A STUDY OF INSIDER THREAT BEHAVIOUR: DEVELOPING A HOLISTIC FRAMEWORK

Asmaa M. Munshi
Curtin University - GPO Box U1987, Perth WA, Australia

ABSTRACT

This research aims to develop a holistic view of insider threat behaviour and ways to manage it. This research will be conducted by data collection in three phases: academic research sources published legal cases, and management and business sources. The study results will develop insider threat behaviour model. This model will be assessed by focus group prior to building the framework. Later, a management framework will be developed to manage insider threat behaviour. Finally, to ensure the practicality of the new framework a focus group will assess the management framework.

KEYWORDS

Insider threat, holistic view, insider threat behaviour, conceptual model, management framework, designs science methodology.

1. INTRODUCTION

Any security system will have to rely on the operators even if it is designed and implemented in a perfect manner. Nowadays, organisations face ongoing threats from external and internal attacks. Insider attacks, which have been recognised as a potential security problem since the 1980s (Chinchani et al. 2005), are associated with legitimate users who abuse their privileges and can easily cause significant damage or loss to an organisation. Most of the research reported on the insider threat cover the problem from the researcher's perspective to match his/her situation which focuses on one primary problem as either a technical or human issue. The models used in such research may be suitable for their particular case but not for other cases covering different aspects. Moreover, most of the models focus largely on technical issues without considering cultural and social aspects. A recent study however, indicated that successful protection against insider threats relies on both technical and behavioural solutions (Martinez-Moyano et al., 2008a).

2. OBJECTIVE

The overall aim of this research is to develop a conceptual insider threat model of the problem space that can frame a holistic view of insider threat behaviour and inform the building of a framework to manage the insider threat. Previous research in this area focused on quite narrow and specific areas and most of the models and frameworks developed so far specialise in either people to people relationships, segmentation of tasks, access to information or network architectures. Little research published so far gives a bigger picture in regard to insider threat behaviour. Therefore, the main aim of this research is to gain a holistic view of the insider threat through understanding the factors that influence insider threat behaviour, both by individuals and organisations, and then develop a framework which centres on security measures to manage insider threat behaviour.

3. BACKGROUND

The insider threat is one of the most serious problems affecting security systems and one that is difficult to overcome (Bishop et al., 2008). The threat is associated with legitimate users who abuse their privileges and can easily cause significant damage or loss to an organisation (Martinez-Moyano et al., 2008b). Trusted employees have the most potentiality to harm the organisation by damaging the information or stability of the operation system (Ho, 2008). However, all employees can pose a potential insider threat in some form.

According to Hayden (1999), some computer investigators have classified the insiders into four categories namely: traitors, who have a malicious intention to harm or destroy their organisation; zealots, who believe that the organisation is being badly run; browsers, who are curious to know everything even if it causes damage to the organisation; and the well intentioned, who are characterized by a lack of concern and who damage the organisation through downloading untrustworthy documents and/or by not activating their virus protection software.

Regardless of which category insiders belong to, they have a significant advantage over externals in the harm they can cause an organisation. Insiders can avoid physical (electronic building access systems) and technical (firewalls, intrusion detection systems) security measures designed to prevent attacks (Besnard and Arief, 2004). Moreover, insiders are aware of the weak points of their organisation's policies and procedures and of the technology it uses (Cappelli et al., 2009). Schultz (2002) confirms that it is difficult to predict or prevent insider attacks because the offenders are authorized employees.

Although insider attacks may occur less frequently than external ones, insiders have a high impact on information since they are familiar with their targets and security countermeasures in place (Chinchani et al., 2005). A survey of insider incidents conducted of banking and financial institutions showed that 30% of incidents had resulted in losses in excess of $500,000 for each (Randazzo et al., 2004). Gonzalez and Sawicka (2002) found that human factors contributed to 80 – 90% of organisational accidents. CERT, a centre of Internet security expertise, reports that 22,716 vulnerabilities (from 1995-2005) and 319,992 incidents (from 1988-2003) were caused by insiders who had legitimate access to the system (Martinez-Moyano et al., 2006). Accordingly, reviewing the previous problems faced by different organisations - any good model can be considered significant.

3.1 Defining the Insider Threat

The problem of insider threats has been investigated by many researchers, and most of these do not give a comprehensive definition of an insider. For example, a RAND Corp. report defines an insider as *"an already trusted person with access to sensitive information and information systems"* (Brackney and Anderson, 2004, p. xi), while on another position it defines the insider as *"someone with access, privilege, or knowledge of information systems and services"(Brackney and Anderson, 2004, p. 10)* ignoring the 'trusted person' in the first definition. Garnkel, Gopal, and Goes (2002, p. 3) define the insider threat as *"a subject of the database [who] thereby has personal knowledge of information in the confidential field"*. Other definitions simply include anyone operating inside the security perimeter (Patzakis, 2003), ignoring factors such as trust and knowledge of the systems. Such different definitions exclude insiders who are not trusted, which results in a binary distinction whereby a person is either an insider or not an insider.

According to Bishop et al. (2008) handling the insiders rather than defining the problem is another complication in understanding the concept of insider threats. This point has been addressed by many researches which do not provide a sufficient description of the problem's nature. Chinchani et al. (cited in Bishop et al., 2008, p. 9) define insiders as *"legitimate users who abuse their privileges, and given their familiarity and proximity to the computational environment, can easily cause significant damage or losses"*. Althebyan and Panda (2007, p. 240) define the insider as an *"individual who has the knowledge of the organisation's information system structure to which he/she has authorized access and who knows the underlying network topologies of the organisation's information systems.* These definitions characterises the insider as an entity which includes not only people but also systems and code, which is very important as no other definitions have addressed these elements as insiders. Most researchers have defined the insider as a person - without any consideration for the other types. However, this definition still focuses on technical issues.

Determining a definition is important for researchers in being able to find a better way and method to minimize the insider threat problem. Without a comprehensive definition of the insider threat, each researcher defines it according to their own assumptions and perspective, which may lead to complexities when using their model for other applications. Therefore, developing a comprehensive definition of the insider threat will allow flexible movement and translation between several domains under one model and thus assist in reducing the insider threat problem. This research will define the insider threat as the potential harm posed by any trusted entity with inside access to the organisation. Each trusted entity will have a different level of trust assigned appropriate to their position and role. Each trusted person will be influenced by different factors, thus resulting in different behaviour.

Insider behaviour refers to human attempts to obtain a self satisfaction. According to Calandrino, McKinney, and Sheldon (2007, p. 1) *"Undesirable insider behaviour involves any wilful or negligent misuse of resources in an organisation's information systems".*

This research will emphasize insider threat behaviour not only arising from within a person, but also controlled and guided by organisational policies, procedures, security restrictions, as well as external factors such as laws.

3.2 Insider Threat Models

Several models have recently been presented to detect and prevent insider threat and most of these have focused on technical issues; however, very few have discussed the social, cultural and demographic factors. Selections of models that are representative of the research space are set out below:

Gonzalez and Sawicka (2002) developed a systems dynamic simulation model to discover complex security problems; their research project is to understand the role of human factors in information security systems. They used a simple case to demonstrate how system dynamics may provide insight into the people security problem and help in designing robust security policies. The model focused on human factors and does not address other insider threat issues such as the technological and organisational environments.

Moreover, Hu, Bradford and Liu (2006) developed a model for detection of insider attacks by intrusion detection systems based on the assumption that an insider is described by job function. However, the influence of social insider factors was not considered in this model.

The final model considered here, by Moore, Cappelli, and Trzeciak (2008) presented a system dynamics model of the insider IT sabotage problem, where the insider's main aim is to harm some parts of the organisation such as business operations, information and the system or network. Their model too, mostly focused on one primary problem and they did not consider any other types of insider threat such as fraud or the stealing of sensitive information.

Most previous models mainly focus on one primary problem, either a technical or human issue. Moreover, current research in the insider threat is centred on advanced western economies in addition to being focussed on technical issues. Little can be found in the prominent academic computer security sources regarding social, cultural and demographic factors and their effects on the insider threat. These missing aspects constitute knowledge gaps. Providing specific models of the insider threat without making a holistic contribution adds to the obstacles to preventing insider threat. The scopes of prior studies have been limited to specialised areas, resulting in isolated findings, where many factors related to insider behaviour have been omitted, for example culture, background and educational factors.

This research will study the insider threat in an effective way by providing a comprehensive global perspective for insider behaviour. To develop a holistic insider threat model, the researcher needs to precisely study social, technical and organisational factors. This research will require investigating other disciplines such as criminology, sociology and possibly psychology to discover any research that could be applied to the insider threat.

4. PRELIMINARY MODEL OF THE INSIDER THREAT

The preliminary model addresses some of the factors that influence the insider threat behaviour to facilitate the development of the management framework.

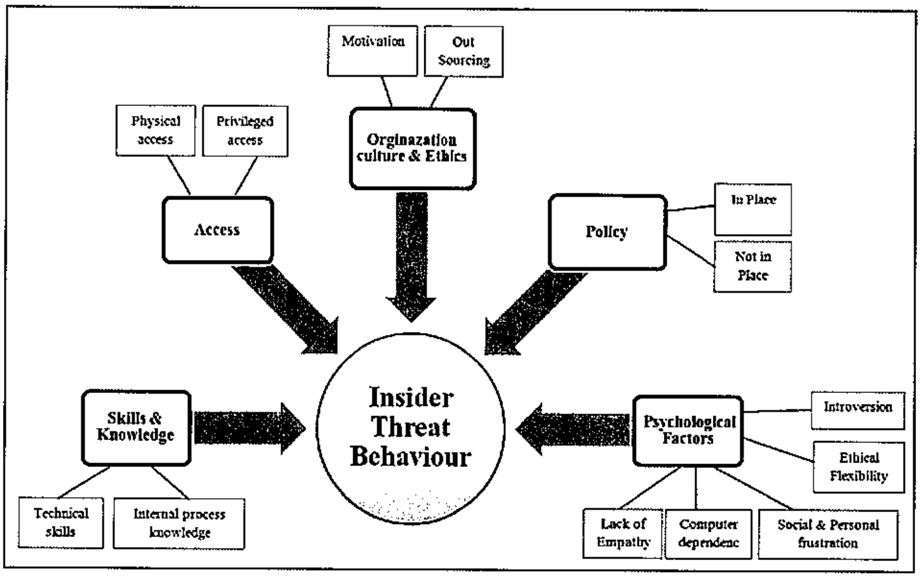

Figure 1. Preliminary model

Figure 1 shows the core areas of the insider threat problem. Each of these is described in the following list.

- **Access***:* The Insider has unrestricted physical and technical access to some parts of the system (Wood, 2000).
- **Privileged Access:** some employees, such as system programmers, have more access than they need, and therefore not only have the potential to compromise their organisation but also to introduce malicious code which may cause a denial of service. Insiders who have authorized root access such as system administrators can be dangerous to the organisation by their ability to change documents, data and access permission without detection (Hayden, 1999).
- **Physical Access:** insiders, for example computer operators and system administrators, have unrestricted physical access to facilities such as computer rooms and network centres which give them the opportunity to access sensitive and confidential areas. The easy access to such facilities can allow them to adjust, stop or steal machines with important and confidential data. The insiders may steal other employee access by performing social engineering techniques to gain physical access to some areas restricted to their entrance (Hayden, 1999).
- **Policy:** is a guide for making decisions and setting action parameters. Any organisation should know who has access to what data, what their access policies are, and what route they take to get into that data (Pramanik et al., 2004). Typically, a security policy determines what actions are authorized for a specific user and purpose. For example, a security policy may state that employee X is authorized to read Y records in order to update the data. If employee X deletes the records, he is violating the security policy. The security policy will also be violated if he reads the records for the purpose of selling the information. Moreover, the security policy is violated if anyone else uses employee X's user account to read the records. This example reveals that security policies may state rules that are difficult to put into action. Users may misuse their privileges because the computer systems do not recognize people - only user accounts (Bishop et al., 2008). Therefore, organisations require a detailed security policy that focuses on both external and internal threats.
- **Employee's Skills:** Employees may use their skills to harm an organisation's system: such as by downloading and using hacker tools, access to the system after termination, and the setup and use of backdoor accounts (Moore et al., 2008).
- **Employee's Knowledge:** Besides their free access to documents and data, insiders have wide knowledge of their organisation's system and procedure (Wood, 2000).
- **Psychological factors:** Based on an interview study, Shaw, Ruby, and Post (2005) concluded that there are several characteristics that, when found together, increase the possibility of insider misbehaviour.

These are: computer dependency, a history of personal and social frustrations, ethical lapses, a sense of entitlement, and lack of empathy.

A deeper investigation of these areas, and others that may be potential factors, is the first step in building a framework for managing the insider threat.

5. RESEARCH QUESTIONS

The research questions investigated by this project are as follows:

1- What factors influence the insider to behave inappropriate with regard to security?
2- How can organisations manage the security abusive behaviour of insiders?

6. RESEARCH METHOD

The Design Science methodology has been adopted in this research. According to Venable (2006), Design Science should yield a theoretical artefact such as a construct, model, method, or improved theory, and the artefact should be evaluated for the research to have rigour.

The current project will be conducted into two phases. In Phase One a conceptual model of the insider threat will be built. The conceptual model will be based upon the Preliminary Model above, and improved upon after an exhaustive analysis of academic literature, published legal cases of insider threat behaviour, and information from management/business sources. The data collection will cease when saturation is reached, that is, when new data only reflects areas which have already been discovered. The resultant model will encapsulate factors associated with the insider threat and the relationships between them, and will be reviewed and evaluated by two independent focus groups consisting of experts across social, technical and executive management roles, dealing with insider threat behavioural considerations. Feedback from the focus groups will be used to refine the model.

Phase Two will focus on developing a management framework to manage insider threat behaviour; thus, this phase involves technology invention/design. This phase will seek to manage and control the problem produced in Phase One via a management framework. The framework will develop a set of security measures to manage insider threat behaviour based upon the factors in the model. These security measures will be devolved by collecting best practices from previous research for each factor, adding missing practices and finally synthesizing these into an integrated coherent framework. Finally, to ensure the practicality of the new framework a focus group will assess the management framework.

7. CONCLUSION

The insider threat is a complex problem involving both human factors and computational elements; this threat is managed by a mixture of technical and behavioural strategies. This research has two important contributions: Theoretical contribution and practical contribution. Conceptual significance refers to the coverage of the literature, the contribution to knowledge in the field of study and future research opportunities within the field of study. This researcher will propose a new conceptual insider threat model for a holistic view of insider threat behaviour to present an insight into the insider threat - including people, tools, technology and environment. The significance of this model lies in its understanding of the insider threat problem space from a wider perspective instead of single view. This model of the problem space will lead to development of a design theory. Propose model will add to the knowledge base for further research and practice since it can be used by other researchers to test and improve the model in further studies. Moreover, this research will minimize the problem of the insider threat by providing a management framework to manage insider behaviour. The contributions of this research are applicable to business and user needs especially in security and IT departments. The proposed framework will contribute to avoiding and preventing insider threats and also provide user awareness. In addition, it will be useful in different organisations and for audiences who are aware of organisational security issues such as chief information officer (CIO). This framework will help the chief information officer to manage insider threat behaviour and increase the awareness of users.

REFERENCES

Althebyan, Q. & Panda, B. 2007. A knowledge-base model for insider threat prediction. *Proceedings of the 2007 IEEE Workshop on Information Assurance United States Military Academy, West Point*, 229-246.

Besnard, D. & Arief, B. 2004. Computer Security Impaired by Legitimate Users. *Computers & Security*, 23, 253-264.

Bishop, M., Engle, S., Peisert, S., Whalen, S. & Gates, C. 2008. We have met the enemy and he is us. *Proceedings of the 2008 workshop on new security paradigms* Lake Tahoe, California, USA.

Brackney, R. & Anderson, R. H. 2004. Understanding the insider threat. *March 2004 Workshop.* Santa Monica, CA, USA: RAND Corporation.

Calandrino, J. A., Mckinney, S. J. & Sheldon, F. T. 2007. Detection of Undesirable Insider Behavior. *Cyber Security and Information Intelligence Research Workshop (CSIIRW),.*

Cappelli, D., Moore, A., Trzeciak, R. & Shimeall, T. 2009. Common sense guide to prevention and detection of insider threats 3rd edition – version 3.1. Software Engineering Institute.

Chinchani, R., Iyer, A., Ngo, H. & Upadhyaya, S. 2005 Towards a theory of insider threat assessment. *IEEE International Conference.* Washington, DC: IEEE Computer Society

Garnkel, R., Gopal, R. & Goes, P. 2002. Privacy protection of binary confidential data against deterministic, stochastic, and insider threat. *Management Science*, 48, 749-764.

Gonzalez, J. & Sawicka, A. 2002. A framework for human factors in information security. *2002 WSEAS Int. Conf. on Information Security.* Rio de Janeiro, Brazil.

Hayden, M. 1999. The insider threat to U. S. government information systems. National Security Telecommunications And Information Systems Security Committee.

Ho, S. M. 2008. Behavorial parameters of trustworthiness for countering insider threats. *The Third Annual iConference.*

Hu, N., Bradford, P. G. & Liu, J. 2006. Applying role based access control and genetic algorithms to insider threat detection. *Proceedings of the 44th Annual ACM Southeast Regional Conference (ACM-SE).* New York, USA: ACM.

Martinez-Moyano, I., Rich, E., Conrad, S. & Andersen, D. 2006 Modeling the emergence of insider threat vulnerabilities. *Proceedings of the 2006 Winter Simulation Conference.* Monterey, California, USA.

Martinez-Moyano, I., Rich, E., Conrad, S., Andersen, D. & Stewart, T. 2008a. A behavioral theory of insider threat risks: a system dynamics approach. *ACM Transactions on Modeling and Computer Simulation*, 18, 1-27.

Martinez-Moyano, I., Samsa, M., Burke, J. & Akcam, B. 2008b. Toward a generic model of security in an organizational context: exploring insider threats to information infrastructure. *Proceedings of the 41st Hawaii International Conference on System Sciences.* Hawaii, USA: IEEE Xplore.

Moore, A., Cappelli, D. & Trzeciak, R. 2008. The "big picture" of insider IT sabotage across U.S. critical infrastructures. Pittsburgh: The Software Engineering Institute.

Patzakis, J. 2003. New incident response best practices: patch and proceed is no longer acceptable incident response. Pasadena: Guidance Software.

Pramanik, S., Sankaranarayanan, V. & Upadhyaya, S. 2004. Security policies to mitigate insider threat in the document control domain. *Proceedings of the 20th Annual Computer Security Applications Conference (ACSAC'04).* Washington, DC, USA: IEEE Computer Society

Randazzo, M., Keeney, M., Kowalski, E., Cappelli, D. & Moore, A. 2004. Insider threat study: Illicit cyber activity in the banking and finance sector. Software Engineering Institute.

Schultz, E. E. 2002. A framework for understanding and predicting insider attacks. *Computers & Security*, 21, 526-531.

Shaw, E., Ruby, K. G. & Post, J. M. 2005. The insider threat to information systems1. the psychology of the dangerous insider. Reprinted from Security Awareness Bulletin, No. 2-98.

Venable, J. 2006 The role of theory and theorising in design science research. *Proceedings of the First International Conference on Design Science Research in Information Systems and Technology in Alan Hevner and Samir Chatterjee.* Claremont, CA, USA.

Wood, B. J. 2000. An insider threat model for adversary simulation. Albuquerque: SRI International.