Proceedings of the South African Information Security Multi-Conference (SAISMC 2010)

A Course Applying Network Analysis to Organizational Risk in Information Security

H. Armstrong, C. Armstrong and I. McCulloh

School of IS, Curtin University, Western Australia
e-mail: h.armstrong@curtin.edu.au; colin.armstrong@cbs.curtin.edu.au; ian.mcculloh@usma.edu

Abstract

Network science has been applied in the hard and soft sciences for several decades. Founded in graph theory, network science is now an expansive approach to the analyses of complex networks of many types of objects (events, people, locations, etc.). Researchers are finding that techniques and tools used in social network analysis have relevant application in projects that span more than just relationships between people. This paper discusses the application of network analysis in a postgraduate course on information security and risks in organisational settings as a special topic course.

Keywords

Information security education, network analysis, organization risk.

1. Introduction

Anything that can be illustrated as nodes and links can be analysed as a network. Network analysis has been carried out in numerous disciplines for many years, originating in the social sciences as social network analysis and the hard sciences as graph theory. Network analysis is sufficiently flexible to be applied to the field of information security in both social and technical areas, and has been the focus of research and practise since the 1980s. It gives the Information Security manager an additional tool for informed decision-making. For example Krebs (2000) used Social Network Analysis to analyse the design of network architectures, with the view to identifying ways to reduce hop counts, available paths and network failures. Lin and Zhang (2007) used SNA methods to analyse knowledge management, proposing an algorithm to identify bottlenecks and obstacles and minimise transfer costs and time. Network analysis tools have been used effectively in the analysis of terrorist networks and have an increasing application in crime (McCulloh 2009, McCulloh & Carley 2009). The concept of 'dark', 'grey' and 'white' networks has been offered by Bergin (2009) in relation to terrorist and crime networks. Of interest when analyzing terrorist groups is the underlying beliefs promoted by members. Modelling a network of persons where the link between nodes is a belief relationship enables members beyond the dark network to be identified. Terrorist networks, as with organised crime networks, contain memberships beyond those directly engaged in illegal activities. These networks exist within other, larger, networks. Bergin (2009) explains dark networks possess characteristics of covertness and illegality or associations causing a threat to society. Those people unknowingly providing

material assistance to terrorist groups may be considered a members of white networks, while those with closer affiliations to the darker criminal core, such as providers of expert knowledge – lawyers, accountants, and the like; may be considered to be members of grey networks.

Government analysts seek to predict transnational crime activity but because they encounter too many variables it is difficult to make sense of the intelligence supplied data. Quiggin (2007) argues that as crime and terror groups function as networks, one gains insights into their invisible operations by applying network science techniques. The application of network science techniques to relatively simple cause and effect provides a surface modelling of inter related incidents. The role of security practitioners is to protect assets requiring them to determine risks and vulnerabilities. Underpinning every aspect of the decision making processes associated with the provision of security is understanding the evidence. The application of network science techniques to crime also may be directed to different focal points. The application of network science techniques may restrict the focus to within a crime scene or within an incident, even a series of related incidents, where attention is directed towards the relationships between evidence and aspects of the incident. On the other hand, techniques may be directed to a higher level of analysis for the purposes of understanding broadly collected intelligence better. Armstrong (2009) discusses an approach for modelling evidence to afford an inquirer a better understanding of an incident using network science techniques. This approach looks to the relationships between items of evidence rather than focus solely on the evidence items. Network science techniques, supported by sound mathematical foundations, provides visualisation of the evidence networks showing the interconnecting relationships between evidence thereby facilitating better understanding of both evidence and relationships in crime incidents. Armstrong (2009) applies network science techniques to mapping four evidence attributes; incident location, actor, and offence against six relationship attributes; what, when, where, who, why, and how quickly shows the twenty four interconnecting relationships of a single evidence item.

This paper describes the presentation of a special topic postgraduate course at the master level dealing with the application of network analyses to social issues of information security and organisational risk, specifically utilising tools and techniques previously used in social network analysis. It describes the content of the course, the assessments and presents the feedback from the students.

2. Risk using Network Analysis

The organization can be viewed as a series of interconnected networks. A network comprises nodes and links with the nodes representing the people, knowledge, tasks and resources, and the links are the relationships between them (see Figure 1). By analysing the networks it is possible to identify areas of potential risk. The investigation comprises the application of statistical analyses to the network to identify key nodes, relationships and paths across the network. Centrality measures are used as the foundation for this analysis.

2.1. Course Overview

The learning outcomes for the course were to (a) analyse networks with relation to social factors, knowledge, skills and resources; (b) employ an automated tool to investigate and visualize networks, and (c) model a real world organisation as a network and make insightful recommendations to reduce risk within the organisation.

The course was run in an intensive mode with classes scheduled over 3 weekends rather than the usual weekly lecture and tutorial sessions. Many masters students are employed full-time and prefer to attend classes on the weekends. Lectures were used to present the theory and a laboratory installed with ORA (Organizational Risk Analyzer) software was used for the practical application exercises. The lectures were assigned approximately 35% and laboratory exercises 65% of the scheduled class time. Students were encouraged to complete additional reading and analyses in their own time. Assessments comprised an individual assignment carrying 20% of the final mark, a major group assignment carrying 40% and a final written examination also carrying 40%. The minor assignment was the analyses of a small network of dolphins (Lusseau et al, 2003) to ensure the students became familiar with the concepts of network analyses and the use of the analysis, charting and visualization tools provided in the ORA software. The students were provided with the User's Guide and a set of tutorials to familiarize them with the software. The major assignment required the analysis and reporting on risks within an organizational network, where the basic details on the people, tasks, knowledge and resources were provided. Students were required to identify relevant analyses to carry out, perform the analyses, and write a report to management summarising their findings and giving recommendations.

2.2. Lecture topics and a brief overview of content.

The lectures covered the theory and explanations of the statistical analyses performed on the different types of nodes and relationships. The curriculum fell into four main areas: network concepts, network measures, analyses of networks and indicators of organizational risk.

Network Concepts: types of networks including small world, random, cellular, core-periphery networks; network data types and data collection for research; network graphs and matrices; nodes and links; geodesics and pathways through the network; informal and formal network structures.

Network Measures: measures of centrality including degree – a node's exposure to the network and its opportunity to directly influence the network; closeness – an estimate of the time to hear information; betweenness – the ability to act as a broker or gatekeeper and control the flow of information between groups; and eigenvector – being connected to other well-connected nodes. The students calculated these manually then again using the automated tools. Figure 1 also illustrates the centrality measures in a visualization of a simple network of individuals (Krackhardt, 2008).

Analyses of Networks: analyzing organizations as networks, identifying key individuals, resources, knowledge and resources, analysis of subgroups and cliques, influence within the network and diffusion across the network. Figure 2 illustrates a series of networks (sub-networks) for a fictitious organization with nodes and relationships for people, resources, knowledge and tasks. Although each sub-network can be a stand-alone network, there are links between the different types of nodes, i.e. knowledge held by people, tasks assigned to people, resources required for tasks, etc.

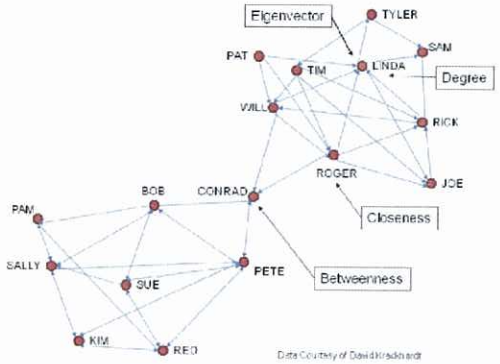

Figure 1: The organization as a network of individuals illustrating degree, closeness, betweenness, and eigenvector.

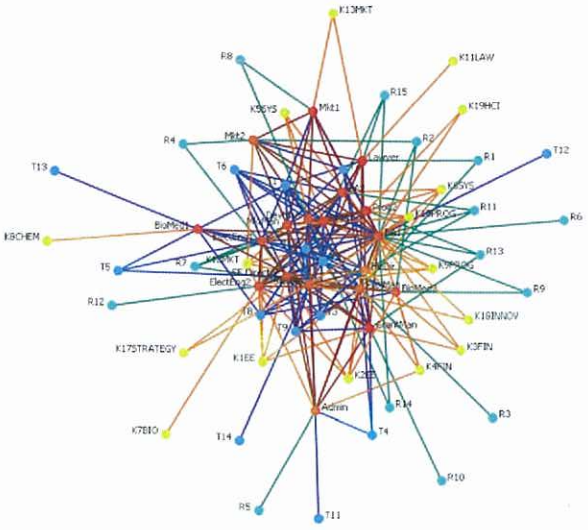

Figure 2: A combined network for the organization linking the people, resources, knowledge and tasks.

Risk Indicators: Risk indicators are based upon the basic centrality measures plus additional algorithms. Potential risks are analysed as Emergent Leaders who need to be connected to many people, resources, and tasks; Exclusivity illustrating specialization of individuals, knowledge and resources; Situational awareness and Clueless individuals; Isolated individuals, resources, knowledge and tasks; Density to reflect transfer of knowledge; Hubs - individuals who have out-links to other individuals that have many in-links; Authorities - individuals who receive information from a wide range of others, each of whom sends information to a large number of others (Carley et. al 2009); Complexity and knowledge breadth.

3. Application of Tools in Main Assignment

The major assignment required the students to analyse a formal and informal organisational network and investigate areas of potential risk. The simulated organization was named LaserTech and was based upon data collected from interviews, emails and documentation from an actual organization and anonymized. The formal network illustrated the official reporting hierarchy and the informal network plotted the informal relationships between the individuals. The formal and informal networks are illustrated in Figures 3 and 4 respectively.

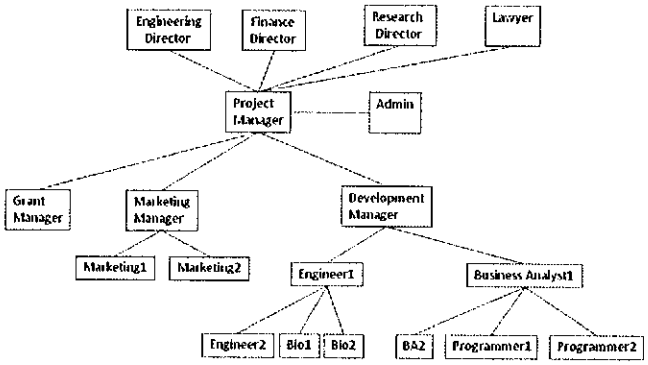

Figure 3: The formal organization chart illustrating the hierarchical people network for the LaserTech organization.

Several people in non-executive positions are key to this informal network because they belong to specific social groups and sports organisations outside the company (church, golf club, gym, Freemasons, etc.), or have relationships via other means (close proximity, marriage, etc). This means the formal network is not directly reflected by the informal network. Much of the work in a day is achieved via the informal network rather than the formal organizational structure. For example, note the positions of BA1 (Business Analyst 1) in the two diagrams. Although several levels lower in the formal structure this individuals holds a central position in the informal network, being better connected than the Project Manager, who should be central to the communications structure. The informal groupings and links also open up risks not inherent in the formal structure.

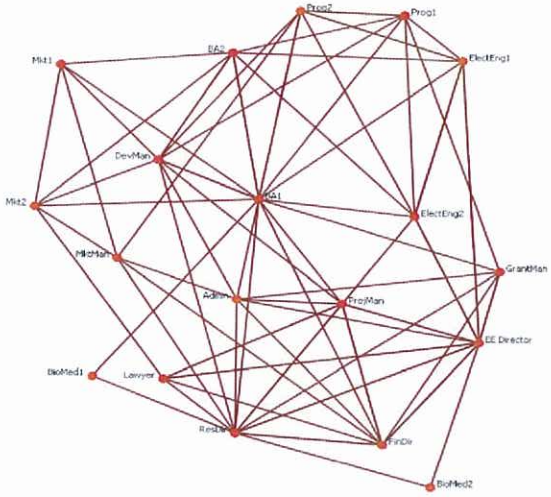

Figure 4: The informal people network for the LaserTech organization.

Figure 5 illustrates the sub-network of agent x knowledge, detailing the areas of key knowledge held my particular individuals. Figure 6 shows the agent x task sub-network showing which individuals are assigned to given key tasks and Figure 7 displays the agent x resource sub-network indicating which individuals control key resources. However, missing from the documentation distributed were two additional sub-networks that were needed to gain a comprehensive view of the situation. The students were expected to identify this missing information and request it.

Figure 5 shows there are several areas of key knowledge held only by one or two individuals, for example K7BIO, K8CHEM, K11LAW and K13MKT; illustrating a high level of knowledge specialisation or exclusivity. Of concern are those knowledge areas isolated from the main network where alternate sources of this knowledge need be made available in the event of non-availability of the individual holding that knowledge. Again, note how central BA1 is to the network of knowledge, with knowledge in numerous areas. This could indicate that this individual is spread too thinly. Several tasks in the sub-network illustrated in Figure 6 have been assigned to only one individual, for example T11, T12, T13 and T14. Although these tasks may be small in size, the analyst must identify how critical these tasks are to the success of the projects that rely on those tasks. Other tasks are much larger in size, for example, T1, T2 and T10, involving many individuals, requiring careful planning and management.

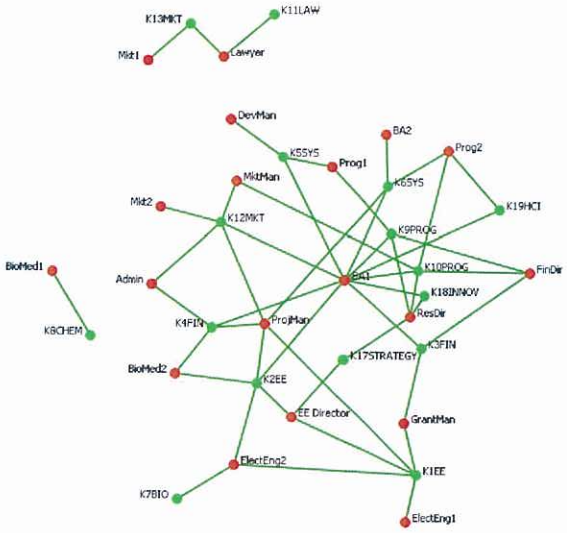

Figure 5: The LaserTech agent x knowledge sub-network. Agents are red nodes and knowledge areas are green nodes.

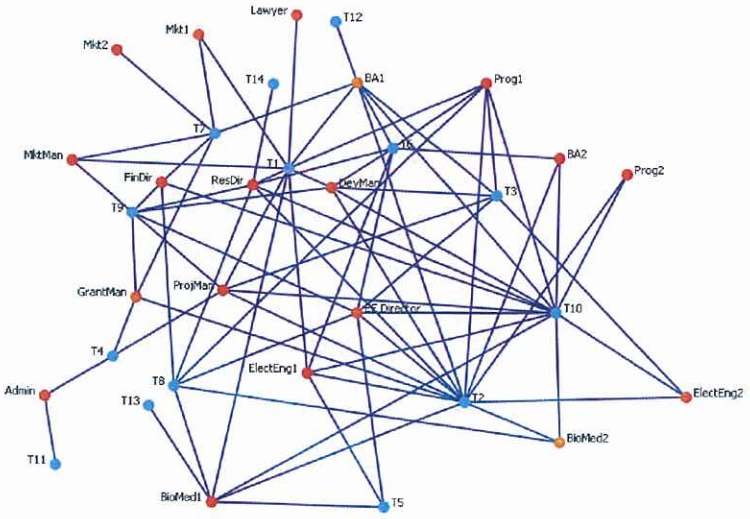

Figure 6: The LaserTech agent x task sub-network. Agents are red nodes and tasks are blue nodes.

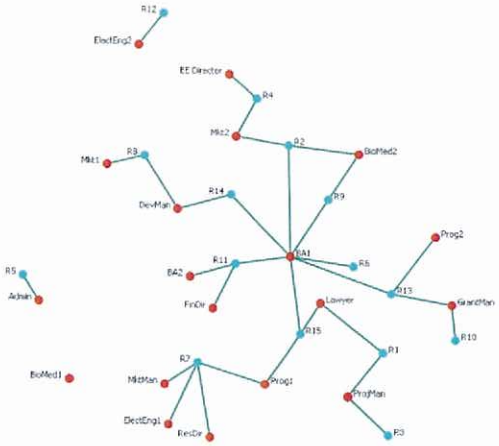

Figure 7: The LaserTech agent x resource sub-network

Resources are key requirements for organizational activities and those who control the resources have power. In Figure 7 BA1 controls seven key resources and would certainly be in demand by those who need those resources. Many resources are controlled by more than one person and this reduces resource exclusivity, spreading the risk. Note the isolates in this sub-network – BioMed1 controls no resources, Admin controls only R5, and ElectEng2 controls only R12. R6 is only controlled by BA1. What needs to be ascertained is how critical are R5, R6 and R12 and who needs these resources to carry out tasks?

In the major assignment the students were required to:

- Analyse the LaserTech organisational network and explain the measures used in the network analyses.
- Explain the risks LaserTech faces and explain the measures used to analyse risks, then describe why they are a potential risk.
- Recommendations for improvement and reduction of risk.

Working in groups of 3-4 the students undertook background reading and used ORA to analyse and visualize their networks. As the students were studying at master level they were expected to use the management reporting facilities provided by ORA to identify potential risks and explain these in their reports. Some groups expected to be given detailed guidance and a step-by-step procedure provided by the academic staff. Others took on the challenge and embraced learning by discovery, delving into publications to find other organizational studies using similar techniques. Three academics were available to answer queries and guide the students' progress, however only 3 of the 20 students sought clarification throughout the exercise.

Although the majority of the students were able to carry out the essential analyses, none of them requested additional information, or sought out criticality details of tasks and resources. Two additional sub-networks were needed in order to obtain a

bigger picture, the task x resource and task x knowledge sub-networks. These would have provided the students with the information regarding the resources required to carry out given tasks as well as the knowledge associated with tasks. Without this information the students only had a blinkered view of the organizational situation. Although students were encouraged to ask questions to gather more information, none requested information regarding these links.

4. Reflections and Conclusion

Feedback and evaluation by the students was positive, with some comments being noted for improvement for the next offering of the course. The standard university course feedback instrument returned high ratings for all the educational criteria. Of more interest to the authors were the free-form comments from the students which will guide enhancements to the course next time it is offered. Remarks on the most helpful aspects of the course included:

- Unit lecturers and contributors are very knowledgeable and approachable. They seem happy to answer any questions I have and are eager to spend extra time helping me learn.
- A very interesting unit. I learned from another view to look at the risk in organizations and how to analyze them.
- The most important point is the lecturer explained the terms in a way that was very easy for me to understand.
- I like to use math to solve the problems. This gave me a deeper understanding about applying math to organizational networks. An excellent Unit.
- The unit opened up a new area of interest to me to conduct my theses on. Experiences shared by the lecturer were extremely valuable.
- Brilliant content, and great lecturers.

Comments regarding ways the unit could be improved included:

More exercises could help make me understand the concepts better.

- A few more handouts would have been good, and perhaps try not to have it on two consecutive weekends, or hold it a bit earlier maybe in the semester. Overall it was fantastic thanks.
- Some of the content presented appears superfluous to what is required as part of the unit outcomes or what may be assessed. This results in uneasy feelings on how much study individual topics require.
- As with other units, better collaboration tools would help group communication, especially to provide remote communication for group members who are unable to meet in person.
- At the time when the first assignment was done we were quite clueless about the software and its usage.

Although students were required to work through an introductory session on network analysis and the ORA software in preparation for the first class it was interesting to

discover that very few students attempted the tutorials or consulted the Users' Guide prior to the first assessment activity. This raises a frequently asked question – How much do we need to spoon feed postgraduate students in information security courses? When the course is offered again greater emphasis will be placed on informing students of resources they will find helpful and managing the students' expectations regarding the amount of initiative expected. Many have yet to realize that the quality of their learning experience relates not to obtaining the one right answer from the lecturer, but directly to the amount of time and effort they are willing to invest.

Nevertheless, the positive evaluation ratings and the comments provided by the feedback instrument and also comments made directly in conversation with the lecturers indicates that overall the course was a success and reinforced that network analysis is an appropriate tool and useful for informed decision making on human-related risk issues in organizations.

5. References

Armstrong, C. J. (2009). "Forensic Evidence Networks". Illicit Networks Workshop, Centre for Translational Crime Prevention, University of Wollongong, Australia.

Bergin, S. (2009). "The Application of Social Network Analysis in the Defence, Security and Law Enforcement Intelligence Domains: A review of progress and prospects up to 2008". INSNA Sunbelt Social Networks Conference, San Diego.

Carley, K, Reminga, J., Storrick, J. & De Reno, M. (2009) "ORA User's Guide 2009", Institute for Software Research, Carnegie Mellon University, Pittsburgh, PA, CASOS Technical Report CMU-ISR-09-115

Krackhardt, D. (2008) "Power and Influence", lecture at the 2008 Center for Computational Analysis of Social and Organizational Systems (CASOS) Summer Institute, 23-29 June 2008, Carnegie Mellon University, Pittsburgh, PA.

Krebs, V., (2000) "The Social Life of Routers: Applying knowledge of human networks to the design of computer networks", The Internet Protocol Journal, Vol. 3, No. 4, pp 14-25

Lin, X. & Zang, Q. (2007). "Optimization of Knowledge Sharing & Transfer Network" in Wireless Communications, Networking and Mobile Computing, WiCom 2007, pp.5613-5616

Lusseau, D., Schneider, K., Boisseau, O.J., Haase, P., Slooten, E. and Dawson, S.M. (2003) "The bottlenose dolphin community of Doubtful Sound features a large proportion of long-lasting associations", Behavioral Ecology and Sociobiology Vol. 54, pp 396-405.

McCulloh, I. (2009), "Detecting Changes in a Dynamic Social Network". Carnegie Mellon University, School of Computer Science, Institute for Software Research, Computation, Organizations and Society, Doctor of Philosophy, Available http://www.casos.cs.cmu.edu/publications/papers/CMU-ISR-09-104.pdf

McCulloh, I. & Carley, K. (2009), "Longitudinal Dynamic Network Analysis: Using the Over Time Viewer Feature in ORA". Carnegie Mellon University, School of Computer Science, Institute for Software Research, Technical Report CMU-ISR-09-118.

Quiggin, T. (2007). Seeing the Invisible: National Security Intelligence in an Uncertain Age. Singapore, World Scientific Publishing Co.