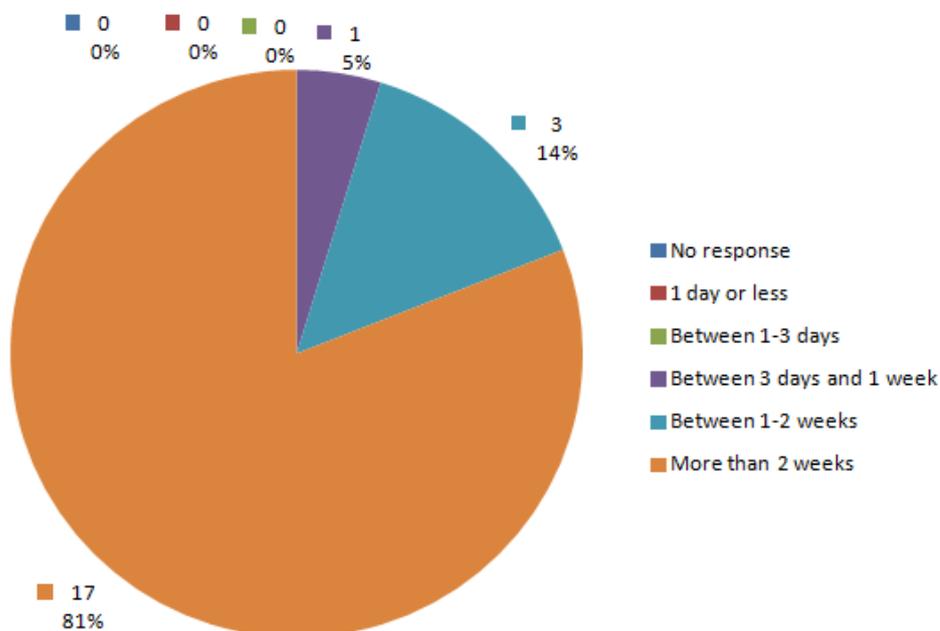


Figure 7-9: Evaluators' responses for the time taken to collect necessary data required to instantiate the model. Data labels show both the number of evaluators (number on top) and the percentage

Most evaluators (81%) feel that it will take more than two weeks to collect the necessary data. This is not surprising since 12 evaluators (57%) are from organisations with more than 300 employees while further 5 (24%) are from organisations with an employee count

between 100 to 300. It takes a considerable amount of time to collect data from larger organisations. Even if most types of data can be obtained by reviewing documents, collecting social interaction data can be time consuming in the absence of automated techniques.

### **Criterion 2(b): Ease of instantiating the model using the software developed in this research**

This criterion evaluates the ease of instantiating the model using the available software. The following question was used to gauge the evaluators' opinions on the ease of instantiating the model:

- *How difficult was it for you to instantiate the model using the collected data and software tools utilised during the workshop?*

The responses obtained for the above question are illustrated in Figure 7-10.

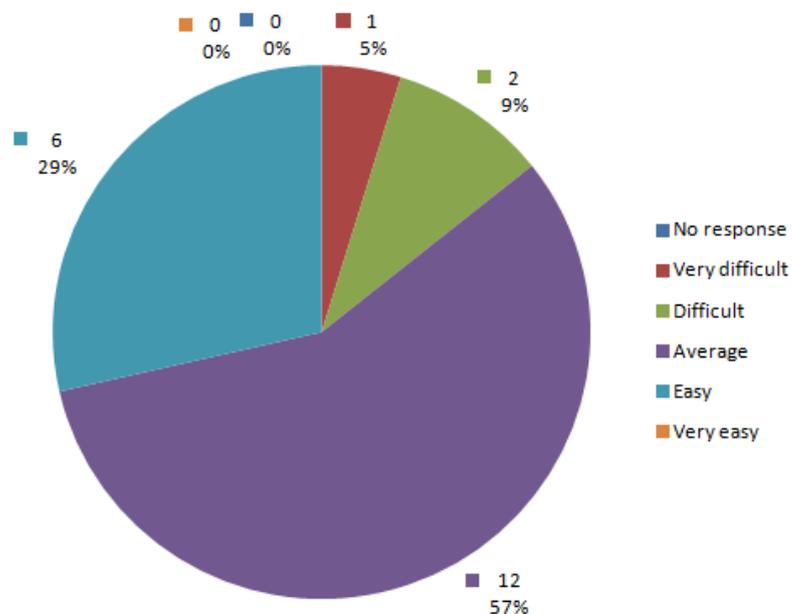


Figure 7-10: Evaluators' opinions on the ease of model instantiation using the available software tools. Data labels show both the number of evaluators (number on top) and the percentage

The majority of the evaluators have responded with difficulty levels equal to or higher than the "average" rating. Only 29% of the evaluators find it easy to instantiate the model using the software provided to them by the researcher. The difficulties experienced by the evaluators could have occurred due to couple of reasons. First, evaluators had very little background or experience in using network analysis tools and all of them tried the methodology for the first time. Second, the model instantiation and metric calculation

software, written by the researcher using the NetworkX Package (Hagberg et al. 2008) available for the Python Programming Language (Rossum 2013), did not contain any graphical user interface. Model instantiation required converting data in to comma separated value files to match the templates provided and then running the required Python Scripts.

#### 7.1.4 Evaluation of the risk assessment method

A single criterion – ease of execution using the software tools provided - was used to evaluate the risk assessment method. In other words, this criterion measures the ease of use of the risk assessment method. Accordingly, the evaluators responded to the following question:

- *Did you find the risk assessment method presented in this workshop easy to follow/carry out using the software tools provided?*

The evaluators' responses to the above question are illustrated in Figure 7-11.

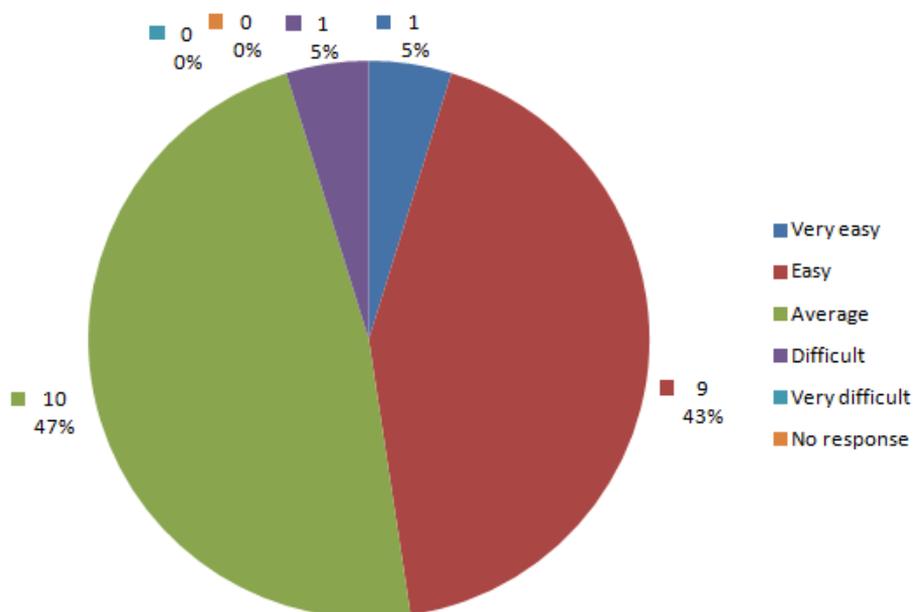


Figure 7-11: Evaluators' opinions on the ease of executing the risk assessment method using the software tools provided. Data labels show both the number of evaluators (number on top) and the percentage

Somewhat mixed responses were given to this question by the evaluators. 48% of the respondents feel it is "easy" or "very easy" to carry out the risk assessment method using the tools provided to them while only one respondent (5%) believed that it is "difficult" to

follow the method. 47% of the evaluators found the difficulty of following the method using the available software tools as “average”.

### 7.1.5 Evaluation of the risk assessment metrics

The risk assessment metrics have been evaluated using two criteria:

1. Applicability of the metric scores in quantifying access risks in organisational contexts (validity of the metrics).
2. Accuracy of the metrics in ranking access risks.

Similar criteria have been prescribed for security metric evaluation by Herrmann (2007, p. 28).

#### Criterion 1: Applicability of the metric scores in quantifying access risks in organisational contexts (validity of the metrics)

The following question was used to gauge the evaluators’ opinions on the applicability of the metrics scores for the purpose of quantifying access risks in organisational contexts:

- *In your opinion, do the metrics used in the analysis produce meaningful results that are applicable in your organisational context for quantifying access risks?*

The evaluators’ responses to the above question are illustrated in Figure 7-12.

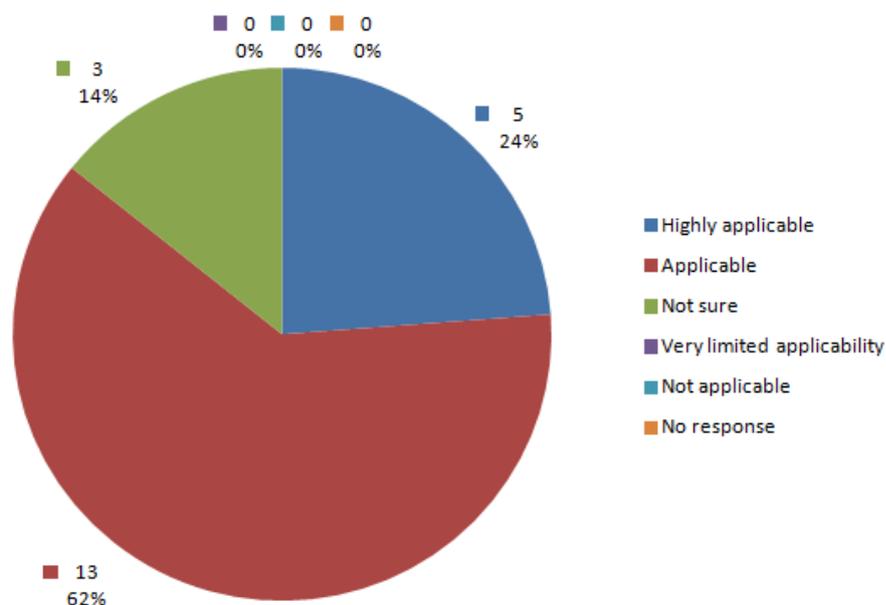


Figure 7-12: Evaluators’ opinions on the applicability of the metric scores in quantifying access risks in organisational contexts (validity of the metrics). Data labels show both the number of evaluators (number on top) and the percentage (number on bottom).

Most of the evaluators (86%) agree that the metrics are either “applicable” or “highly applicable” for the purpose of quantifying access risks in organisational contexts. Only three evaluators (14%) are unsure of the validity of the metrics.

### Criterion 2: Accuracy of the metrics in ranking access risks

The following question was asked from the evaluators in order to gauge the accuracy of the metrics in ranking the information systems access risks:

- *In your opinion, how accurately do the metrics rank socio-technical access risks in your organisation?*

The evaluators’ responses to the above question are illustrated in Figure 7-13.

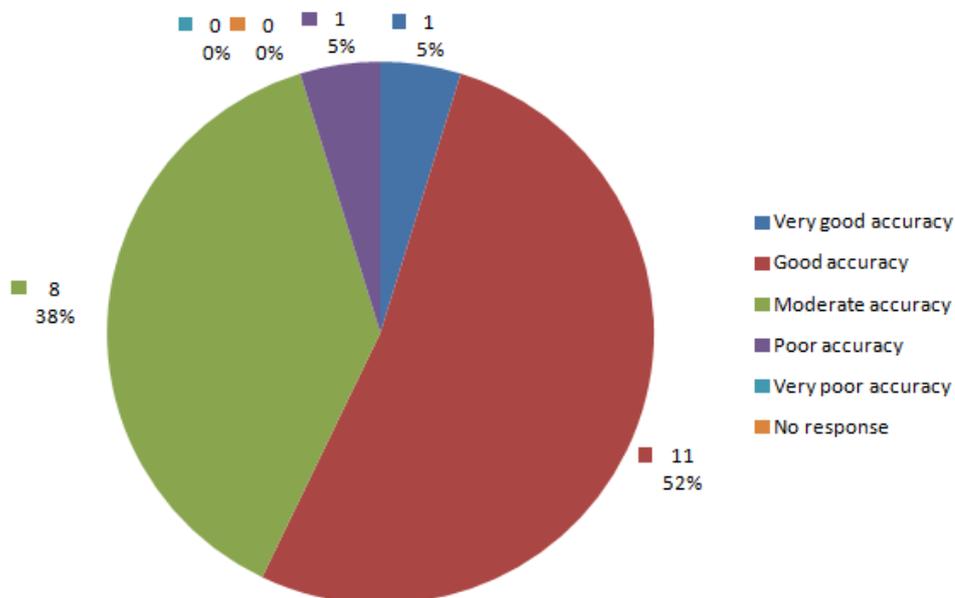


Figure 7-13: Evaluators’ opinions on the accuracy of the metrics in ranking the information systems access risks. Data labels show both the number of evaluators (number on top) and the percentage

Majority of the evaluators’ (57%) believe that the metrics have either “good” or very good” accuracy in ranking information systems access risks while 38% think that the accuracy is moderate. Only one respondent (5%) rated the accuracy of the metrics as poor.

#### 7.1.6 Discussion of the evaluators’ Opinions

Evaluators’ responses to the three evaluation criteria related to the results produced by the risk assessment methodology are very positive. However, they seem to be more convinced about the validity and applicability than the usability of the results in

communicating risks to the decision makers. This becomes clear since the first two evaluation criteria related to the results produced by the methodology receive 81% and 86% positive responses respectively while the third criterion only receives a positive response rate of 71%. The results produced by applying the methodology were visualised using network diagrams and heat-maps to convey the risks effectively to the decision makers. Existing analysis tools were used for this purpose. However, since most of the evaluators used such tools for the first time, generating compelling visualisations was not straightforward. This could be the reason behind the slight reduction of the positive response rate in the case of the third evaluation criteria related to the results produced by the risk assessment methodology. Nevertheless, considering that most evaluators did not have any background on network science, their appreciation of the utility of the methodology is very encouraging.

Evaluators' response to the first criterion related to the validity and the completeness of the risk assessment model is very positive as illustrated in Figure 7-8. In terms of improvements to the model, there is only one suggestion which is given in the following comment by an evaluator: *"Look at psychological aspects of individuals as another vector."*

However, with regards to the ease of using the model, evaluators indicate that collecting necessary data is a time consuming exercise. Moreover, they indicate that instantiating the risk assessment model using the available software is not an easy task. Somewhat mixed responses are also obtained with regards to the ease of use of the risk assessment method where only 47% of the respondents believe that it is easy to follow it using the software tools provided. Some of the comments given by the evaluators in terms of the ease of use of the risk assessment model and method are given below:

*"Development of a GUI that will intake organisational data will help. This GUI can feed data to a DB and process real-time graphs for analysis. The GUI data collection can be in the form of questionnaires, tables and file uploads."*

*"It is better if the complexity of the whole data analysis and representation could be less so that it will be more user-friendly. In my opinion, a larger organisation with thousands of employees it will be much harder if we try to feed data manually. Therefore, it might be better to phase it out department-wise."*

*"Look in to how sensor networks/topologies can be integrated in to this."* (Note: It seems that the evaluator is referring to using sensor networks to collect data)

*“Should build automated tools for the analysis to provide more meaningful presentations and reporting”*

*“It will be good to develop a customised analysis tool which combines the generic toolset used in the workshop.”*

*“According to my knowledge it will be difficult to give weighted values human behaviour based on personal history and other characteristics since they change rapidly. Therefore, composite agent risks have to be changed from time to time. Therefore, it will be very helpful if customised tools are available for this purpose. It is really interesting to know about this research area.”*

*“Visual representations can be carefully described with reports, detailing the analytical scenario and explaining what it is about or what an organisation needs to do about it. Reports can be auto-generated with a software tool developed.”*

The evaluators' responses raise the need for two enhancements. First, the efficiency of the data collection process must be improved, possibly by the development of automated collection techniques. Second, more user friendly software tools must be developed to aid the analysis. The risk assessment method used in this research used an entire chain of tools starting from the Python scripts written by the researcher (used to instantiate the model and to calculate the metrics) to statistical and network analysis tools (used to generate visualisations). The analysis task would be much easier if there is a single software tool that provides the full functionality from data integration to visualisation. However, these enhancements are clearly beyond the scope of this research due to time and resource constraints.

In terms of the applicability of the metrics, evaluators have provided very positive feedback. Although mostly positive feedback is given with regards to accuracy of the metrics in quantifying the risks, several evaluators (38%) believe that the accuracy is only moderate. There are two ways to improve the accuracy of the metric results – by increasing the accuracy of the data used in the metric calculations and by enhancing the metrics by providing a more accurate representation of the socio-technical variables. Since almost all evaluators agreed on the completeness and validity of the risk assessment model, which provides the foundation for the metrics, it can be assumed that the accuracy of the data is the main aspect that should be improved to obtain more accurate results.

## 7.2 Evaluation Using the Three Case Studies

### 7.2.1 Evaluation of the results produced by applying the methodology

As discussed in Section 7.1, information security professionals who participated in the evaluation workshop endorsed the validity and applicability of the results produced by the methodology. Researcher's observations in the analysis of the three case-studies are also in agreement with the above conclusion. Almost all metric calculations produce a small number of very high risk values among many other moderate to low risk scores. This enables organisations to effectively identify entities and relationships that cause high risks. For example, Figure 7-14 shows the distribution of three different metric scores in Organisation-2. In the case of all three metrics, most of the resource access authorisations have either zero or low risk scores while a few high metric values indicate the access authorisations that need the organisation's attention.

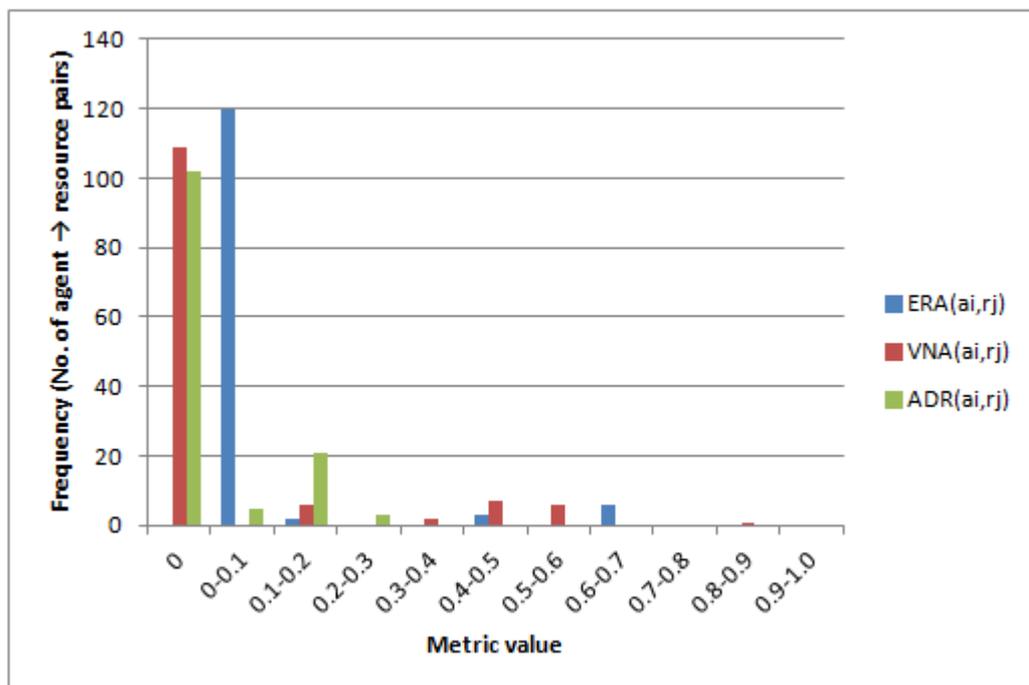


Figure 7-14: Distribution of ERA( $a_i, r_j$ ), VNA( $a_i, r_j$ ) and ADR( $a_i, r_j$ ) scores in Organisation-2

The results produced by the methodology also provide multiple perspectives; using metrics that calculate risks per agent, information resource, task, resource access authorisation and task assignment. Such multiple perspectives give flexibility to the analyst to look at risks and mitigation strategies in different ways. Results produced by the risk

assessment methodology can be used in several ways to guide insider threat mitigation decisions in organisations. Some usage possibilities are:

1. The methodology can be used as a periodic risk assessment of information systems access in organisations to identify the most serious risks and take measures to mitigate them (The three case studies and the evaluation workshop were carried out with a similar objective).
2. Methodology can be used to compare risks across departments, employees and information resources to decide which departments or information resources require more security controls and which employees should be targeted for increased monitoring or information security awareness training.
3. During times of organisational change (e.g., introduction of new information systems or phasing out old systems, acquisitions or mergers, downsizing and changing access permissions of users), the methodology can be used to determine how the changes would impact the information systems security risks, with a particular focus on insider threats.
4. During an information security incident, to help contain the incident and in the subsequent investigation (e.g., during a data breach related to a particular information resource  $IAC(a_i, r_j)$  can be used to estimate which agents are more likely to obtain indirect access to that resource).

This research uses several types of visualisations such as charts, heat-maps and network diagrams for the presentation of risks in a user-friendly manner. These visualisations provide the ability to drill down and find possible causes of high risk scores as illustrated in Chapter 6. Therefore, the researcher is in the opinion that the visualisations play a central role in communicating risks effectively to the decision makers.

### **7.2.2 Evaluation of the risk assessment model**

The evaluators who participated in the workshop endorsed the validity and the completeness of the risk assessment model presented in Section 5.2. The applicability and the validity of the results obtained from the three case-studies also support the above conclusion. In terms of instantiating the model, one of the most difficult aspects was to decide on the granularity of some entities. For example, an information resource can be an

information system, a database of the system, a single table in the database or even a single record. If the entities are too granular, it will be very difficult to collect data and instantiate the model. On the other hand, if the entities are modelled at a very high-level, some risks won't be detected.

In comparison to the validity and the completeness of the model, the evaluators were less convinced about the ease of instantiating it with regards to the time taken to collect the necessary data. Researchers experience in the data collection phase of the case studies also agrees with the views expressed by the evaluators. In the absence of automated data collection techniques, it takes a significant effort and time to collect various types of data required for the analysis. Not all types of data can be extracted from systems or found in documents and this is especially true for the social interaction data. Another problem with collecting social interaction data is the reliability of the relationships nominated by people. Only strong relationships were considered in the three case studies to overcome this problem.

### **7.2.3 Evaluation of the risk assessment method**

The risk assessment method illustrated in Figure 7-15 was carried out in the three case studies with the help of software tools. Instantiation of the model and metric calculation utilised software developed in this research while other network and statistical analysis software were used to generate the visualisations. This process required manually entering some of the data collected and feeding the outputs produced by one software tool to another. As suggested by some of the evaluators, this process can be made more efficient and user friendly if an integrated software tool can be developed to cover the complete risk assessment process in an automated manner.

Another aspect important for the usability of the risk assessment method is its compatibility with the existing technology focused risk assessment standards and frameworks. Since organisations conduct routine risk assessments according to these standards and frameworks, the access risk assessment method developed in this research can be easily integrated with them if it is compatible. Therefore, the socio-technical access risk assessment method is compared for compatibility with three widely used risk assessment standards - ISO/IEC 27005:2011 - *Information technology - Security techniques - Information security risk management standard* (International Organisation for Standardisation 2011); NIST SP 800-30 Revision 1– *Guide for Conducting Risk Assessments* (National Institute of Standards and Technology 2012) and OCTAVE - *Operationally Critical*

*Threat, Asset, and Vulnerability Evaluation* (Alberts et al. 2003) in Section 7.3. The comparison demonstrates the usability of the risk assessment methodology developed in this research with the above three standards/frameworks.

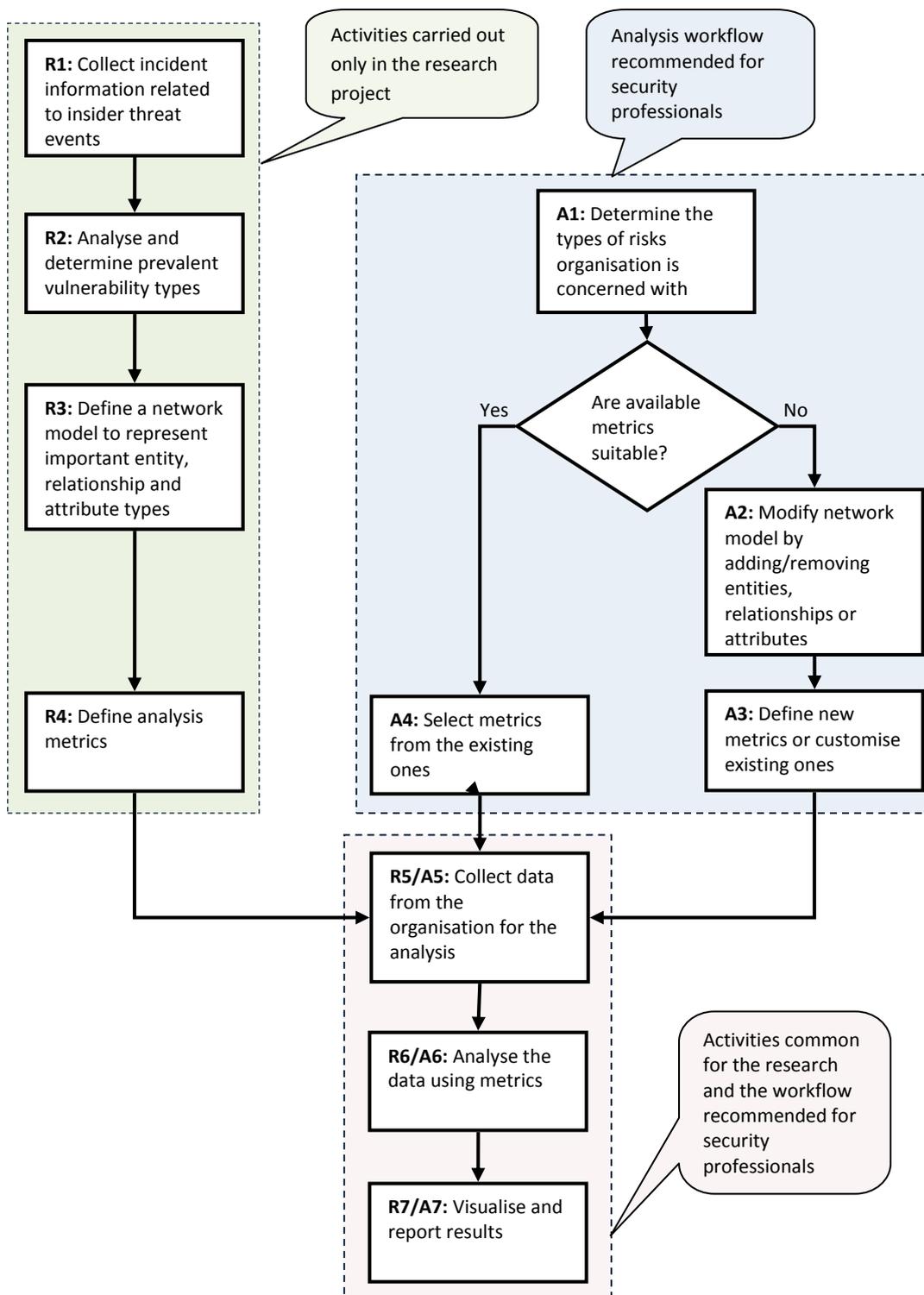


Figure 7-15: The risk assessment activities followed in the research and the assessment method recommended for information security professionals (re-illustration taken from Chapter 5)

#### **7.2.4 Evaluation of the risk assessment metrics**

In terms of the validity, the results produced by the application of the metrics, presented in Chapter 6, demonstrate that the metrics produce meaningful results. The metric scores can be used to produce visualisations that enhance the capability of interpreting the risk values as well as examining the underlying causes of the risks. The validity and the applicability of the results produced by the methodology, discussed under section 7.2.1, also confirm the validity of the metrics used for the risk assessment.

The accuracy of the metric results largely depends on the reliability and granularity of the inputs used to calculate them. If inaccurate information is used for the calculations, metric results will not rank the risks in the correct order of severity. During the case studies, the main reliability concerns occurred in relation to social interaction data. Reliable sources such as documents were available to verify most other types of data while social interaction data completely relied on responses provided by employees of the organisations. Therefore, in order to improve the reliability, only strong, mutually acknowledged social interaction relationships were included in the analysis. A notable exception to this is the formal reporting relationships, which were mapped using organisational charts.

Organisations using the metrics presented in this research or developing new metrics based on the same methodology can use similar criteria for evaluation. Accuracy of the metrics can be determined based on the ability of metrics to rank the risks in correct order of severity according to expert opinion. Applicability and validity of the metrics can be determined by evaluating whether the metrics produce meaningful results that improve the risk awareness of the organisation.

### **7.3 Compatibility with Existing Risk Assessment Standards and Frameworks**

Typically, an organisation would not perform a socio-technical access risk assessment in isolation to analyse and mitigate insider threats. In fact, the risk assessment methodology developed in this research would be a component of a larger enterprise-wide security risk assessment carried out according to accepted industry standards and frameworks. Therefore, this section compares the socio-technical access risk assessment methodology for compatibility with three widely used risk assessment standards - ISO/IEC 27005:2011 - *Information technology - Security techniques - Information security risk management standard* (International Organisation for Standardisation 2011); NIST SP 800-30 Revision 1–

*Guide for Conducting Risk Assessments* (National Institute of Standards and Technology 2012) and OCTAVE - *Operationally Critical Threat, Asset, and Vulnerability Evaluation* (Alberts et al. 2003).

### Compatibility with ISO/IEC 27005:2011

ISO/IEC 27005:2011 is the information technology risk management standard developed by the International Organisation for Standardisation (2011). The core processes included in the standard are illustrated in Figure 7-16.

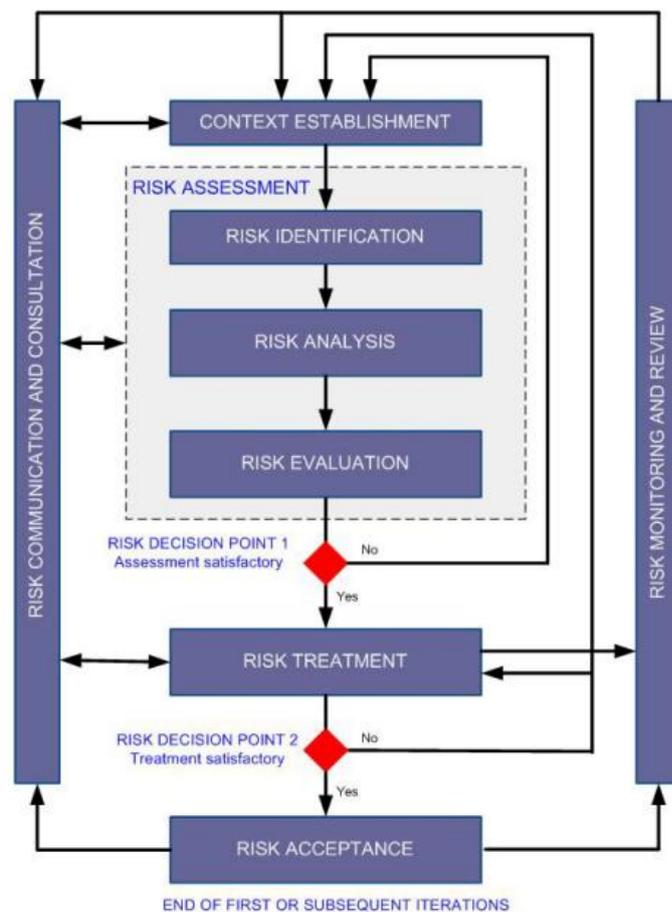


Figure 7-16: Activities involved in the ISO/IEC 27005:2011 Standard (International Organisation of Standardisation 2011)

In Figure 7-16, the core risk assessment activities are grouped within the box with the dotted line. Other activities are either pre-requisites or actions resulting from the risk assessment exercise. The *context establishment* phase of ISO/IEC 27005:2011 establishes the scope of risk assessment and defines the terms and criteria used such as classification of information resources. Therefore, Information security professionals can include the socio-technical access risk assessment methodology as part of the scope of overall risk assessment during this phase.

The second step in ISO/IEC 27005:2011 is called the *risk identification*. This step deals with the identification of information resources, security threats to these resources, potential vulnerabilities and existing controls. The activity *A1* of the socio-technical access risk assessment method given in Figure 7-15 can be carried out under this step. The next step in ISO/IEC 27005:2011, termed *risk analysis*, deals with the analysis of risks and estimation of the level of risk either qualitatively or quantitatively. Activities from *A2* or *A4* (note the two possible process pathways) to *R6/A6* in the socio-technical access risk assessment method, which forms the core activities of the process, correspond to this step. The next step in ISO/IEC 27005:2011, called *risk evaluation*, is concerned with making risk mitigation decisions based on the risk values obtained from the previous risk analysis phase. Activity *R7/A7* in the socio-technical security risk assessment method closely aligns with this step since the activity involves interpreting the risk scores using visualisations and reporting them to the decision makers. The final step of ISO/IEC 27005:2011, called *risk treatment*, is outside the scope of the socio-technical access risk assessment method since it involves taking appropriate action based on the results of the previous steps. Additionally, as shown in Figure 7-16, communication and consultation with all stakeholders and continuous monitoring and review of the risk assessment process occurs throughout the ISO/IEC 27005:2011.

### **Compatibility with NIST SP 800-30: Revision 1**

NIST SP 800-30: Revision 1, illustrated in Figure 7-17, describes the risk assessment process prescribed by the National Institute of Standards and Technology (NIST), USA (2012).

The first step of NIST SP 800-30 establishes the scope and the constraints of the risk assessment. This phase, similar to the *context establishment* in ISO/IEC 27005:2011 (International Organisation for Standardisation 2011), also defines constructs and methods used for the risk assessment. Therefore, during this step, information security professionals should explicitly include the socio-technical access risk assessment methodology as a component of the overall risk assessment process of the organisation.

The second step, termed *conduct assessment*, consists of several tasks as illustrated in Figure 7-17. The first two tasks – *identify threat sources and events* and *identify vulnerabilities and predisposing conditions* are equivalent to the Activity *A1* in the socio-technical risk assessment method presented in Figure 7-15.

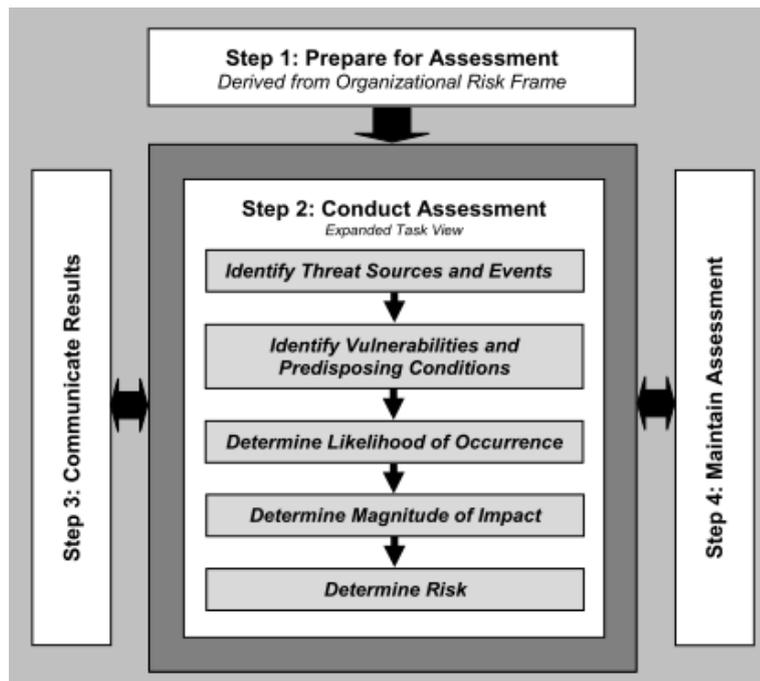


Figure 7-17: The risk assessment process described in NIST SP 800-300: Revision 1 (National Institute of Standards and Technology 2012)

The threat source identification is straightforward in the case of socio-technical access risk assessment since all threats occur due to malicious insiders. Identifying and analysing vulnerabilities that could be exploited by the threat sources lead to the selection of model entities and relationships as well as defining the metrics. Next three tasks of NIST SP 800-30 – *determine the likelihood of occurrence, determine impact and determine risks* are the core tasks dealing with the risk calculations. These three tasks are integrated to the metrics defined in this research and activities from A2 or A4 (depending on the chosen pathway) to R6/A6 correspond to the estimation of *impact, likelihood* and *risks*. The integration of likelihood and impact factors in the metrics defined in this research can be demonstrated using an example. If the  $IAC(a_i, r_j)$  metric, defined in equation (1.39) - page 145, is scrutinised, there are three likelihood factors which affect the metric score – length and number of shortest paths from the agent –  $a_i$  to the information resource –  $r_j$  as well as the composite risk attribute values –  $C_a(a_i)$  of the agents along the path. It is assumed that shorter paths through the social network increase the likelihood of the agents obtaining indirect access to the information. At the same time, if the agents along the path have shown concerning behaviour (based on historical observations) they are more likely to collaborate in such indirect access attempts that violate the security policies of the organisation. The impact factor is included in the metric in the form of standardised

resource criticality/sensitivity –  $C_r(r_j)$ . If the resource is more critical or sensitive, then the damage will be higher due to unauthorised access via the social networks.

The third step of NIST SP 800-30, termed *communicate results*, is a task spread throughout the risk assessment process. This step closely aligns with activity R7/A7 of the risk assessment method depicted in Figure 7-15.

### Compatibility with OCTAVE methodology

The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) is a risk management methodology developed by the Software Engineering Institute of the Carnegie Mellon University, USA (Alberts et al. 2003). The methodology consists of three main phases as illustrated in Figure 7-18.

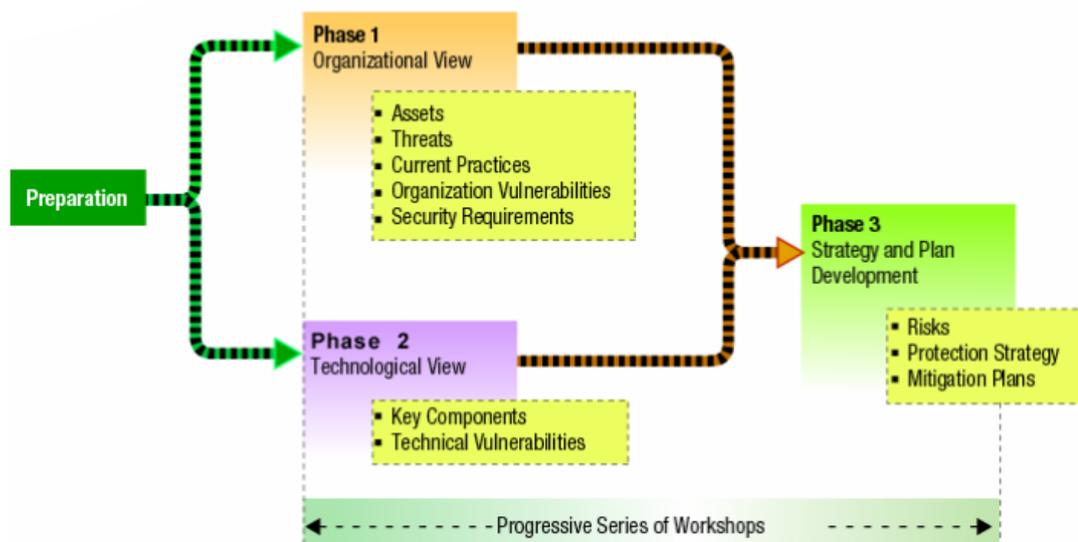


Figure 7-18: The three main phases of the OCTAVE risk management methodology (Alberts et al. 2003)

The first phase, called *build asset-based threat profiles* (labelled organisational view in Figure 7-18), creates profiles of threats, vulnerabilities and information assets using data collected from managers and other staff members. The second phase, termed *identify infrastructure vulnerabilities*, deals with the identification of key IT infrastructure assets and the analysis of their vulnerabilities in a technological standpoint. The first and second phases of OCTAVE are equivalent to the Activity A1 of the risk assessment method developed in this research, illustrated in Figure 7-15. Under the third phase – *develop security strategy and plans*, the risk analysis and the development of strategies to mitigate the risks are performed. Activities from A2 or A4 (depending on the pathway selected by

the analysts) to R7/A7 in the socio-technical risk assessment method developed in this research (refer Figure 7-15) can be carried out under this phase.

One unique feature of the OCTAVE methodology is other risk assessment methods can be used with it as long as they satisfy a set of requirements called the “OCTAVE criteria” (Albert and Dorofee 2001). The first criterion – *self direction*, means that the organisations’ employees themselves take the responsibility of risk management and the risk mitigation decisions. While the employees, especially the ones entrusted with information security risk management, can play a leading role in the socio-technical risk assessment, it does pose some problems due to privacy issues. On the other hand, if external consultants carry out the analysis and report findings confidentially to the decision makers, some privacy concerns can be addressed. Therefore, organisations need to decide whether they can minimise privacy issues if the risk assessment is carried out completely by internal teams.

The second criterion – *adaptable measures*, demand that the risk assessment metrics to be adaptable according to constantly changing threats and vulnerabilities. As shown in Figure 7-15, the socio-technical access risk assessment method developed in this research provides flexibility for the analysts to modify the risk assessment metrics and the model (refer activities A2 and A3 in the figure) according to the changing threats, vulnerabilities and organisational concerns.

The third criterion – *Defined process*, requires the risk assessment method to have a well defined set of activities, a clear set of tools and documentation for the analysts to follow and standard formats to report results. While some of these are well defined, such as the risk assessment method, model and metrics, development of supporting documentation and standard formats for reporting results are beyond the scope of this research. However, future research can be aimed toward developing the missing components.

The fourth criterion – *foundation for a continuous process*, specify that the risk assessment method should allow for continuous improvement of the information security posture by carrying out the processes in an iterative manner. Although the socio-technical access risk assessment method does not explicitly specify an iterative process, it can be repeated in a cyclic manner as a part of a larger information security risk management program of an organisation.

According to the fifth criterion – *forward looking view*, the risk assessment method has to look beyond the current vulnerabilities and focus on a range of risks that could even

occur in the future. Some of the metrics in the socio-technical access risk assessment methodology, especially the ones that involve the social networks, focus on such risks that could occur in the future.

The sixth criterion – *focus on the critical few*, specifies that the risk assessment should be able to focus on the most critical risks thereby efficiently using the limited resources available to safeguard against security threats. The metrics used with the socio-technical access risk assessment method helps in the identification of the most critical risks. As discussed in Section 7.2.1, metrics highlighted few cases of high risks among many other instances of moderate to low risks in the three case-studies.

The seventh OCTAVE criterion – termed *integrated management*, requires close alignment of information systems security policies and goals with the business requirements and strategies. This criterion should be part of the wider information security management system of the organisation and it is clearly beyond the scope of the risk assessment methodology developed in the research project.

According to the eighth criterion, called *open communication*, an OCTAVE compatible risk assessment method should allow the open communication of security issues and concerns as well as the results of risk assessment among staff members. The socio-technical access risk assessment methodology collects information from all staff members regarding concerns they have, their observations and their socio-technical interactions important for security. However, such openness cannot be maintained always in communicating results of the assessment since some of the information will be sensitive and private in nature.

The ninth criterion – *global perspective* calls for a more holistic perspective of information security risks aligned with the business goals. The risk assessment methodology developed in this research takes a more holistic view of the security related interactions in an organisation by taking socio-technical factors in to account.

According to the tenth and final criterion – *teamwork*, the risk management tasks should be carried out by interdisciplinary teams offering multiple perspectives. The analysts using the risk assessment methodology developed in this research can be part of the wider risk management team offering their unique perspectives on insider risks to the organisation.

The comparison of the socio-technical access risk assessment methodology with the two standards - ISO/IEC 27005:2011 and NIST SP 800-30 demonstrate that the methodology

presented in this research can be carried out within the framework provided by these two standards. However, if the analysts wish to use the socio-technical access risk assessment methodology within the OCTAVE framework, they have to adopt additional processes, tools and documentation templates in order to make the risk assessment fully compatible with OCTAVE.

## 7.4 Research Summary and Conclusions

The primary objective of this research, as described under the Research Methodology (Chapter 3), was to develop a methodology that can be used to assess risks occurring due to organisational information systems access. Accordingly, the high level research question was stated as: *What models, methods and metrics are appropriate for the assessment of security risks occurring due to organisational information systems access?*

The following research sub-questions were used to help answer the main research question:

1. *Which entity and relationship types must be included in a security risk assessment model of information systems access?*
2. *What factors should be integrated into metrics that can be used to quantify risks related to information systems access?*
3. *What activities (steps) must be carried out to assess security risks related to information systems access?*

In response to the main research question, this research developed a risk assessment methodology that factors in socio-technical interactions and the inherent risk characteristics of the entities involved in these interactions. The methodology developed encapsulates a risk assessment model that represents socio-technical interactions between entities as well as their intrinsic risk attributes, a risk assessment method that specify the process to be followed by the analysts and metrics that can be used to quantify the security risks.

In response to the first research sub-question, a meta-matrix representation that specifies the entity and relationship types that must be included in the risk assessment was developed. This meta-matrix is illustrated in Table 5-3 (page 98) while the equivalent meta-network representation is illustrated in Figure 5-3 (page 63). In response to the second

research sub-question, metrics described in Chapter 5 were developed in this research. The third research question has been answered by the development of the risk assessment method illustrated in Figure 7-15.

The risk assessment methodology was evaluated to determine how well they answer the research questions stated above. Two main types of evaluations were carried out – by engaging information security professionals in a risk assessment workshop and by conducting three case studies of financial sector organisations. The results of these two forms of evaluations are discussed in sections 7.1 and 7.2 respectively. The results of the evaluation support the conclusion that the risk assessment model, method and metrics answer the research questions satisfactorily.

Furthermore, since the research adopted a design science paradigm, the initial utility theory was stated in Chapter 3 as: *A socio-technical risk assessment methodology would help organisations to effectively assess information systems access risks that contribute to insider security breaches.* The results of the evaluation also justify this utility theory.

## **7.5 Limitations of the Research**

This research had to be carried out within certain constraints. First, the data used to determine common types of socio-technical access risks and their underlying causes are U.S. centric. At the moment, such insider threat data repositories on a global scale are not publicly available. Despite this constraint, it can be assumed that similar types of access risks would occur in organisations in other countries as well. The three case studies used to evaluate the research outcomes (risk assessment model, method and metrics) were based on financial sector organisations in Sri Lanka. The reasons for this choice are explained in Section 4.2 under Chapter 4. The validity of the research outcomes will certainly improve if the methodology can be applied in various industry sectors around the globe, although such endeavours are clearly beyond the scope of this research project.

The evaluation of the research outcomes using only three financial sector organisations in Sri Lanka also constraints the generalisability of the results. Although the risk assessment methodology may be safely applied in other financial sector organisations in Sri Lanka, it should not be generalised across different organisational sectors or countries. In order to achieve wider generalisability, further evaluation of the risk assessment methodology in various organisational contexts is required.

The practical use of the risk assessment methodology is also complicated due to the lack of an integrated software solution that can handle the risk analysis workflow from feeding in data to the visualisation of the results. This research used software code developed by the researcher to calculate the risk metrics in combination with existing network and statistical visualisation tools. Although information security professionals who evaluated the methodology were able to implement the analysis workflow, using the code provided by the researcher and the other software tools, they clearly prefer an integrated software solution as evident from the feedback provided.

Furthermore, collecting data required for the analysis is a highly time consuming process as indicated by the responses given by the majority of the security professionals who participated in the evaluation workshop. Therefore, this methodology requires considerable time and effort to be used in larger organisations if automated techniques for data collection are not used.

Another limitation of the risk assessment methodology can arise due to ethical and privacy concerns. Since the methodology requires the collection of social interaction data and behavioural attributes of individuals, organisations need to adhere to strict ethical guidelines and applicable privacy laws. In this research project, the case-studies of the three organisations were carried out after obtaining research ethics approval from the Curtin University. Researcher obtained informed consent from both organisations and participants for the research. Participants were also given the option of withdrawing from the study at any time without penalty and all references to participants were anonymised in publications. Participants not consenting to data sharing and anonymising results can limit the utility of the methodology in some organisations. In such cases, organisations must develop innovative ways to encourage participation of employees while adhering to ethical guidelines and preserving privacy at the same time.

The other limitation related to the data collection aspect is the reliability of self-reported social interaction data. In the case of malicious individuals, wrong information might be provided to mislead the risk assessment exercise. On the other hand, non-malicious individuals may report false information due to the fear of any negative consequences of their disclosures. This research used thresholds based on the link strength and mutual acknowledgement to improve the reliability of self-reported social interactions as described in Section 6.5. The next section discusses how the limitations described above can be addressed through future research.

## 7.6 Future Research

Many opportunities for further research stem from this project. First of all, insider threat data collected from around the world and multiple organisation sectors should be used to enhance the metrics defined in this research and to develop new metrics that address additional types of socio-technical information systems access risks. A major obstacle for achieving this goal is the lack of information sharing on information security incidents. Organisations are reluctant to report information security incident details due to various factors such as the potential for loss of reputation and privacy concerns. Future research could extract data from sources such as published court cases and insider threat incidents reported in the media to further enhance the methodology. Another obstacle for analysing insider threat events is the lack of standardised formats for organisations to report insider threat incidents and investigation outcomes. A recently initiated project, called Vocabulary for Event Recording and Incident Sharing (VERIS – refer <http://www.veriscommunity.net>), is an attempt to solve this problem and promote sharing of incident information using standard, anonymised formats. Developing similar incident reporting formats, customised for sharing insider threat data, would be useful to further enhance the risk assessment methodology presented in this research.

Moreover, evaluating the methodology presented in this research in various other organisational contexts would improve its validity and generalisability. Ideally, the methodology should be evaluated in organisations belonging to different industry sectors and countries. It would also help information security analysts if clear guidelines and standard documentation templates are available to be used with the methodology. The development of such standards and templates would require a consensus among information systems security experts, which in turn depends on evaluating the methodology in many industry sectors.

One of the major difficulties experienced by the researcher was the significant amount of effort and time required to collect the data needed for the risk assessments. Information security professionals also pointed out the same problem during the workshop evaluations. Research in to automated data collection techniques would help solve this problem. Research efforts could be directed at developing software agents that extract data required for the assessment from sources such as access control systems, ERP systems, compliance management systems and human resource information systems. For example, a software agent connected to identity and access management systems can extract data on *who has*

*access to what information resources*. The software agents can then automatically feed the data to the risk assessment software.

The other challenge is to automate the collection of face-to-face human interaction data such as employees obtaining advice from others. It takes time to collect such data manually and the reliability of self-reported interaction data can be low at times. Recent advancements in sensor network research have resulted in the creation of wearable sociometric badges as a possible solution for this problem (Olguin and Pentland 2008; Olguin et al. 2009; Waber et al. 2011; Kim et al. 2008). These badges, typically worn in a lanyard, similarly to the employee identification badges, can provide a wide range of information on interactions between people (Olguin et al. 2009; Waber et al. 2011). Social interaction data collected using the sociometric badges can be automatically fed in to the socio-technical risk assessment software. However, more research is required to use this emerging technology for security risk assessment since researchers must determine what level of granularity to be used, what forms of data need to be collected, the frequency of data collection and how to address privacy concerns.

The evaluators who participated in the workshop also suggested the development of an integrated software tool for the socio-technical access risk assessment that covers all analysis tasks from collecting data to the visualisation of the results. The proposed structure of such a system is illustrated in Figure 7-19. As shown in the figure, a fully automated system for socio-technical access risk assessment would collect data through software agents placed in information systems as well as sociometric badges worn by employees. At the same time, a behavioural reporting system should be available for staff members to report any concerning behaviours they observe among their colleagues. The behavioural monitoring reports can be used to calculate intrinsic risk characteristics of people described in Section 5.2.2. Based on the inputs provided, the core system would calculate risk metric values, which are then used for report generation and visualisation.

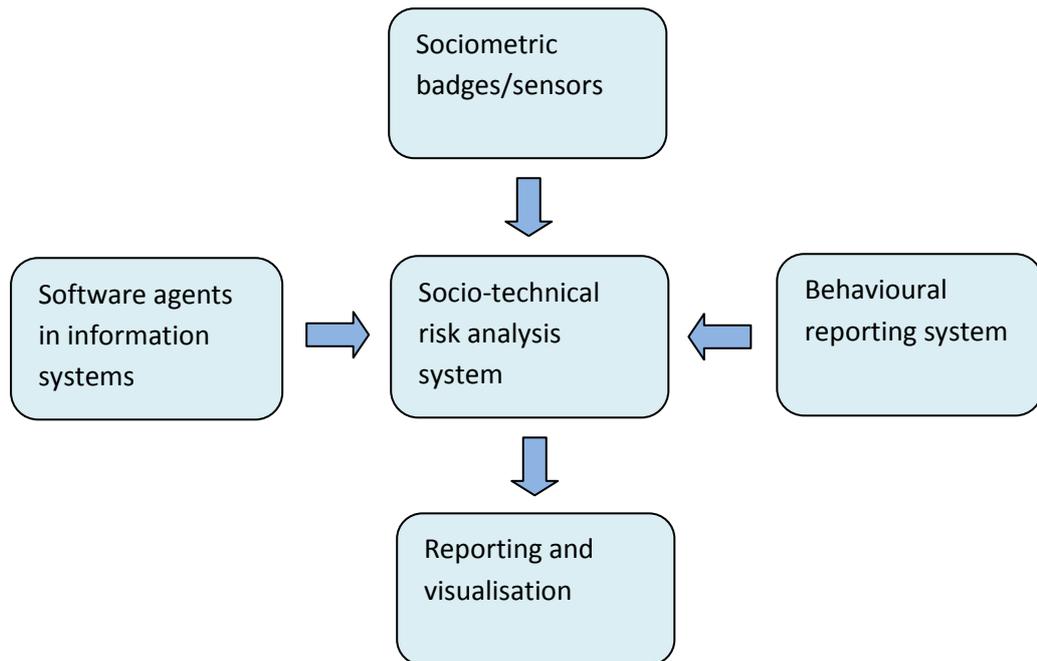


Figure 7-19: Proposed components of a socio-technical risk assessment system that automates all functions from data collection to visualisation

Another aspect that requires further research is the impact of the insider risk assessment methodology on employee privacy and organisational ethics. While organisations need to collect sensitive personal and social-interaction data to mitigate insider risks, it can be detrimental to employee privacy. Therefore, research should focus on ways of balancing organisational requirements with the privacy expectations of employees in collecting data for the risk assessment. Some basic guidelines for organisations and consultants on this subject has been provided by Borgatti and Molina (2005). However, more research is required in areas such as privacy policies, techniques for preserving anonymity and guidelines that enable organisations to decide the scope and granularity of data collection while addressing privacy concerns at the same time.

The socio-technical access risk assessment methodology provides static snap-shots of access risks in organisations. However, the relationships and attributes used in the risk calculations are dynamic in nature. Hence, research aimed at modelling dynamics of the access relationships would be beneficial for the mitigation of insider threats. Furthermore, individuals might modify their behaviour and social interactions in response to the risk assessments carried out even if their intentions are not malicious. Such behavioural changes might result in an organisation moving to a state of either higher or lower risk in terms of information systems security. Therefore, one potential research topic is to explore

the techniques that could be used to drive relationships related to information systems access, modelled as a meta-network, from a state of higher risk to a state of lower risk. Another research area would be to provide organisations with dynamic risk indicators that could serve as early warnings.

**7.7 Research Contributions**

Despite the limitations mentioned in Section 7.5, this research makes a valuable contribution to the theory and practice of the information systems security discipline. This section describes these theoretical and practical contributions.

**7.7.1 Theoretical contributions of the research**

Theoretical contributions made in this research and the relevant sections in the thesis that describe the contributions are summarised in Table 7-1.

Table 7-1: Summary of theoretical contributions of this research

No	Theoretical contribution	Relevant topic, diagram or table in the thesis
1	Classification scheme for access risks based on the socio-technical causes and thirteen types of access vulnerabilities.	Classification scheme is illustrated in Figure 5-2. (Page 96) Access risks under each category are listed in Table 5-4, Table 5-5, Table 5-6 and Table 5-7.
2	Model for the assessment of socio-technical access risks	Section 5.2 describes the analysis model. Meta-matrix representation of the model is given in Table 5-3. (Page 98) Meta-network representation of the model is illustrated in Figure 5-3. (Page105)
3	Method (process) for the assessment of socio-technical access risks	Analysis method is described in Section 5.8. A diagrammatic illustration is given in Figure 5-16.
4	Thirteen metrics suitable for the assessment of socio-technical access risks	Sections 5.3, 5.4, 5.5 and 5.6 describe the metrics. Metrics are also summarised in Table 5-8.

The first contribution refers to the access risk classification (based on their socio-technical causes) developed in this research. Furthermore, the research identified thirteen unique risk types that occur within this classification. The second contribution refers to the risk assessment model described in Section 5.2, which consists of entities, relationships between them and attributes of entities important for the assessment. The third contribution refers to the risk assessment method described in Section 5.8 while the fourth

one refers to the thirteen risk assessment metrics described in Sections 5.3, 5.4, 5.5 and 5.6.

### **7.7.2 Practical contributions of the research**

This research also makes valuable contributions to the information systems security profession. As pointed out by Gartner IT Research (Carpenter and Walls 2011), due to the changes in the threat landscape in recent years, organisations need to focus on security risks originating from people within their trust boundary (in other words, risks due to insiders - people having legitimate access to information systems). The same organisation labelled insider threats as one of the top-five issues for Chief Information Security Officers (Heiser and Scholtz 2009). Recent industry reports (Pricewaterhouse Coopers et al. 2013; Pricewaterhouse Coopers et al. 2014) also highlight the prevalence of insider risks.

Despite the seriousness of the insider threat problem, there is a clear capability gap between organisations' ability to counter insider threats as opposed to their ability to face the threats originating from outside. Today, almost all organisations deploy technical countermeasures such as anti-malware systems, firewalls and intrusion protection systems that protect against external attacks. However, according to the 2014 Global State of Information Security Survey (Pricewaterhouse Coopers et al. 2014) only 31% of the organisations conduct regular review of users and access. A major reason for this is the unavailability of models, methods and metrics that can be used for access risk assessment. This problem has been there for several years and bodies such as the INFOSEC Research Council, U.S.A. have called for more research in this area by including insider threat mitigation in their "hard problems" list (INFOSEC Research Council 2005).

The risk assessment model, method and metrics developed in this research offer a solution to the problems faced by organisations with regards to the mitigation of access risks that can result in insider threat events. Furthermore, the software code developed in this research can be used by information security professionals to calculate socio-technical access risk metrics for their organisations. The research also demonstrates how metric results can be used to create risk visualisations using the existing network and statistical analysis tools. Furthermore, the compatibility of the socio-technical risk assessment methodology with existing standards/frameworks such as - ISO/IEC 27005:2011 (International Organisation for Standardization 2011), NIST SP 800-30 (National Institute of

Standards and Technology 2012) and OCTAVE (Alberts et al. 2003) enable security professionals to embed the methodology in to their regular risk assessment exercises.

## References

- Albert, Cecilia, and Audrey Dorofee. 2001. *OCTAVE Criteria - Version 2.0*. Pittsburgh, PA: Software Engineering Institute of Carnegie Mellon University. <http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=5645>.
- Alberts, Christopher, Audrey Dorofee, James Stevens, and Carol Woody. 2003. *Introduction to OCTAVE Approach*. Pittsburgh, PA: Software Engineering Institute of Carnegie Mellon University. <http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=51546>.
- Alberts, Christopher J., and Audrey J. Dorofee. 2001. *OCTAVE Method Implementation Guide - Version 2.0*. Pittsburgh, PA: Software Engineering Institute of Carnegie Mellon University. <http://www.cert.org/resilience/products-services/octave/octave-s-method.cfm>.
- Allan, Ant. 2013. *Technology Overview for Privileged Account Management*. Stamford, CT: Gartner Research. <https://www.gartner.com/doc/2513015/technology-overview-privileged-account-management>.
- Althebyan, Q., and B. Panda. 2007. "A Knowledge-Base Model for Insider Threat Prediction" *IEEE SMC Information Assurance and Security Workshop, 2007. IAW '07.*, West Point, NY doi: <http://dx.doi.org/10.1109/iaw.2007.381939>.
- Anderson, J.P. 1972. *Computer Security Technology Planning Study. Volume 2*. Springfield, VA: NTIS of U.S. Dept. of Commerce. <http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=AD0772806>.
- Ashworth, Michael J., and Kathleen M. Carley. 2006. "Who You Know Vs. What You Know: The Impact of Social Position and Knowledge on Team Performance." *The Journal of Mathematical Sociology* 30 (1): 43-75. doi: <http://dx.doi.org/10.1080/00222500500323101>.
- Astley, W. Graham, and Paramjit S. Sachdeva. 1984. "Structural Sources of Intraorganizational Power: A Theoretical Synthesis." *Academy of Management Review* 9 (1): 104-113. doi: <http://dx.doi.org/10.5465/AMR.1984.4278071>.
- Band, Stephen R, Dawn M Cappelli, Lynn F Fischer, Andrew P Moore, Eric D Shaw, and Randall F Trzeciak. 2006. *Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis*. <http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA459911>.
- Barab, Sasha, Steve Schatz, and Rebecca Scheckler. 2004. "Using Activity Theory to Conceptualize Online Community and Using Online Community to Conceptualize Activity Theory." *Mind, Culture, and Activity* 11 (1): 25-47. doi: [http://dx.doi.org/10.1207/s15327884mca1101\\_3](http://dx.doi.org/10.1207/s15327884mca1101_3).
- Batagelj, Vladimir, and Andrej Mrvar. 2002. "Pajek— Analysis and Visualization of Large Networks." In *Graph Drawing*, 8-11. Berlin: Springer.

- Bell, D.E., and L.J. LaPadula. 1973. *Secure Computer Systems: Mathematical Foundations*. Bedford, MA: MITRE Corporation.  
<http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=AD0770768>.
- Benbasat, Izak, David K. Goldstein, and Melissa Mead. 1987. "The Case Research Strategy in Studies of Information Systems." *MIS Quarterly* 11 (3): 369-386.  
<http://www.jstor.org/stable/248684>.
- Beznosov, Konstantin, and Olga Beznosova. 2007. "On the Imbalance of the Security Problem Space and Its Expected Consequences." *Information Management & Computer Security* 15 (5): 420-431.  
<http://search.proquest.com/docview/212368690?accountid=10382>.
- Biba, K.J. 1977. *Integrity Considerations for Secure Computer Systems*. Bedford, MA: MITRE Corporation.  
<http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA039324>.
- Bishop, Matt. 2005. "Position: "Insider" Is Relative." In *Proceedings of the 2005 Workshop on New Security Paradigms, Lake Arrowhead, CA, USA*, 77-78. 1146288: ACM. doi: <http://dx.doi.org/10.1145/1146269.1146288>.
- Bishop, Matt, Sophie Engle, Sean Peisert, Sean Whalen, and Carrie Gates. 2008. "We Have Met the Enemy and He Is Us." In *Proceedings of the 2008 Workshop on New Security Paradigms, Lake Tahoe, California, USA*, 1-12. 1595678: ACM. doi: <http://dx.doi.org/10.1145/1595676.1595678>.
- Bishop, Matt, and Carrie Gates. 2008. "Defining the Insider Threat" *Proceedings of the 4th Annual Workshop on Cyber Security and Information Intelligence Research: Developing Strategies to Meet the Cyber Security and Information Intelligence Challenges Ahead*: ACM. doi: <http://dx.doi.org/10.1145/1413140.1413158>.
- Bishop, Matt, Dieter Gollmann, Jeffrey Hunker, Christian W Probst, Ulrich Flegel, Florian Kerschbaum, Richard Wacker, Julien Vayssière, and Gunter Bitz. 2008. "Countering Insider Threats" *Dagstuhl Seminar Proceedings 08302, Dagstuhl, Germany*: <http://drops.dagstuhl.de/opus/volltexte/2008/1793/pdf/08302.SWM.1793.pdf>.
- Bloomfield, Brian P., Rod Coombs, David J. Cooper, and David Rea. 1992. "Machines and Manoeuvres: Responsibility Accounting and the Construction of Hospital Information Systems." *Accounting, Management and Information Technologies* 2 (4): 197-219. doi: [http://dx.doi.org/10.1016/0959-8022\(92\)90009-H](http://dx.doi.org/10.1016/0959-8022(92)90009-H).
- Bonner, William, and Mike Chiasson. 2005. "If Fair Information Principles Are the Answer, What Was the Question? An Actor-Network Theory Investigation of the Modern Constitution of Privacy." *Information and Organization* 15 (4): 267-293. doi: <http://dx.doi.org/10.1016/j.infoandorg.2005.03.001>.
- Borgatti, Stephen P. 2005. "Centrality and Network Flow." *Social Networks* 27 (1): 55-71. doi: <http://dx.doi.org/10.1016/j.socnet.2004.11.008>.

- Borgatti, Stephen P., and José-Luis Molina. 2005. "Toward Ethical Guidelines for Network Research in Organizations." *Social Networks* 27 (2): 107-117. doi: <http://dx.doi.org/10.1016/j.socnet.2005.01.004>.
- Bostrom, Robert P., and J. Stephen Heinen. 1977a. "MIS Problems and Failures: A Socio-Technical Perspective, Part II: The Application of Socio-Technical Theory." *MIS Quarterly* 1 (4): 11-28. doi: <http://dx.doi.org/10.2307/249019>.
- . 1977b. "MIS Problems and Failures: A Socio-Technical Perspective. Part I: The Causes." *MIS Quarterly* 1 (3): 17-32. doi: <http://dx.doi.org/10.2307/248710>.
- Brass, Daniel J. 1984. "Being in the Right Place: A Structural Analysis of Individual Influence in an Organization." *Administrative Science Quarterly* 29 (4): 518-539. doi: <http://dx.doi.org/10.2307/2392937>.
- Brass, Daniel J., and Marlene E. Burkhardt. 1993. "Potential Power and Power Use: An Investigation of Structure and Behavior." *The Academy of Management Journal* 36 (3): 441-470. doi: <http://dx.doi.org/10.2307/256588>.
- Brewer, D. F. C., and M. J. Nash. 1989. "The Chinese Wall Security Policy" *Proceedings of the IEEE Symposium on Security and Privacy*, doi: <http://dx.doi.org/10.1109/secpri.1989.36295>.
- Burt, R.S. 1992. *Structural Holes: The Social Structure of Competition*. Cambridge, MA: Harvard University Press.
- Byres, Eric, Matthew Franz, and Darrin Miller. 2004. "The Use of Attack Trees in Assessing Vulnerabilities in Scada Systems" *IEEE International Infrastructure Survivability Workshop (IISW '04), Lisbon, Portugal*: <http://www.ida.liu.se/labs/rtslab/iisw04/camready/SCADA-Attack-Trees-Final.pdf>.
- Callon, M. 1986. "Some Elements of Sociology of Translation: Domestication of the Scallops and the Fishermen of the Saint Brieuc Bay." In *Power, Action, and Belief: A New Sociology of Knowledge?*, ed. J. Law, 196-223. London: Routledge.
- Cappelli, D., A. Moore, T.J. Shimeall, and R. Trzeciak. 2009. *Common Sense Guide to Prevention and Detection of Insider Threats*. Pittsburgh, PA: Software Engineering Institute of Carnegie Mellon University. <http://www.cylab.cmu.edu/files/pdfs/CERT/CSG-V3.pdf>.
- Cappelli, D., A. Moore, and R. Trzeciak. 2012. *The CERT Guide to Insider Threats*. Upper Saddle River, NJ: Addison-Wesley.
- Carayon, Pascale, and Sara Kraemer. 2002. "Macroergonomics in WWDU: What About Computer and Information System Security" *Proceedings of the Sixth International Scientific Conference on Work With Display Units—WWDU 2002—World Wide Work, Berlin, Germany*: ERGONOMIC Institut für Arbeits- und Sozialforschung Forschungsgesellschaft mbH. <http://cqpi.engr.wisc.edu/system/files/berlin.pdf>.
- Carley, K M. 2003. *Dynamic Network Analysis*. Washington, DC: The National Academies Press. [http://www.nap.edu/catalog.php?record\\_id=10735](http://www.nap.edu/catalog.php?record_id=10735).

- Carley, K. M. 2002. "Smart Agents and Organizations of the Future." In *Handbook of New Media: Social Shaping and Consequences of ICT*, eds Lievrouw A.L. and Livingstone S.M. London: SAGE.
- Carley, K.M. 2000. *Information Security: The Human Perspective*. Pittsburgh, PA: Institute for Software Research , School of Computer Science, Carnegie Mellon University.  
[http://www.casos.cs.cmu.edu/publications/working\\_papers/InfoSecforPita.pdf](http://www.casos.cs.cmu.edu/publications/working_papers/InfoSecforPita.pdf).
- Carley, K.M., and J. Reminga. 2004. *ORA: Organization Risk Analyzer*. Pittsburgh, PA: Institute for Software Research , School of Computer Science, Carnegie Mellon University.  
<http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA460034>.
- Carley, Kathleen M., Jürgen Pfeffer, Jeff Reminga, Jon Storricks, and Dave Columbus. 2012. *ORA User's Guide 2012*. Pittsburgh, PA: Institute for Software Research, School of Computer Science, Carnegie Mellon University.  
<http://www.casos.cs.cmu.edu/publications/papers/CMU-ISR-12-105.pdf>.
- Carley, Kathleen M., Jeffrey Reminga, and Natasha Kamneva. 2003. "Destabilizing Terrorist Networks" *Proceedings of the NAACSOS Conference, Pittsburgh, PA*:  
<http://casos.cs.cmu.edu/publications/papers/Carley-NAACSOS-03.pdf>.
- Carpenter, Perry, and Andrew Walls. 2011. *Best Practices for Managing 'Insider' Security Threats, 2011 Update*. Gartner IT Research.  
<https://www.gartner.com/doc/1604216/best-practices-managing-insider-security>.
- Checkland, Peter B. 1989. "Soft Systems Methodology." *Human Systems Management* 8 (4): 273-289. doi: <http://dx.doi.org/10.3233/HSM-1989-8405>.
- Chee-Wooi, Ten, Liu Chen-Ching, and M. Govindarasu. 2007. "Vulnerability Assessment of Cybersecurity for Scada Systems Using Attack Trees" *IEEE Power Engineering Society General Meeting., Tampa, FL, USA*, doi: <http://dx.doi.org/10.1109/PES.2007.385876>.
- Chen, WenShin, and Rudy Hirschheim. 2004. "A Paradigmatic and Methodological Examination of Information Systems Research from 1991 to 2001." *Information Systems Journal* 14 (3): 197-235. doi: <http://dx.doi.org/10.1111/j.1365-2575.2004.00173.x>.
- Cheng, Pau-Chen, P. Rohatgi, C. Keser, P. A. Karger, G. M. Wagner, and A. S. Reninger. 2007a. "Fuzzy Multi-Level Security: An Experiment on Quantified Risk-Adaptive Access Control" *IEEE Symposium on Security and Privacy, Berkeley, CA*, doi: <http://dx.doi.org/10.1109/SP.2007.21>.
- Cheng, Pau-Chen, Pankaj Rohatgi, Claudia Keser, Paul A. Karger, Grant M. Wagner, and Angela Schuett Reninger. 2007b. *Fuzzy Multi-Level Security : An Experiment on Quantified Risk-Adaptive Access Control*. RC24190 (W0702-085). Yorktown Heights, NY, USA.  
[http://domino.research.ibm.com/library/cyberdig.nsf/papers/D2C93A2DF2AFD3968525728F00528D26/\\$File/RC24190.pdf](http://domino.research.ibm.com/library/cyberdig.nsf/papers/D2C93A2DF2AFD3968525728F00528D26/$File/RC24190.pdf).
- Cherns, A. 1987. "Principles of Sociotechnical Design Revisted." *Human Relations* 40 (3): 153-161. doi: <http://dx.doi.org/10.1177/001872678704000303>

- Cherns, Albert. 1976. "The Principles of Sociotechnical Design." *Human Relations* 29 (8): 783-792. doi: <http://dx.doi.org/10.1177/001872677602900806>.
- Chew, Elizabeth, Marianne Swanson, Kevin Stine, Nadya Bartol, Anthony Brown, and Will Robinson. 2008. *NIST Special Publication 800-55 Revision 1: Performance Measurement Guide for Information Security*. Gaithersburg, MD, USA: National Institute of Standards and Technology (NIST), USA. <http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf>.
- Chinchani, R., A. Iyer, H. Q. Ngo, and S. Upadhyaya. 2004. *A Target-Centric Formal Model for Insider Threat and More*. Buffalo, NY, USA: University of Buffalo. <http://www.cse.buffalo.edu/tech-reports/2004-16.pdf>.
- . 2005. "Towards a Theory of Insider Threat Assessment" *Proceedings of the International Conference on Dependable Systems and Networks (DSN 2005)*, Yokohama, Japan, doi: <http://dx.doi.org/10.1109/dsn.2005.94>.
- Ching, W.K., and K.N. Michael. 2006. *Markov Chains: Models, Algorithms and Applications*. New York: Springer.
- Cho, Hichang, Geri Gay, Barry Davidson, and Anthony Ingraffea. 2007. "Social Networks, Communication Styles, and Learning Performance in a CSCL Community." *Computers & Education* 49 (2): 309-329. doi: <http://dx.doi.org/10.1016/j.compedu.2005.07.003>.
- Christopoulos, D., and Lucia Quaglia. 2009. "Network Constraints in EU Banking Regulation: The Capital Requirements Directive." *Journal of Public Policy* 29 (Special Issue 02): 179-200. [http://journals.cambridge.org/article\\_S0143814X09001068](http://journals.cambridge.org/article_S0143814X09001068).
- Christopoulos, Dimitrios C. 2006. "Relational Attributes of Political Entrepreneurs: A Network Perspective." *Journal of European Public Policy* 13 (5): 757-778. doi: <http://dx.doi.org/10.1080/13501760600808964>.
- Clark, David D., and David R. Wilson. 1987. "A Comparison of Commercial and Military Computer Security Policies" *IEEE Symposium on Security and Privacy, Oakland, CA*: <http://doi.ieeecomputersociety.org/10.1109/SP.1987.10001>.
- Clegg, Chris, Carolyn Axtell, Leela Damodaran, Barbara Farbey, Richard Hull, Raymond Lloyd-Jones, John Nicholls, R. E. G. Sell, and Christine Tomlinson. 1997. "Information Technology: A Study of Performance and the Role of Human and Organizational Factors." *Ergonomics* 40 (9): 851-871. doi: <http://dx.doi.org/10.1080/001401397187694>.
- Clegg, Chris W. 2000. "Sociotechnical Principles for System Design." *Applied Ergonomics* 31 (5): 463-477. doi: [http://dx.doi.org/10.1016/S0003-6870\(00\)00009-0](http://dx.doi.org/10.1016/S0003-6870(00)00009-0).
- Clemens, Pat L. 2002. "Fault Tree Analysis." <http://fault-tree.net/papers/clemens-fta-tutorial.pdf>.
- Coyle, Robert Geoffrey. 1996. *System Dynamics Modelling: A Practical Approach*. Vol. 1. Boca Raton, FL, USA: CRC Press.

- Cummings, Adam, Todd Lewellen, David McIntire, Andrew Moore, and Randall Trzeciak. 2012. *Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector*. CMU/SEI-2012-SR-004. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University. <http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=27971>.
- Dacier, M., and Y. Deswarte. 1994. "Privilege Graph: An Extension to the Typed Access Matrix Model." In *Computer Security—ESORICS 94*, edited by Dieter Gollmann, Berlin, Germany: Springer.
- Dacier, M., Y. Deswarte, and M. Kaâniche. 1996. "Quantitative Assessment of Operational Security: Models and Tools." In *Information Systems Security*, edited by S. K. Katsikas and D. Gritzalis, London: Chapman & Hall.
- Dantu, R., K. Loper, and P. Kolan. 2004. "Risk Management Using Behavior Based Attack Graphs" *Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC 2004), Las Vegas, NV*: IEEE. doi: <http://dx.doi.org/10.1109/ITCC.2004.1286496>.
- Darke, Peta, Graeme Shanks, and Marianne Broadbent. 1998. "Successfully Completing Case Study Research: Combining Rigour, Relevance and Pragmatism." *Information Systems Journal* 8 (4): 273-289. doi: <http://dx.doi.org/10.1046/j.1365-2575.1998.00040.x>.
- Denning, Dorothy E. 1976. "A Lattice Model of Secure Information Flow." *Communications of the ACM* 19 (5): 236-243. doi: <http://dx.doi.org/10.1145/360051.360056>.
- Dhillon, Gurpreet, and James Backhouse. 2001. "Current Directions in IS Security Research: Towards Socio-Organizational Perspectives." *Information Systems Journal* 11 (2): 127-153. doi: <http://dx.doi.org/10.1046/j.1365-2575.2001.00099.x>.
- Dijkstra, E. W. 1959. "A Note on Two Problems in Connexion with Graphs." *Numerische Mathematik* 1 (1): 269-271. doi: <http://dx.doi.org/10.1007/BF01386390>.
- Ekelhart, A., S. Fenz, and T. Neubauer. 2009. "AURUM: A Framework for Information Security Risk Management" *42nd Hawaii International Conference on System Sciences. HICSS '09., Big Island, Hawaii*: IEEE. doi: <http://dx.doi.org/10.1109/HICSS.2009.82>.
- Eschenfelder, K. R., and L. C. Chase. 2002. "Socio-Technical Networks of Large, Post-Implementation Web Information Systems: Tracing Effects and Influences" *Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS), Big Island, Hawaii*: IEEE Computer Society. doi: <http://dx.doi.org/10.1109/HICSS.2002.994032>.
- Evangelidis, Adrianos. 2004. "Frames—a Risk Assessment Framework for E-Services." *Electronic Journal of e-Government* 2 (1): 21-30. <http://www.ejeg.com/issue/download.html?idArticle=19>.
- Ferraiolo, D.F., and D.R. Kuhn. 1992. "Role-Based Access Controls." In *15th National Computer Security Conference, Baltimore, MD*, 554 - 563. <http://arxiv.org/abs/0903.2171v1>.

- Ferraiolo, David, Janet Cugini, and D Richard Kuhn. 1995. "Role-Based Access Control (RBAC): Features and Motivations" *Proceedings of 11th Annual Computer Security Application Conference, New Orleans, Louisiana*: IEEE Computer Society Press. <http://csrc.nist.gov/groups/SNS/rbac/documents/ferraiolo-cugini-kuhn-95.pdf>.
- Ferraiolo, David F., Ravi Sandhu, Serban Gavrila, D. Richard Kuhn, and Ramaswamy Chandramouli. 2001. "Proposed NIST Standard for Role-Based Access Control." *ACM Transactions on Information and System Security* 4 (3): 224-274. doi: <http://dx.doi.org/10.1145/501978.501980>.
- Flyvbjerg, Bent. 2006. "Five Misunderstandings About Case-Study Research." *Qualitative Inquiry* 12 (2): 219-245. doi: <http://dx.doi.org/10.1177/1077800405284363>.
- Freeman, Linton C. 1978. "Centrality in Social Networks - Conceptual Clarification." *Social Networks* 1 (3): 215-239. doi: [http://dx.doi.org/10.1016/0378-8733\(78\)90021-7](http://dx.doi.org/10.1016/0378-8733(78)90021-7).
- Frigault, M., and Wang Lingyu. 2008. "Measuring Network Security Using Bayesian Network-Based Attack Graphs" *32nd Annual IEEE International Conference on Computer Software and Applications. COMPSAC '08., Turku, Finland*, doi: <http://dx.doi.org/10.1109/COMPSAC.2008.88>.
- Frohmann, Bernd. 1995. "Taking Information Policy Beyond Information Science: Applying the Actor Network Theory" *23rd Annual Conference of the Canadian Association for Information Science, Edmonton, Alberta*: <http://www.ualberta.ca/dept/slis/cais/frohmann.htm>.
- Gao, Ping. 2005. "Using Actor-Network Theory to Analyse Strategy Formulation." *Information Systems Journal* 15 (3): 255-275. doi: <http://dx.doi.org/10.1111/j.1365-2575.2005.00197.x>.
- Garg, P. K., and W. Scacchi. 1989. "ISHYS: Designing an Intelligent Software Hypertext System." *IEEE Expert* 4 (3): 52-63. doi: <http://dx.doi.org/10.1109/64.43270>.
- Gibbons, Deborah E. 2004. "Friendship and Advice Networks in the Context of Changing Professional Values." *Administrative Science Quarterly* 49 (2): 238-262. <http://asq.sagepub.com/content/49/2/238.short#cited-by>.
- Glaser, Edward L. 1967. "A Brief Description of Privacy Measures in the Multics Operating System." In *Proceedings of the Spring Joint Computer Conference, Atlantic City, New Jersey*, 303-304. 1465529: ACM. doi: <http://dx.doi.org/10.1145/1465482.1465529>.
- Godik, Simon, Anne Anderson, Bill Parducci, Polar Humenn, and Sekhar Vajjhala. 2002. *OASIS Extensible Access Controlmarkup Language (XACML)* <https://www.oasis-open.org/committees/xacml/repository/draft-xacml-schema-policy-13.pdf>.
- Graham, G. Scott, and Peter J. Denning. 1972. "Protection: Principles and Practice." In *Proceedings of the Spring Joint Computer Conference, Atlantic City, New Jersey*, 417-429. 1478928: ACM. doi: <http://dx.doi.org/10.1145/1478873.1478928>.
- Granovetter, Mark. 1983. "The Strength of Weak Ties: A Network Theory Revisited." *Sociological Theory* 1 (1): 201-233. doi: <http://dx.doi.org/10.2307/202051>.

- Granovetter, Mark S. 1973. "The Strength of Weak Ties." *American Journal of Sociology* 78 (6): 1360-1380. <http://www.jstor.org/stable/2776392>.
- Greenwald, Glenn. 2013. The NSA Files. The Guardian. Jan 20, 2014 Accessed Jan 20, 2014, <http://www.theguardian.com/world/the-nsa-files>.
- Greitzer, F., P. Paulson, L. Kangas, L. Franklin, T. Edgar, and D. Frincke. 2009. *Predictive Modelling for Insider Threat Mitigation*. <http://www.pnl.gov/CogInformatics/media/pdf/TR-PACMAN-65204.pdf>.
- Hagberg, Aric A., Daniel A. Schult, and Pieter J. Swart. 2008. "Exploring Network Structure, Dynamics, and Function Using NetworkX" *7th Python in Science Conference (SciPy2008)*, Pasadena, CA, USA: <http://math.lanl.gov/~hagberg/Publications/hagberg-2008-exploring.shtml>.
- Hanley, Michael. 2011. *Deriving Candidate Technical Controls and Indicators of Insider Attack from Socio-Technical Models and Data*. CMU/SEI-2011-TN-003. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University. <http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=9787>.
- Harrison, Michael A., Walter L. Ruzzo, and Jeffrey D. Ullman. 1976. "Protection in Operating Systems." *Communications of the ACM* 19 (8): 461-471. doi: <http://dx.doi.org/10.1145/360303.360333>.
- Haythornthwaite, Caroline. 1996. "Social Network Analysis: An Approach and Technique for the Study of Information Exchange." *Library & Information Science Research* 18 (4): 323-342. doi: [http://dx.doi.org/10.1016/S0740-8188\(96\)90003-1](http://dx.doi.org/10.1016/S0740-8188(96)90003-1).
- Haythornthwaite, Caroline, and Barry Wellman. 1998. "Work, Friendship, and Media Use for Information Exchange in a Networked Organization." *Journal of the American Society for Information Science* 49 (12): 1101-1114. doi: [http://dx.doi.org/10.1002/\(SICI\)1097-4571\(1998\)49:12<1101::AID-ASI6>3.0.CO;2-Z](http://dx.doi.org/10.1002/(SICI)1097-4571(1998)49:12<1101::AID-ASI6>3.0.CO;2-Z).
- Hedstrom, K., G. Dhillon, and F. Karlsson. 2010. "Using Actor Network Theory to Understand Information Security Management." In *Security and Privacy - Silver Linings in the Cloud*, eds K. Rannenber, V. Varadharajan and C. Weber, 43-54. Berlin: Springer-Verlag
- Heiser, Jay, and Tom Scholtz. 2009. *Top-Five Issues and Research Agenda, 2009-2010: The Chief Information Security Officer*. Gartner IT Research. [http://www.gartner.com/it/content/1219300/1219313/top\\_five\\_issues\\_research.pdf](http://www.gartner.com/it/content/1219300/1219313/top_five_issues_research.pdf).
- Herrmann, Debra S. 2007. *Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience, and ROI*. Boca Raton, Florida: Taylor and Francis Group.
- Hevner, A R, Salvatore T. March, Jinsoo Park, and Sudha Ram. 2004. "Design Science in Information Systems Research." *MIS Quarterly* 28 (1): 75-105. <http://www.jstor.org/stable/25148625>.
- Hevner, AR. 2007. "The Three Cycle View of Design Science Research." *Scandinavian Journal of Information Systems* 19 (2): 87-92. <http://aisel.aisnet.org/sjis/vol19/iss2/4/>.

- Hitchings, Jean. 1995. "Deficiencies of the Traditional Approach to Information Security and the Requirements for a New Methodology." *Computers & Security* 14 (5): 377-383. doi: [http://dx.doi.org/10.1016/0167-4048\(95\)97088-R](http://dx.doi.org/10.1016/0167-4048(95)97088-R).
- Hu, Vincent C., David Ferraiolo, Rick Kuhn, Adam Schnitzer, Kenneth Sandlin, Robert Miller, and Karen Scarfone. 2014. *Guide to Attribute Based Access Control (ABAC) Definition and Considerations*. NIST SP 800-162. Gaithersburg, MD: National Institute of Standards and Technology, USA. <http://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.sp.800-162.pdf>.
- Hunker, J., and C.W. Probst. 2011. "Insiders and Insider Threats—an Overview of Definitions and Mitigation Techniques." *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications* 2 (1): 4-27. <http://isyu.info/jowua/papers/jowua-v2n1-1.pdf>.
- Iivari, Juhani, Rudy Hirschheim, and Heinz K. Klein. 1998. "A Paradigmatic Analysis Contrasting Information Systems Development Approaches and Methodologies." *Information Systems Research* 9 (2): 164-193. doi: <http://dx.doi.org/10.1287/isre.9.2.164>.
- INFOSEC Research Council. 2005. *Hard Problems List*. [http://www.infosec-research.org/docs\\_public/20051130-IRC-HPL-FINAL.pdf](http://www.infosec-research.org/docs_public/20051130-IRC-HPL-FINAL.pdf).
- International Organisation for Standardisation. 2005a. *ISO/IEC 27001:2005 - Information Technology - Security Techniques - Information Security Management Systems - Requirements*. ISO (ISO/IEC 27001:2005). <http://www.iso.org/iso/home/standards/management-standards/iso27001.htm>.
- . 2005b. *ISO/IEC 27002:2005 - Information Technology - Security Techniques - Code of Practice for Information Security Management*. ISO (ISO/IEC 27002:2005). [http://www.iso.org/iso/catalogue\\_detail?csnumber=50297](http://www.iso.org/iso/catalogue_detail?csnumber=50297).
- . 2009. *ISO/IEC 31010: Risk Management - Risk Assessment Techniques*. ISO (ISO/IEC 31010:2009). <http://infostore.saiglobal.com/store/Details.aspx?productID=1382224>.
- . 2011. *ISO/IEC 27005:2011 Information Technology—Security Techniques—Information Security Risk Management Standard*. ISO (ISO/IEC 27005:2011). [http://www.iso.org/iso/catalogue\\_detail?csnumber=56742](http://www.iso.org/iso/catalogue_detail?csnumber=56742).
- Jansen, Wayne. 2009. *Directions in Security Metrics Research*. Gaithersburg, MD, USA: USA National Institute of Standards and Technology. [http://csrc.nist.gov/publications/nistir/ir7564/nistir-7564\\_metrics-research.pdf](http://csrc.nist.gov/publications/nistir/ir7564/nistir-7564_metrics-research.pdf).
- Jaquith, Andrew. 2007. *Security Metrics: Replacing Fear, Uncertainty, and Doubt*. Upper Saddle River, NJ, U.S.A: Addison-Wesley
- Jin, Xin, Ram Krishnan, and Ravi Sandhu. 2012. "A Unified Attribute-Based Access Control Model Covering DAC, MAC and RBAC." In *Data and Applications Security and Privacy XXVI*, eds Nora Cuppens-Bouahia, Frédéric Cuppens and Joaquin Garcia-Alfaro, 41-55. Berlin: Springer
- Jones, Eric, Travis Oliphant, and Pearu Peterson. 2001. *SciPy: Open Source Scientific Tools for Python* <http://www.scipy.org>.

- Kaghan, William N., and Geoffrey C. Bowker. 2001. "Out of Machine Age?: Complexity, Sociotechnical Systems and Actor Network Theory." *Journal of Engineering and Technology Management* 18 (3–4): 253-269. doi: [http://dx.doi.org/10.1016/S0923-4748\(01\)00037-6](http://dx.doi.org/10.1016/S0923-4748(01)00037-6).
- Kandala, S., R. Sandhu, and V. Bhamidipati. 2011. "An Attribute Based Framework for Risk-Adaptive Access Control Models" *Sixth International Conference on Availability, Reliability and Security (ARES), Vienna, Austria*: IEEE. doi: <http://dx.doi.org/10.1109/ARES.2011.41>.
- Karp, Alan H, Harry Haury, and Michael H Davis. 2009. *From ABAC to ZBAC: The Evolution of Access Control Models*. HPL-2009-30. Hewlett-Packard Development Company. [http://www.hpl.hp.com/techreports/2009/HPL-2009-30.pdf?jumpid=reg\\_R1002\\_USEN](http://www.hpl.hp.com/techreports/2009/HPL-2009-30.pdf?jumpid=reg_R1002_USEN).
- Kim, Taemie, Agnes Chang, Lindsey Holland, and Alex Sandy Pentland. 2008. "Meeting Mediator: Enhancing Group Collaboration Using Sociometric Feedback." In *Proceedings of the 2008 ACM Conference on Computer Supported Cooperative Work, San Diego, CA, USA*, 457-466. 1460636: ACM. doi: <http://dx.doi.org/10.1145/1460563.1460636>.
- Kissel, Richard. 2013. *Glossary of Key Information Security Terms*. NIST IR 7298. Gaithersburg, MD: National Institute of Standards and Technology , USA. <http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf>.
- Kleiner, Brian M. 2006. "Macroergonomics: Analysis and Design of Work Systems." *Applied Ergonomics* 37 (1): 81-89. doi: <http://dx.doi.org/10.1016/j.apergo.2005.07.006>.
- Kling, R, and W Scacchi. 1982. "The Web of Computing: Computer Technology as Social Organisations." *Advances in Computers* 21: 1-90. <http://ics.uci.edu/~wscacchi/Papers/Vintage/Kling%26Scacchi1982-OCR.pdf>.
- Kling, Rob, Geoffrey McKim, and Adam King. 2003. "A Bit More to It: Scholarly Communication Forums as Socio-Technical Interaction Networks." *Journal of the American Society for Information Science and Technology* 54 (1): 47-67. doi: <http://dx.doi.org/10.1002/asi.10154>.
- Krackhardt, D, and KM Carley. 1998. "A PCANS Model of Structure in Organization" *1998 International Symposium on Command and Control Research and Technology, Monterey, California*: [http://www.casos.cs.cmu.edu/publications/working\\_papers/pecans1.pdf](http://www.casos.cs.cmu.edu/publications/working_papers/pecans1.pdf).
- Krackhardt, David. 1990. "Assessing the Political Landscape: Structure, Cognition, and Power in Organizations." *Administrative Science Quarterly* 35 (2): 342-369. doi: <http://dx.doi.org/10.2307/2393394>.
- . 1992. "The Strength of Strong Ties: The Importance of Philos in Organizations." In *Networks and Organizations: Structure, Form, and Action*, eds N. Nohria and R. Eccles, 216-239. Boston, MA: Harvard Business Review Press.
- Kraemer, Sara, and Pascale Carayon. 2007. "Human Errors and Violations in Computer and Information Security: The Viewpoint of Network Administrators and Security Specialists." *Applied Ergonomics* 38 (2): 143-154. doi: <http://dx.doi.org/10.1016/j.apergo.2006.03.010>.

- Kraemer, Sara, Pascale Carayon, and John Clem. 2009. "Human and Organizational Factors in Computer and Information Security: Pathways to Vulnerabilities." *Computers & Security* 28 (7): 509-520. doi: <http://dx.doi.org/10.1016/j.cose.2009.04.006>.
- Krebs, Valdis. 2002. "Uncloaking Terrorist Networks." *First Monday*. <http://journals.uic.edu/ojs/index.php/fm/article/view/941>.
- Kuechler, B, and V Vaishnavi. 2008. "On Theory Development in Design Science Research: Anatomy of a Research Project." *European Journal of Information Systems* 17 (5): 489-504. <http://dx.doi.org/10.1057/ejis.2008.40>.
- Kuhn, D. Richard, Vincent C. Hu, W. Timothy Polk, and Shu-Jen Chang. 2001. *NIST SP 800-32: Introduction to Public Key Technology and the Federal PKI Infrastructure*. Gaithersburg, MD: National Institute of Standards and Technology (NIST) , USA. <http://csrc.nist.gov/publications/nistpubs/800-32/sp800-32.pdf>.
- Lampson, Butler W. 1971. "Protection" *Proceedings of the Fifth Princeton Symposium on Information Sciences and Systems, Princeton, NJ, 775268* doi: <http://dx.doi.org/10.1145/775265.775268>.
- Latour, Bruno. 1988. *The Pasteurization of France*. Cambridge, MA: Harvard University Press.
- . 2005. *Reassembling the Social : An Introduction to Actor-Network-Theory*. Oxford, U.K.: Oxford University Press.
- Law, John. 1992. "Notes on the Theory of the Actor-Network: Ordering, Strategy, and Heterogeneity." *Systems Practice* 5 (4): 379-393. doi: <http://dx.doi.org/10.1007/BF01059830>.
- Lee, Allen S. 1989. "A Scientific Methodology for MIS Case Studies." *MIS Quarterly* 13 (1): 33-50. <http://www.jstor.org/stable/248698>.
- Lee, JS, and KM Carley. 2004. *OrgAhead: A Computational Model of Organizational Learning and Decision Making*. CMU-ISRI-04-117. Pittsburgh, PA: Carnegie Mellon University School of Computer Science. <http://www.casos.cs.cmu.edu/publications/papers/CMU-ISRI-04-117.pdf>.
- Lewis, T.G. 2006. *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*. Hoboken, New Jersey: John Wiley and Sons.
- Likert, R. 1932. "A Technique for the Measurement of Attitudes." *Archives of Psychology* 22 55.
- Lincoln, James R., and Miller Jon. 1979. "Work and Friendship Ties in Organizations: A Comparative Analysis of Relation Networks." *Administrative Science Quarterly* 24 (2): 181-199. doi: <http://dx.doi.org/10.2307/2392493>.
- Lipner, Steven B. 1982. "Non-Discretionary Controls for Commercial Applications" *IEEE Symposium on Security and Privacy, Oakland, CA*: <http://doi.ieeecomputersociety.org/10.1109/SP.1982.10022>.

- Lyytinen, Kalle, Lars Lyytinen, Janne Mathiassen, and Ropponen. 1998. "Attention Shaping and Software Risk—a Categorical Analysis of Four Classical Risk Management Approaches." *Information Systems Research* 9 (3): 233-255.  
<http://pubsonline.informs.org/doi/abs/10.1287/isre.9.3.233>.
- Lyytinen, Kalle, and Mike Newman. 2008. "Explaining Information Systems Change: A Punctuated Socio-Technical Change Model." *European Journal of Information Systems* 17 (6): 589-613. doi: <http://dx.doi.org/10.1057/ejis.2008.50>.
- Maglogiannis, I., E. Zafiroopoulos, A. Platis, and C. Lambrinouidakis. 2006. "Risk Analysis of a Patient Monitoring System Using Bayesian Network Modeling." *Journal of Biomedical Informatics* 39 (6): 637-647. doi: <http://dx.doi.org/10.1016/j.jbi.2005.10.003>.
- Mahring, Magnus, Jonny Holmstrom, Mark Keil, and Ramiro Montealegre. 2004. "Trojan Actor-Networks and Swift Translation: Bringing Actor-Network Theory to IT Project Escalation Studies." *Information Technology & People* 17 (2): 210-238.  
<http://www.emeraldinsight.com/journals.htm?articleid=883603&show=abstract>.
- March, Salvatore T., and Gerald F. Smith. 1995. "Design and Natural Science Research on Information Technology." *Decision Support Systems* 15 (4): 251-266. doi: [http://dx.doi.org/10.1016/0167-9236\(94\)00041-2](http://dx.doi.org/10.1016/0167-9236(94)00041-2).
- Markus, M. Lynne, Ann Majchrzak, and Les Gasser. 2002. "A Design Theory for Systems That Support Emergent Knowledge Processes." *MIS Quarterly* 26 (3): 179-212.  
<http://www.jstor.org/stable/4132330>.
- Marsden, Peter V. 1990. "Network Data and Measurement." *Annual Review of Sociology* 16 (1): 435-463. doi: <http://dx.doi.org/10.1146/annurev.so.16.080190.002251>.
- Massacci, F., J. Mylopoulos, and N. Zannone. 2007. "An Ontology for Secure Socio-Technical Systems." In *Handbook of Ontologies for Business Interaction*, ed. Peter Rittgen. Hershey, PA: IGI Global.
- McCulloh, Ian A., and Kathleen M. Carley. 2008. *Social Network Change Detection*. ADA488427. Pittsburgh, PA: Institute of Software Research, Carnegie Mellon University. <http://www.casos.cs.cmu.edu/publications/papers/CMU-CS-08-116.pdf>.
- McCulloh, Ian, Helen Armstrong, and Anthony Johnson. 2013. *Social Network Analysis with Applications*. New Jersey, U.S.A: Wiley.
- McGraw, R. 2009. "Risk-Adaptable Access Control (RAdAC)" *NIST Privilege (Access) Management Workshop, Gaithersburg, MD*: National Institute of Standards and Technology (NIST), U.S.A.: [http://csrc.nist.gov/news\\_events/privilege-management-workshop/presentations/Bob\\_McGraw.pdf](http://csrc.nist.gov/news_events/privilege-management-workshop/presentations/Bob_McGraw.pdf).
- Meyer, Eric T. 2006. "Socio-Technical Interaction Networks: A Discussion of the Strengths, Weaknesses and Future of Kling's STIN Model." In *Social Informatics: An Information Society for All? In Remembrance of Rob Kling*, eds Jacques Berleur, Markku Nurminen and John Impagliazzo, 37-48. Springer US.
- Monteiro, Eric, and Ole Hanseth. 1996. "Social Shaping of Information Infrastructure: On Being Specific About the Technology." In *Information Technology and Changes in Organizational Work*, ed. W.J. Orlikowski, 325-343. London: Chapman and Hall.

- Moore, Andrew, Dawn Cappelli, Thomas Caron, Eric Shaw, Derrick Spooner, and Randall Trzeciak. 2011. Preliminary Model of Insider Theft of Intellectual Property. ,Software Engineering Institute, Carnegie Mellon University.  
<http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=9855>.
- Moore, Andrew P, David A Mundie, and Matthew L Collins. 2013. "A System Dynamics Model for Investigating Early Detection of Insider Threat Risk" *Proceedings of the 31st International Conference of the System Dynamics Society, Cambridge, MA*:  
<http://www.systemdynamics.org/conferences/2013/proceed/papers/P1028.pdf>.
- Moore, Andrew P., Dawn M. Cappelli, and Randall F. Trzeciak. 2008. *The "Big Picture" of Insider IT Sabotage across U.S. Critical Infrastructures*. CMU/SEI-2008-TR-009. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University.  
<http://www.cert.org/archive/pdf/08tr009.pdf>.
- Motiee, Sara, Kirstie Hawkey, and Konstantin Beznosov. 2010. "Do Windows Users Follow the Principle of Least Privilege?: Investigating User Account Control Practices." In *Proceedings of the Sixth Symposium on Usable Privacy and Security, Redmond, Washington*, 1-13. 1837112: ACM. doi: <http://dx.doi.org/10.1145/1837110.1837112>.
- Mumford, Enid. 1983. *Designing Human Systems for New Technology: The Ethics Method*. Manchester, U.K.: Manchester Business School.
- . 2000. "A Socio-Technical Approach to Systems Design." *Requirements Engineering*. 5 (2): 125-133. doi: <http://dx.doi.org/10.1007/PL00010345>.
- . 2003. "Socio-Technical Design: Its Early History." In *Redesigning Human Systems*, 12-32. Hershey, PA: Information Science Publishing.
- Munteanu, Adrian. 2006. "Information Security Risk Assessment: The Qualitative Versus Quantitative Dilemma" *Managing Information in the Digital Economy: Issues & Solutions - Proceedings of the 6th International Business Information Management Association (IBIMA) Conference, Bonn, Germany*: <http://ssrn.com/abstract=917767>.
- Nash, M. J., and K. R. Poland. 1990. "Some Conundrums Concerning Separation of Duty" *Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy*., doi: <http://dx.doi.org/10.1109/risp.1990.63851>.
- National Institute of Standards and Technology. 2012. *NIST Special Publication 800-30 Revision 1 - Guide for Conducting Risk Assessments*. NIST (NIST 800-30 Rev. 1).  
[http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800\\_30\\_r1.pdf](http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf).
- Nelson, Reed E. 1989. "The Strength of Strong Ties: Social Networks and Intergroup Conflict in Organizations." *The Academy of Management Journal* 32 (2): 377-401. doi: <http://dx.doi.org/10.2307/256367>.
- Ni, Qun, Elisa Bertino, and Jorge Lobo. 2010. "Risk-Based Access Control Systems Built on Fuzzy Inferences." In *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, Beijing, China*, 250-260. 1755719: ACM. doi: <http://dx.doi.org/10.1145/1755688.1755719>.

- Noll, John, and Walt Scacchi. 2001. "Specifying Process-Oriented Hypertext for Organizational Computing." *Journal of Network and Computer Applications* 24 (1): 39-61. doi: <http://dx.doi.org/10.1006/jnca.2000.0122>.
- Olguin, D. O., B. N. Waber, Kim Taemie, A. Mohan, K. Ara, and A. Pentland. 2009. "Sensible Organizations: Technology and Methodology for Automatically Measuring Organizational Behavior." *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*. 39 (1): 43-55. doi: <http://dx.doi.org/10.1109/TSMCB.2008.2006638>.
- Olguin, Daniel Olguin, and Alex Sandy Pentland. 2008. "Social Sensors for Automatic Data Collection" *14th Americas Conference on Information Systems, Toronto, Ontario*: <http://aisel.aisnet.org/amcis2008/171/>.
- Orlikowski, Wanda J., and Jack J. Baroudi. 1991. "Studying Information Technology in Organizations: Research Approaches and Assumptions." *Information Systems Research* 2 (1): 1-28. doi: <http://dx.doi.org/10.1287/isre.2.1.1>.
- Ortalo, R., Y. Deswarte, and M. Kaaniche. 1999. "Experimenting with Quantitative Evaluation Tools for Monitoring Operational Security." *IEEE Transactions on Software Engineering*. 25 (5): 633-650. doi: <http://dx.doi.org/10.1109/32.815323>.
- Peffer, Ken, Tuure Tuunanen, Charles E Gengler, Matti Rossi, Wendy Hui, Ville Virtanen, and Johanna Bragge. 2006. "The Design Science Research Process: A Model for Producing and Presenting Information Systems Research" *Proceedings of the First International Conference on Design Science Research in Information Systems and Technology (DESRIST 2006), Claremont, California*: [http://www.wrsc.org/sites/default/files/documents/000designscresearchproc\\_desrist\\_2006.pdf](http://www.wrsc.org/sites/default/files/documents/000designscresearchproc_desrist_2006.pdf).
- Peffer, Ken, Tuure Tuunanen, Marcus Rothenberger, and Samir Chatterjee. 2008. "A Design Science Research Methodology for Information Systems Research." *Journal of Management Information Systems* 24 (3): 45-77. doi: <http://dx.doi.org/10.2753/MIS0742-1222240302>.
- Peterson, J.L. 1981. *Petri Net Theory and the Modelling of Systems*. Englewoods Cliffs: Prentice-Hall.
- Pfeffer, J. 2013. "Fundamentals of Visualizing Communication Networks." *China Communications* 10 (3): 82-90. doi: <http://dx.doi.org/10.1109/CC.2013.6488833>.
- Pfeffer, J., T. Zorbach, and K. M. Carley. 2013. "Understanding Online Firestorms: Negative Word-of-Mouth Dynamics in Social Media Networks." *Journal of Marketing Communications* 20 (1-2): 117-128. doi: <http://dx.doi.org/10.1080/13527266.2013.797778>.
- Pfeffer, Jürgen, and Kathleen M Carley. 2012a. "Social Networks, Social Media, Social Change." In *Advances in Design for Cross-Cultural Activities Part II*, 273-282. Boca Raton, FL: Taylor and Francis Group.
- Pfeffer, Jürgen, and Kathleen M. Carley. 2012b. "K-Centralities: Local Approximations of Global Measures Based on Shortest Paths." In *Proceedings of the 21st International Conference Companion on World Wide Web, Lyon, France*, 1043-1050. 2188239: ACM. doi: <http://dx.doi.org/10.1145/2187980.2188239>.

- Phillips, C., and L. P. Swiler. 1998. "A Graph-Based System for Network-Vulnerability Analysis" *Proceedings of the 1998 Workshop on New Security Paradigms - NSPW '98, Charlottesville, Virginia*, doi: <http://dx.doi.org/10.1145/310889.310919>.
- Pieters, Wolter. 2011. "Representing Humans in System Security Models: An Actor-Network Approach." *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications* 2 (1): 75-92. <http://doc.utwente.nl/76541/>.
- Pricewaterhouse Coopers, CIO magazine, and CSO magazine. 2014. *The Global State of Information Security Survey*,. Pricewaterhouse Coopers. <http://www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml>.
- Pricewaterhouse Coopers, CSO Magazine, U.S. Secret Service, and CERT Program at Carnegie Mellon University. 2013. *Key Findings from the 2013 U.S. State of Cybercrime Survey*. Pricewaterhouse Coopers. <http://www.pwc.com/us/en/increasing-it-effectiveness/publications/us-state-of-cybercrime.jhtml>.
- Pries-Heje, Jan, Richard Baskerville, and John R Venable. 2008. "Strategies for Design Science Research Evaluation" *Proceedings of the 16th European Conference on Information Systems (ECIS 2008), Galway, Ireland*: <http://aisel.aisnet.org/ecis2008/87>.
- R-core-team. 2013. *R: A Language and Environment for Statistical Computing*. Vienna, Austria. <http://www.R-project.org/>.
- Randazzo, M.R. , M. Keeney, E. Kowalski, D. Cappelli, and A. Moore. 2005. *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector*. CMU/SEI-2004-TR-021 Pittsburgh, PA: Software Engineering Institute , Carnegie Mellon University. <http://repository.cmu.edu/cgi/viewcontent.cgi?article=1459&context=sei>.
- Ray, Indrajit, and Nayot Poolsapassit. 2005. "Using Attack Trees to Identify Malicious Attacks from Authorized Insiders." In *Computer Security – ESORICS 2005*, eds Sabrina deCapitani Vimercati, Paul Syverson and Dieter Gollmann, 231-246. Berlin, Germany: Springer
- Robert H. Courtney, Jr. 1977. "Security Risk Assessment in Electronic Data Processing Systems." In *Proceedings of the National Computer Conference, Dallas, Texas*, 97-104. New York, NY: ACM. doi: <http://dx.doi.org/10.1145/1499402.1499424>.
- Rossum, Guido van. 2013. *The Python Language Reference*. Python Software Foundation. 2013 <http://docs.python.org/py3k/reference/index.html>.
- Saltzer, J. H., and M. D. Schroeder. 1975. "The Protection of Information in Computer Systems." *Proceedings of the IEEE* 63 (9): 1278-1308. doi: <http://dx.doi.org/10.1109/proc.1975.9939>.
- Saltzer, Jerome H. 1974. "Protection and the Control of Information Sharing in Multics." *Communications of the ACM* 17 (7): 388-402. doi: <http://dx.doi.org/10.1145/361011.361067>.
- Samarati, P., and S. de Vimercati. 2001. "Access Control: Policies, Models, and Mechanisms." In *Foundations of Security Analysis and Design*, edited by Riccardo Focardi and Roberto Gorrieri, Berlin, Germany: Springer.

- Sandhu, R., D. Ferraiolo, and R. Kuhn. 2000. "The NIST Model for Role-Based Access Control: Towards a Unified Standard" *ACM workshop on Role-based access control, Berlin, Germany*, doi: <http://dx.doi.org/10.1145/344287.344301>.
- Sandhu, R. S. 1993. "Lattice-Based Access Control Models." *Computer* 26 (11): 9-19. doi: <http://dx.doi.org/10.1109/2.241422>.
- . 1994. "Access Control: Principle and Practice." *IEEE Communications Magazine* 32 (9): 40. doi: <http://dx.doi.org/10.1109/35.312842>.
- Sandhu, R. S., E. J. Coyne, H. L. Feinstein, and C. E. Youman. 1996. "Role-Based Access Control Models." *Computer* 29 (2): 38-47. doi: <http://dx.doi.org/10.1109/2.485845>.
- Sandhu, Ravi, and Pierangela Samarati. 1996. "Authentication, Access Control, and Audit." *ACM Computing Surveys (CSUR)* 28 (1): 241-243. doi: <http://dx.doi.org/10.1145/234313.234412>.
- Satoh, Naoki, and Hiromitsu Kumamoto. 2009. "Analysis of Information Security Problem by Probabilistic Risk Assessment." *International Journal of Computers* 3 (1): 337-347. <http://www.naun.org/main/NAUN/computers/ijcomputers-154.pdf>.
- Saunders, Mark NK, Mark Saunders, Philip Lewis, and Adrian Thornhill. 2011. *Research Methods for Business Students*. 5th Ed. ed: Pearson Education, Harlow, England.
- Savola, Reijo M. 2007. "Towards a Taxonomy for Information Security Metrics." In *Proceedings of the 2007 ACM Workshop on Quality of Protection, Alexandria, Virginia, USA*, 28-30. 1314266: ACM. doi: <http://dx.doi.org/10.1145/1314257.1314266>.
- Scacchi, Walt. 2005. "Socio-Technical Interaction Networks in Free/Open Source Software Development Processes." In *Software Process Modeling*, eds SilviaT Acuña and Natalia Juristo, 1-27. Springer US.
- Schneider, F. B. 2003. "Least Privilege and More " *IEEE Security & Privacy* 1 (5): 55-59. doi: <http://dx.doi.org/10.1109/MSECP.2003.1236236>.
- Schneider, Fred B. 2000. "Enforceable Security Policies." *ACM Transactions on Information Systems Security (TISSEC)* 3 (1): 30-50. doi: <http://dx.doi.org/10.1145/353323.353382>.
- Schneier, Bruce. 1999. "Attack Trees." *Dr. Dobb's Journal* 24 (12): 21-29. <https://www.schneier.com/attacktrees.pdf>.
- Shane, Scott, and Andrew W. Lehren. 2010. "Leaked Cables Offer Raw Look at U.S. Diplomacy." *The New York Times*. Accessed Jan 20, 2014, [http://www.nytimes.com/2010/11/29/world/29cables.html?\\_r=0](http://www.nytimes.com/2010/11/29/world/29cables.html?_r=0).
- Simon, R. T., and M. E. Zurko. 1997. "Separation of Duty in Role-Based Environments" *Proceedings of the 10th Computer Security Foundations Workshop, Rockport, Massachusetts* doi: <http://dx.doi.org/10.1109/csfw.1997.596811>.
- Siponen, Mikko T., and Harri Oinas-Kukkonen. 2007. "A Review of Information Security Issues and Respective Research Contributions." *ACM SIGMIS Database* 38 (1): 60-80. doi: <http://dx.doi.org/10.1145/1216218.1216224>.

- Smith, M., N. Milic-Frayling, B. Shneiderman, E. Mendes Rodrigues, J. Leskovec, and C. Dunne. 2010. "NodeXL: A Free and Open Network Overview, Discovery and Exploration Add-in for Excel 2007/2010." The Social Media Research Foundation. <http://nodexl.codeplex.com/>.
- Standards Australia/Standards New Zealand. 2013. *SA/SNZ HB 89:2013 Handbook - Risk Management - Guidelines on Risk Assessment Techniques*. SAI Global (SA/SNZ HB 89:2013). <http://infostore.saiglobal.com/store/Details.aspx?productID=1696535>.
- Strens, Ros, and John Dobson. 1993. "How Responsibility Modelling Leads to Security Requirements" *Proceedings on the 1992-1993 Workshop on New Security Paradigms, Little Compton, Rhode Island, United States*, doi: <http://dx.doi.org/10.1145/283751.283828>.
- Tatnall, Arthur. 2005. "Actor-Network Theory in Information Systems Research." In *Encyclopedia of Information Science and Technology*, 42-46. Hershey, PA: IGI Global.
- Ten, Chee-Wooi, Chen-Ching Liu, and M. Govindarasu. 2007. "Vulnerability Assessment of Cybersecurity for Scada Systems Using Attack Trees" *IEEE Power Engineering Society General Meeting, Tampa, FL*, doi: <http://dx.doi.org/10.1109/PES.2007.385876>.
- U.S. Department of Defense. 1985. *Trusted Computer System Evaluation Criteria*. U.S. Department of Defense <http://csrc.nist.gov/publications/history/dod85.pdf>.
- Vaishnavi, V., and W. Kuechler. 2004. Design Research in Information Systems. August 16, 2009 Accessed August 1, 2010, <http://desrist.org/design-research-in-information-systems>.
- Venable, John. 2006a. "A Framework for Design Science Research Activities" *Proceedings of the 2006 Information Resource Management Association Conference, Washington, DC*, Hershey, PA, USA: Idea Group Publishing. <http://www.irma-international.org/viewtitle/32739/>.
- . 2006b. "The Role of Theory and Theorising in Design Science Research" *Proceedings of the 1st International Conference on Design Science in Information Systems and Technology (DESIST 2006), Claremont, California*: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.110.2475&rep=rep1&type=pdf>.
- Venable, John, Jan Pries-Heje, and Richard Baskerville. 2012. "A Comprehensive Framework for Evaluation in Design Science Research." In *Design Science Research in Information Systems. Advances in Theory and Practice*, eds Ken Peffers, Marcus Rothenberger and Bill Kuechler, 423-438. Berlin, Germany: Springer
- Waber, Benjamin N., Sinan Aral, Daniel Olguin Olguin, Lynn Wu, Erik Brynjolfsson, and Alex Pentland. 2011. "Sociometric Badges: A New Tool for IS Research." In *Social Science Research Network*.
- Walls, Joseph G., George R. Widmeyer, and Omar A. El Sawy. 1992. "Building an Information System Design Theory for Vigilant EIS." *Information Systems Research* 3 (1): 36-59. <http://www.jstor.org/stable/23010780>.

- Walsham, G. 1997. "Actor-Network Theory and IS Research: Current Status and Future Prospects." In *Information Systems and Qualitative Research*, eds Allen S Lee, Jonathan Liebenau and Janicel DeGross, 466-480. Springer US.
- Walsham, Geoff, Veronica Symons, and Tim Waema. 1988. "Information Systems as Social Systems: Implications for Developing Countries." *Information Technology for Development* 3 (3): 189-204. doi: <http://dx.doi.org/10.1080/02681102.1988.9627126>.
- Walther, Olivier J, and Dimitris Christopoulos. 2012. "A Social Network Analysis of Islamic Terrorism and the Malian Rebellion." *CEPS/INSTEAD Working Papers* 38. doi: <http://dx.doi.org/10.2139/ssrn.2173139>
- Wang, Lingyu, Duminda Wijesekera, and Sushil Jajodia. 2004. "A Logic-Based Framework for Attribute Based Access Control." In *Proceedings of the 2004 ACM workshop on Formal methods in security engineering, Washington DC, USA*, 45-55. 1029140: ACM. doi: <http://dx.doi.org/10.1145/1029133.1029140>.
- Ward, Peter, and Clifton L. Smith. 2002. "The Development of Access Control Policies for Information Technology Systems." *Computers & Security* 21 (4): 356-371. doi: [http://dx.doi.org/10.1016/S0167-4048\(02\)00414-5](http://dx.doi.org/10.1016/S0167-4048(02)00414-5).
- Wasserman, S, and K Faust. 1994. *Social Network Analysis: Methods and Applications, Structural Analysis in Social Sciences*. Cambridge: Cambridge University Press.
- Watts, Duncan J., and Steven H. Strogatz. 1998. "Collective Dynamics of Small-World Networks." *Nature* 393 (6684): 440-442. <http://dx.doi.org/10.1038/30918>.
- Weber, P., G. Medina-Oliva, C. Simon, and B. Lung. 2012. "Overview on Bayesian Networks Applications for Dependability, Risk Analysis and Maintenance Areas." *Engineering Applications of Artificial Intelligence* 25 (4): 671-682. doi: <http://dx.doi.org/10.1016/j.engappai.2010.06.002>.
- Werlinger, R., K. Hawkey, and K. Beznosov. 2009. "An Integrated View of Human, Organizational, and Technological Challenges of IT Security Management." *Information Management & Computer Security* 17 (1): 4-19. doi: <http://dx.doi.org/10.1108/09685220910944722>.
- Willis, David A. 2014. *Bring Your Own Device: The Results and the Future*. G00264028. Gartner Research. <https://www.gartner.com/doc/2730217/bring-device-results-future>.
- Wiseman, Jacqueline P. 1986. "Friendship: Bonds and Binds in a Voluntary Relationship." *Journal of Social and Personal Relationships* 3 (2): 191-211. doi: <http://dx.doi.org/10.1177/0265407586032005>.
- Yin, Robert. 2002. *Case Study Research : Design and Methods*. Edited by Leonard Bickman and Debra G. Rog, *Applied Social Research Methods Series*. Thousand Oaks, CA, USA: SAGE Publications.
- Yuan, E., and J. Tong. 2005. "Attributed Based Access Control (ABAC) for Web Services" *Proceedings of the 2005 IEEE International Conference on Web Services (ICWS 2005), Orlando, FL, USA*, doi: <http://dx.doi.org/10.1109/ICWS.2005.25>.

*Every reasonable effort has been made to acknowledge the owners of copyright material. I would be pleased to hear from any copyright owner who has been omitted or incorrectly acknowledged*



**Question 3:** Given the following staff roster of your department, from whom do you seek advice or help for work related matters? (Please indicate the regularity with a tick – x)

Staff Member/Role	I consider this person as my primary advisor/mentor	I regularly (weekly or more frequently) seek this persons advise/help	I occasionally (monthly) seek this persons advise/help	I have never sought this persons advise/help
A/Role 1				
B/Role2				
....				
n/Role n				

**Question 4:** Given the following staff roster of your department, to whom do you give advice or help for work related matters? (Please indicate the regularity with a tick – x)

Staff Member/Role	I am the principle advisor or mentor of this person	I regularly (weekly or more frequently) give this person advice/help	I occasionally (monthly) give this person advice/help	I have never given advice or helped this person
A/Role 1				
B/Role2				
....				
n/Role n				

**Question 5:** Given the following staff roster of your department, rate your friendship with the staff members?

Staff Member/Role	I dislike this person	I am neutral toward this person	I like this person	This person is one of my better friends	This person is one of my closest friends
A/Role 1					
B/Role2					
....					
n/Role n					

**Question 6:** Given the following list what are the primary tasks you perform?

Task	Related information system module	I perform this task	I supervise or approve this task
Task 1			
Task 2			
.....			
Task n			

**Question 7:** Please name any of your relatives working in this organisation, their designation and the department?

**Question 8** Please name the external entities you interact with in order to perform the tasks assigned to you by the organisation?

**Question 9:** What are your core competencies or areas of expertise?

**Question 10:** Mention any project related or informal teams you belong to?

**Part 2: Additional Questions for Long Interview Sessions (Only applicable for primary information resource owners, managers and custodians):**

**Question 11:** Are you an owner of any information resource (hardware, software, data stores, documents etc.) or manager of your company?

- a) If yes, what are the information resources you own?
- b) Do they depend on any other information systems? Do other Information systems depend on them?
- c) What tasks require these information resources?
- d) What type of knowledge is required to operate these resources?
- e) What are the primary functions (tasks) of the information resources? What is the criticality of each task supervised by you?
- f) What dependencies are there for tasks you manage?
- g) Who are the custodians of information resources you own?

- h) Who has access to these information resources? At what level (Read, write, execute, administer)? (Note: this information can be obtained through a directory service or identity and access management system report)
- i) Which organisational policies and procedures govern their usage?
- j) Do business partners or customers get access to information resources you own? What level of access do they get?
- k) What are the criteria you used in granting access to the information resources you own?
- l) Have you classified the information resources you own or tasks you control? If yes, what classification levels are associated with them?
- m) Have you experienced any information security incident related to information resources you own? Do you know of any disgruntlement or concerning behaviour among other staff members? Please provide details.

**Question 12:** Are you an information custodian (administrator) of your company?

- a) If yes, what are the information resources you administer?
- b) Do they depend on any other information systems? Do other Information systems depend on them?
- c) What are the functions of the information resources?
- d) Who has access to these information resources? At what level (Read, write, execute, administer)? (Note: this information can be obtained through a directory service or identity and access management system report)
- e) Who is the owner of the information resources you own?
- f) Which organisational policies and procedures govern their usage?
- g) Do business partners or customers get access to information resources you administer? What level of access do they get?

- h) What are the criteria you used in granting access to the information resources you own?
- i) Have you classified the information resources you administer? If yes, what classification levels are associated with them?
- j) Have you experienced any information security incident related to information resources you administer? Do you know of any disgruntlement or concerning behaviour among other staff members? Please provide details.

## Appendix B

### Questionnaire Administered at the End of the Evaluation Workshops

#### Section I – The Model

1. In your opinion, how well does the network model represent important socio-technical access interactions in your organisation?

- Provides a very good representation     Provides a good representation     Provides an average representation     Provides a poor representation     Provides a very poor representation

2. How long did it take/will it take for you to collect the data required to populate the model using the resources available to you in your organisation?

- More than two weeks     Between one to two weeks     Between 3 days one week     Between 1-3 days     One day or less

3. How difficult was it for you to instantiate the model using the collected data and software tools utilised during the workshop?

- Very easy     Easy     Average     Difficult     Very difficult

4. Do you have any suggestions to improve the network model presented in the workshop?

**Section II – The Metrics**

1. In your opinion, do the metrics used in the analysis produce meaningful results that are applicable in your organisational context for quantifying access risks?  
 Highly applicable       Applicable       Not sure       Applicability is very limited       Not applicable at all
2. In your opinion, how accurately do the metrics rank socio-technical access risks in your organisation?  
 Very good accuracy       Good accuracy       Moderate accuracy       Accuracy is poor       Accuracy is very poor
3. Does the repeated analysis using the same input data produce the same metric values?  
 All the time       Most of the time       Sometimes       On few occasions       Never
4. Do you have any suggestions to improve the metrics used during the workshop?

**Section III – The Risk Assessment Method**

1. Did you find the analysis method presented in this workshop easy to follow/carry out using the software tools provided?  
 Very easy       Easy       Average       Difficult       Very difficult
2. In your opinion, would the development of a customised analysis tool improve the analysis capabilities?  
 There will be a huge improvement       There will be an improvement       Not Sure       There will be only minor improvements       There will be no improvement
3. Do you have any suggestions to improve the analysis method presented in this workshop?

**Section IV – Results Produced**

1. Do you think the results produced in the analysis are helpful in the assessment of socio-technical access risks in your organisation?

- Very helpful    Helpful    Somewhat helpful    Not helpful    Makes the situation worse

2. Will the results improve the overall access risk awareness of your organisation?

- Greatly improve    Improve    Somewhat improve    No improvement    Makes the situation worse

3. How effectively do the results produced by the metrics combined with the visualisations communicate the risks to the decision makers?

- Very effective    Effective    Somewhat effective    Very limited effectiveness    Not effective at all

**Section V – Evaluator’s Background**

1. To which industry sector does your organisation belong?

- Government    ICT Services    Finance    Manufacturing    Education    Other  
Please specify  
.....

2. How many employees are there in your organisation?

- More than 300    Between 100-300    Between 50-100    Between 50-25    Less than 25

3. What is your job role in terms of information systems security in your organisation?

- Manager/ Decision Maker    Information owner/Dept. Manager    IT/Security Administrator    Consultant    End user    Other  
Please specify  
.....

**Section – VI - Other Comments or Suggestions**

1. Do you have any other comments or suggestions regarding the model, method or metrics presented in this workshop?