Proceedings of Informing Science & IT Education Conference (InSITE) 2014

Cite as: Ophoff, J., Jensen, A., Sanderson-Smith, J., Porter, M., & Johnston, K. (2014). A descriptive literature review and classification of insider threat research. *Proceedings of Informing Science & IT Education Conference (InSITE) 2014* (pp. 211-223). Retrieved from http://Proceedings.InformingScience.org/InSITE2014/InSITE14p211-223Ophoff0543.pdf

A Descriptive Literature Review and Classification of Insider Threat Research

Jacques Ophoff, Adrian Jensen, Jonno Sanderson-Smith, Michael Porter and Kevin Johnston
Department of Information Systems, University of Cape Town, Cape Town, South Africa

jacques.ophoff@uct.ac.za jnsadr006@myuct.ac.za
sndjon010@myuct.ac.za prtmic010@myuct.ac.za
kevin.johnston@uct.ac.za

Abstract

Insider threat is an information security problem. It specifically refers to the users of an information system exploiting their legitimate access rights to that system, in order to perform malicious acts. The purpose of this paper is to describe the body of knowledge of insider threat research through a descriptive literature review. The scope of the report is academic research articles. The objective of this study is to create a classification of insider threat research. This was achieved by gathering relevant journal articles and categorizing them. A classification was created, comprising five main categories: 'Insider Threat Mitigation', 'Theoretical Perspectives', 'Insider Threat Management', 'Insider Threat Overview' and 'Insider Threat Behavior'. The key findings are that the main volume of research is currently concentrated in the 'Theoretical Perspectives' and Insider 'Threat Mitigation' categories. Comparatively, there is very little research in any of the other categories, with 'Insider Threat Management' being particularly sparse. There is a clear opportunity for future research in the three under-researched areas, particularly in 'Insider Threat Management', where there are numerous frameworks and standards to use as research guidelines.

Keywords: Information security, insider threat, descriptive literature review, classification.

Introduction

Traditionally, information security has placed its focus on external threats, whilst largely ignoring the threats posed to an organization from internal members of staff (Hamin, 2000). The assumption has been that the risk and likelihood of a threat from within was low in comparison to external threats (Hong, Kim, & Cho, 2010). While outsider threats are more prevalent, insider threats are regarded as more costly and detrimental to organizations (CERT, 2010).

Insiders, according to Hamin (2000), are in an advantageous position to misuse organizational information systems, due

to their familiarity with system structures and potential weak spots in security administration. "The insider threat identifies a serious threat to computer security. It describes a breach of trust by people within an organization or system, as contrasted to external entities for whom firewalls and other mechanisms can deny access" (Bishop, Engle, Peisert, Whalen, & Gates, 2009, p.1). A security incident perpetrated by an insider can impact an organization in various ways. Potential results of insider threat incidents could be negative impact on the public image of an organization, negative impact on the revenue of an organization or litigation due to disclosure of confidential information (Colwill, 2009).

The review and classification of literature is to provide a comprehensive source of reference for further research and studies. Relevant literature reviews are essential to facilitate theory development and to identify over- and under-researched area's (Webster & Watson, 2002). The purpose of this study is descriptive. The research question being addressed is the following: What is the current state of Insider Threat research? In order to answer this question, valid articles on the topic of insider threat were collected, divided into categories which were then used to create a classification. The objective of this study is to descriptively review and classify existing literature.

Following the introduction the background critically examines current literature on the topic of insider threat. This is followed by a description of the research methodology, which outlines the approach adopted in this study. Next the classification is presented, including analysis and detailed discussion of the findings. Finally the conclusion presents a summary of the research and directions for future study.

Background

Numerous security surveys point to a considerable insider threat related to employee computer crime (Willison & Siponen, 2009). The following section will define the term insider threat, as well as the concept of the insider. Focus will be placed on the different perspectives in the literature with regards to what constitutes an insider threat.

Definition of an Insider Threat

There are multiple perspectives on what actually defines an insider threat. Theoharidou, Kokolakis, Karyda and Kiountouzis (2005) define the term insider threat as the misuse of privileges, and violation of the IS security policy of the organization, by people who have been given access rights to an information system. Pfleeger, Predd, Hunker, and Bulford (2010) define an insider threat as the action of an insider that puts an organization's data, processes, or resources at risk in a disruptive or unwelcome way.

These definitions clearly outline the actions of the insider, but do not place any focus on the motivation behind the misuse. In contrast, Roy Sarkar (2010) points out that an insider can commit misuse acts maliciously, or by accident whilst trying to do their job. The view that insider threats can be accidental or intentional is also supported by Carroll (2006). There is a contrasting viewpoint, as expressed by Shultz (2002), that only intentional malicious acts should be considered under the auspices of insider threat. The definition adopted in this research is that offered by Theoharidou et al. (2005), taking into account both malicious and accidental acts. The reason for this is to ensure that a holistic literature review is conducted, inclusive of the literature focusing on accidental insider misuse.

Definition of an Insider

With respect to insider threat, the term 'Insider' could apply to a broad spectrum of individuals. Hamin (2000) defines the 'insider' as any person with legitimate access to an organization's information systems, including employees, contractors, vendors and consultants.

This definition is expanded on by Willison and Warkentin (2006), who suggest that insiders use access privileges and knowledge of internal processes to exploit inherent information security vulnerabilities in their organizations. The definition of insider is stretched even further by Roy Sarkar (2010) to include spouses, friends and clients of employees.

Having defined the fundamental concepts of this research topic, the following section will move on to discuss the industry perspectives on insider threat.

Industry Perspective of Insider Threat

According to Steele and Wargo (2007), insiders are as much a threat to the information security of an organization as outsiders, but organizations are not implementing the necessary counter-measures to address these threats. Colwill (2009) quantifies this somewhat, noting that there has been an overreliance on technical solutions to information security problems, without sufficient consideration of the other factors involved.

CSO Magazine (2011) states in their Cybersecurity Watch Survey that insider attacks are more damaging than attacks from an external party, even though insider attacks make up only 22% of total security breaches. Verizon Business (2011), on the other hand, posits in their data breach report that 17% of security breaches are insider related. However, they do not offer any position on the level of damage done by insider attacks. Widup (2010) offers a different perspective on the insider incidents, noting that at least half of them were shown to be accidental.

A number of sources in the literature posit that insider incidents are not always reported. Roy Sarkar (2010), for example, offers four reasons, from the perspective of the organization, for insider incidents not being reported: fear of negative publicity; difficulty identifying culprits; ignorance of the attacks; overlooking incidents due to low impact. Colleagues of a malicious insider may notice suspicious activity, but not report what they have seen. This could be due to the witnesses being unaware of the significance of the activity they are seeing (Colwill, 2009). Shaw, Ruby and Post (1998) expand further on the non-reporting of incidents, noting that incidents are often handled internally, avoiding adverse personal and organizational impact.

The growing organizational trend towards mobile computing, outsourcing and home working increases the probability of malicious acts by insiders (Jones, 2008). Outsourcing increases the risk of data confidentiality being breached, as data becomes available to third parties (Roy Sarkar, 2010). Outsourcing, according to Steele and Wargo (2007), has reduced cost and increased efficiency, but has led to sensitive data being moved beyond the control of the organization.

Home working tends to cause information security to become lax, as people merge their home lives and working lives (Colwill, 2009). Silowash, Cappelli, Moore, Trzeciak, Shimeall, and Flynn (2012) state that organizations must be aware of the remote access technologies used by staff members who work from home, in order to mitigate risks caused by remote access networking.

Laptops, PDAs and other mobile devices are a great source of data leakage in organizations (Roy Sarkar, 2010). There is a high likelihood that system users could store company data on the local drives of their laptops, but the portability of laptops render them highly vulnerable to loss or theft (Widup, 2010).

The industry perspective of insider threat discussed the real world factors affecting insider threat, and focused on case studies outlining the impact of insider threat incidents. The following section will elaborate on the impact of insider threat incidents.

The Impact of Insider Threat

Insider threat incidents can impact the affected organization in a myriad of ways. This section will describe the impact of insider threat, illustrated, where relevant, by examples found in the literature.

Financial impact

Insider threat can result in financial loss for the affected organization. An example of this is offered by Dhillon and Moores (2001), who use the example of the Kidder Peabody case to illustrate financial loss due to insider threat. Joseph Jett defrauded Kidder Peabody & Co out of millions of dollars by exploiting flaws in the Kidder accounting system. Jett's bonuses and salary during his fraudulent period were over 9 million US dollars. According to Reddy Randazzo, Keeney, Kowalski, Cappelli, and Moore (2005), the malicious actions of a just a single insider can cause financial damage so severe that the affected business could be forced to shut down.

Loss of reputation

An insider threat incident can also result in loss of reputation for the affected organization. A misuse act was perpetrated by Robert Hanssen, which resulted in immense damage to the reputation of the United States Federal Bureau of Investigation (FBI). Hanssen was an FBI veteran, who abused his access to confidential data by selling information that he had stolen to Russian agencies, resulting in immense damage to the public image of the FBI and the national security of the United States (Magklaras & Furnell, 2002).

Sabotage

Disgruntled employees are able to use their insider knowledge of systems and processes to sabotage their employer, or former employer's, information systems. A good example of this is the Abdelkader Smires case. Smires reacted to personal differences with his employer, Internet Trading Technologies, by launching a Denial of Service (DoS) attack on them, causing downtime and loss of revenue (Magklaras & Furnell, 2002). Another case is offered by Dhillon (2001), who refers to the erasing of all the computers in the Digital Technology group, an internet service provider. The disgruntled employee who had committed this act of sabotage was subsequently arrested and jailed. Other potential impacts also exist, such as intellectual property theft or industrial espionage (Roy Sarkar, 2010).

The case studies and real world examples in this section described and quantified the impact of insider threat incidents. In summary, insider threat according to the literature reviewed is a risk to information security and can have a significant impact on an organization. This impact could be financial, reputational or operational, even resulting in the loss of life in extreme cases.

Research Methodology

Webster and Watson (2002) support the view that literature reviews can be used to identify areas where research is needed. They also state that they can create foundations for advancing knowledge and facilitate theory development. A specific method for conducting rigorous, descriptive literature reviews has been proposed by Wolfswinkel, Furtmueller, and Wilderom (2013). This method uses grounded theory methods as a way of thoroughly analyzing a topic.

Grounded theory is an approach to building theories based on observations, patterns in data or behaviors. In this study the data analysis followed a grounded theory approach employing a coding strategy using open, axial and selective coding techniques. The research methodology consisted of a five stage iterative approach for the systematic and rigorous review of literature that can be seen in Table 1.

Table 1: Stages of the literature review method (Wolfswinkel et al., 2013)

Stage	Task
1. Define	1.1 Define the criteria for inclusion/exclusion
	1.2 Identify the fields in the research
	1.3 Determine the appropriate sources
	1.4 Decide on the specific search terms
2. Search	2.1 Search
3. Select	3.1 Refine the sample
4. Analyse	4.1 Open coding
	4.2 Axial coding
	4.3 Selective coding
5. Present	5.1 Represent and structure the content
	5.2 Structure the article

The research method was considered suitable as it provides a systematic and rigorous approach for conducting a concept-centric literature review. It allows for the review of a potentially large selection of articles within clearly defined criteria. The approach enables textual data to be arranged into concepts, categories and sub-categories that are analyzed in a variety of ways. This inductive approach allows for patterns and findings to emerge and for the classification to be made (Wolfswinkel et al., 2013).

Sampling

The field of research was restricted to Information Systems (IS). The sample included the top 50 ranked MIS Journals from IS World, as well as top security journals in the IS domain. To determine the appropriate search terms, preliminary searches were done on the databases using multiple variations and other terms associated with insider threat. The search term 'Insider Threat' was chosen as it is the key term relating to the research and a total of 622 articles resulting from this search term was obtained. After removing duplicate articles and eliminating irrelevant articles a sample of 90 unique and valid articles remained.

Internal Validity

According to Randolph et al. (2005), Fleiss Kappa is a widely used statistical measure in the fields of content analysis and meta-analysis, determining how well raters agree on the coding of nominal variables. If the amount of cases per category is fixed prior to the start of coding, a fixed-marginal validity measure is appropriate.

However, whilst Fleiss' Multirater Kappa is appropriate for fixed-marginal validity studies, it is not appropriate for agreement studies that have free-marginal distributions (Randolph et al., 2005). In the case of this research project there was no fixed number of allowed articles per category, and therefore the Free-Marginal Multirater Kappa was used to measure the agreement levels of the researchers. A Kappa of 1 indicates almost perfect agreement and a Kappa of 0 indicates poor, or chance, agreement.

A Kappa of 1.0 was achieved for article elimination and a 0.6111 Kappa was achieved for article coding, which denotes a substantial level of agreement.

Classification

Analysis resulted in a classification of the 90 valid articles into 6 high-level categories and 13 subcategories. A graphical representation of these categories and subcategories and their relationships can be seen in Figure 1.

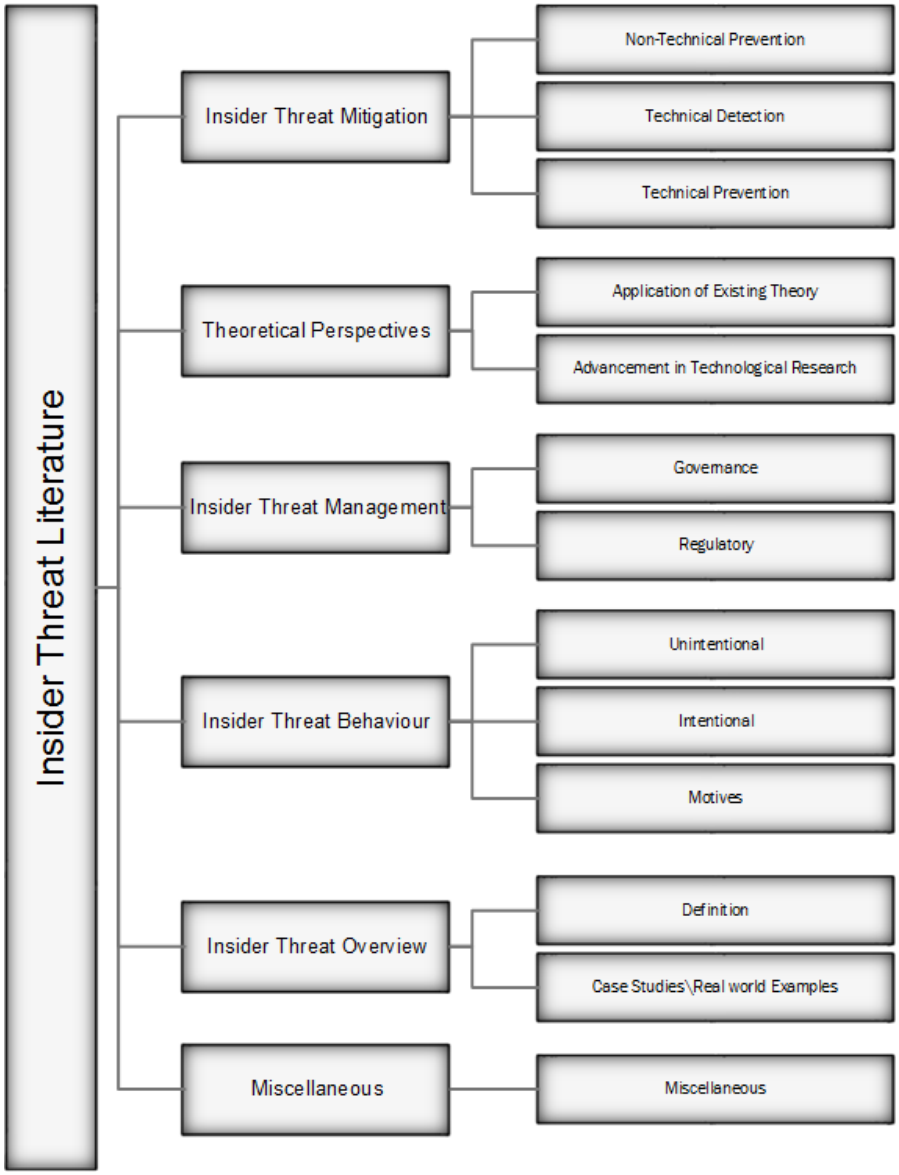


Figure 1: Classification of Categories and Subcategories in Insider Threat Research

Insider Threat Overview

The articles in this category include explanations of the insider and of insider threat. Also in this category are case studies that examine the impact of insiders and insider threat incidents.

Definition: This subcategory contains articles that provide topic and concept detail and explanations. These articles provide definitions for the 'insider' and the 'insider threat', the different types of insider attacks, the scope of insiders and their actions, the differences between insider and outside threats, what motivates insiders and then the specific role the insider plays in data

leakage challenges. There are some that look at traditional security measures and their shortcomings, what characterizes security compliant behavior and areas of interest for future research.

Case Studies and/or Real world Examples: The articles in this subcategory focus on specific instances of insider threat and practical examples of problems relating to the topic. The lack of integration of logical and physical security systems and the missed potential are reviewed, the of role education and human nature in insider threat management, the impact of human error resulting in data leakage and the costs incurred to industry as a result of insider incidents.

Insider Threat Behavior

The articles in this category include insider threat behavior, both intentional and unintentional, and the motives of insiders.

Unintentional: This subcategory focuses on articles that examine the unintentional behavior of insiders that result in insider incidents. Although people are considered the most effective attack vector for insider attacks, this is largely attributed to lack of awareness and training and the lack of clearly defined policy to support awareness. These policies need to extend to applications as they too can contain inherent insider flaws.

Intentional: This subcategory examines the impact and nature of intentional cyber-attacks and techniques. Increasing industrial espionage and cyber theft is requiring equally swift updates in legislation. Articles here also look at the challenges Data Leakage Protection solutions face and the prevalence of low-tech attack vectors.

Motives: This subcategory examines good and bad end user behavior and what motivates each. Articles here review factors that support compliant behavior and factors that lead to malicious behaviors, but not necessarily resulting in a security incident.

Insider Threat Management

This category looks at both governance and regulatory aspects of organizations' approach to dealing with insider threat.

Governance: The article in this subcategory looks at how the insider threat is an essential factor in a holistic enterprise risk management strategy.

Regulatory: The articles in this subcategory would examine regulatory considerations and factors. There were no articles that were categorized with this subcategory as their major concept.

Insider Threat Mitigation

This category covers all forms of threat detection and threat prevention solutions including both technical and non-technical techniques, strategies, policies and frameworks.

Non-Technical Prevention: The articles in this subcategory include developing neutralization techniques that actively reduce intentions of users to violate security policies, developing Situational Crime Prevention scripts specifically for the mitigation of insider behavior, looking at where IT security policies do not align with implemented technical solutions and the relationship between user effort and effective security trade off. Minor topics include the changing risk profile of employees as insider threats through their employment life-cycle, the role of trust in organizational culture for IS security, the use of Game Theory to profile legitimate user behavior, the role of standards like ISO 27001 in organizational compliance, user education with formalized user and security policies, and the role of access control policies in the enterprise.

Technical Detection: The articles in this subcategory cover mechanisms that review access in terms of fulfilment of security obligations, document management system (DMS) usage profiling,

file access monitoring, internal webserver log monitoring, frameworks that leverage multiple log sources for detection, host-based monitoring for database management systems (DBMS) and network flow analysis technologies.

Technical Prevention: This subcategory covers early warning systems based on the traditional honey-pot concept, the evolution of incident management technologies, Intrusion Detection System (IDS) tampering mitigation and the role of identity management and user provisioning systems to limit user access to user life-cycles.

Theoretical Perspectives

This category is where theories, frameworks or technologies are used, proposed, developed and expanded on to further the understanding of insider threats, behavior or motives.

Application of Existing Theory: In this subcategory the articles fall into one of three themes; threat-prevention research, threat-detection research and theory application. All articles in this subcategory build on or reference existing technologies or theories. Threat prevention articles range from the use of risk metrics in the automated access request process to combat data leakage to the relocation of data and applications away from potential attackers. Also in this subcategory are articles reviewing host-based monitoring and decoys for prediction, combining static analysis techniques with existing prevention mechanisms, data leakage prevention by means of random data perturbation (RDP), real-time updating and enforcing of access control policies and system hardening combined with organizational learning as protective layers.

Threat detection seems to be the most prevalent topic in this subcategory with articles on behavioral consistency and anomalies, parsing social media for indication of data exfiltration, the use of Role Based Access Control (RBAC) assignments as a baseline for user behavior, the use of Signal Detection Theory to identify precursors to threats and threat incident and perpetrator identification. An attempt to provide a correlation between insider incidents and the sophistication of the perpetrators. Beyond articles that look at behavior for detection are ones that use technological indicators, such as the use of directory virtualization, custom built correlation engines for Active Directory, node-based authentication schemes for unattended network elements, detection of anomalies in development processes, graph-based anomaly detection, the various attack vectors of threats, trends in detection research and even the use of criminal court proceedings to identify insider vulnerabilities.

The third theme ranges from the relevance of behavioral science theories in the cyber-security risk context, the effectiveness of ISO17799 enforcing criminology theories, the importance of user trust for the adoption of security policies and use of Game Theory and simulated insider attacks to configure Intrusion Detection Systems (IDS) to a colorful paradigm of network security compared to castle walls.

Advancement in Technological Research: Articles in this subcategory investigate and simulate the use of Bayesian Network to model insider attack profiles, the development and simulation of detection systems for Collaborative information systems (CIS) and the exploitation of object dependencies in databases for data exfiltration. Preventing exfiltration of data through ad-hoc database query result obfuscation and identifying insider threat using data exfiltration patterns are also covered here. Threat prediction by correlating user behavior and threat rating is explored and the need for aggressive firewall and perimeter testing is reviewed. In-depth research has been done to identify long term patterns of insider behavior for prediction, frameworks that take the organization, the systems, the environment and the individuals into consideration have been developed and the development of a common language in threat prediction and detection applications.

Miscellaneous

The articles in this subcategory do not align with any of the other categories and contain concepts that are unique. There were no articles that were classified with their major concepts in this sub-category.

Distribution of Articles per Year

Shown in Figure 2, the first reference to 'Insider Threat' in the data set was in 1997. There was seemingly very little interest in the subject up to 2007, at which point there was a marked increase in the volume of research articles, culminating in a peak in 2009, with 18 articles published in that year. Post the 2009 peak there seems to have been a stabilizing of the research volume, with an average of 8.5 articles per year between 2010 and 2013.

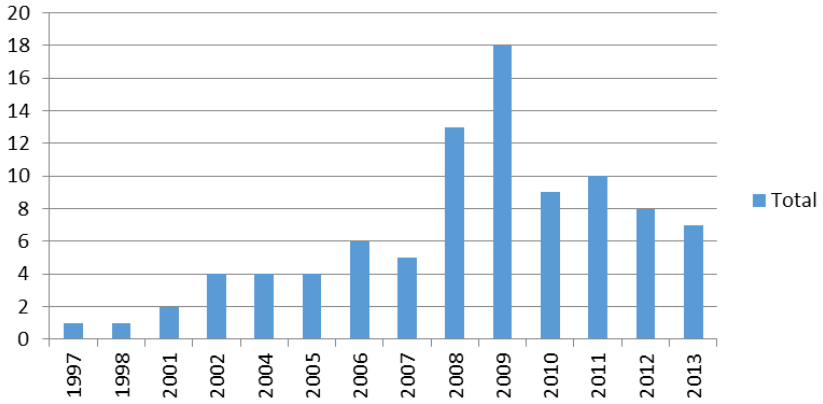


Figure 2: Distribution of articles by year

Distribution of Articles by Category

Table 2 tells an interesting story with regards to the comparison of main category vs. secondary category. Adding up articles with 'Insider Threat Mitigation' as a main category or secondary category results in a total of 60 articles. Conversely, adding up articles with 'Theoretical Perspectives' as a main category or secondary category results in a total of 52 articles. Note that in this exercise articles with the same main and secondary categories are only added once, incrementing the main category tally. Given this tally it could be argued that 'Insider Threat Mitigation' is actually the most dominant category in the dataset.

Conclusion

As per the objectives of the study, a classification was created which described the insider threat body of knowledge. The most heavily populated main category in the classification was the 'Theoretical Perspectives' category. This was offset by the prevalence of 'Insider Threat Mitigation' as both a main and secondary category in the dataset. It is interesting to note that whilst a significant number of technology advancements were proposed in the 'Theoretical Perspectives' category, there is very little to indicate whether or not any of these proposed solutions have been successfully implemented. This indicates a potential opportunity for future research, possibly in the form of case study, to investigate the real world application of some of these proposed solutions.

Another interesting point is the relative lack of articles with 'Insider Threat Management' as the main focus. Information security controls are referred to in the literature, with standards such as ISO17799 getting specific focus. It is therefore quite surprising to see that existing governance

Table 2: Distribution of articles by main category and secondary category

	SECONDARY CATEGORIES						
Main Categories	Insider Threat Behaviour	Insider Threat Management	Insider Threat Mitigation	Insider Threat Overview	Miscellaneous	Theoretical Perspectives	Grand Total
Insider Threat Behaviour	2	1	4	0	0	2	9
Insider Threat Management	0	0	1	0	0	0	1
Insider Threat Mitigation	1	4	8	4	0	5	22
Insider Threat Overview	4	1	6	4	0	2	17
Theoretical Perspectives	4	3	27	3	1	5	43
Grand Total	**11**	**9**	**46**	**11**	**1**	**14**	**92**

structures are not being used as a lens for researching insider threat. Given the fact that regulatory compliance is mandatory for many organizations, the paucity of articles in this area is quite unexpected. This presents an opportunity for future research, in order to examine insider threat from the perspective of governance and compliance.

In terms of trends, an interesting pattern is visible in the distribution of articles over time (Figure 2). The spike in research frequency in 2008 and 2009 is very interesting. This unexplained phenomenon is an opportunity for an explanatory study.

References

Bishop, M., Engle, S., Peisert, S., Whalen, S., & Gates, C. (2009). We have met the enemy and he is us. *Proceedings of the 2008 Workshop on New Security Paradigms*, 1-12.

Carroll, M. D. (2006). Information security: examining and managing the insider threat. *Proceedings of the 3rd Annual Conference on Information Security Curriculum Development* (pp. 156-158). ACM.

Colwill, C. (2009). Human factors in information security: The insider threat – Who can you trust these days? *Information Security Technical Report, 14*(4), 186-196. doi:10.1016/j.istr.2010.04.004

CSO Magazine. (2011). *2011 Cybersecurity watch survey*. CSO Magazine. Retrieved from https://www.cert.org/insider-threat/research/cybersecurity-watch-survey.cfm

Dhillon, G. (2001). Violation of safeguards by trusted personnel and understanding related information security concerns. *Computers & Security, 20*(2), 165-172.

Dhillon, G., & Moores, S. (2001). Computer crimes: Theorizing about the enemy within. *Computers & Security, 20*(8), 715.

Hamin, Z. (2000). Insider cyber-threats: Problems and perspectives. *International Review of Law, Computers & Technology, 14*(1), 105-113. doi:10.1080/13600860054944

Hong, J., Kim, J., & Cho, J. (2010). The trend of the security research for the insider cyber threat. *International Journal of Security & its Applications, 4*(3), 55-63.

Jones, A. (2008). Catching the malicious insider. *Information Security Technical Report, 13*(4), 220-224. doi:10.1016/j.istr.2008.10.008.

Magklaras, G. B., & Furnell, S. M. (2002). Insider threat prediction tool: Evaluating the probability of IT misuse. *Computers & Security, 21*(1), 62-73.

Pfleeger, S. L., Predd, J. B., Hunker, J., & Bulford, C. (2010). Insiders behaving badly: Addressing bad actors and their actions. *Information Forensics and Security, IEEE Transactions on, 5*(1), 169-179.

Randolph, J. J., Thanks, A., Bednarik, R., & Myller, N. (2005). *Free-marginal multirater kappa (multirater κfree): An alternative to Fleiss' fixed-Marginal multirater kappa*. In Joensuu University learning and instruction symposium.

Reddy Randazzo, M., Keeney, M., Kowalski, E., Cappelli, D., & Moore, A. (2005). *Insider threat study: Illicit cyber activity in the banking and finance sector*. (Performing organization report number CMU/SEI-2004-TR-021). Pittsburgh, PA: Carnegie Mellon University. Retrieved from: http://www.sei.cmu.edu/reports/04tr021.pdf

Roy Sarkar, K. (2010). Assessing insider threats to information security using technical, behavioural and organisational measures. *Information Security Technical Report, 15*(3), 112-133. doi:10.1016/j.istr.2010.11.002

Schultz, E. E. (2002). A framework for understanding and predicting insider attacks. *Computers & Security, 21*(6), 526-531. doi:10.1016/S0167-4048(02)01009-X

Shaw, E. D., Ruby, K. G,. & Post, J. M. (1998). The insider threat to information systems. *Security, Awareness Bulletin, 2*(98). Political Psychology Associates.

Silowash, G. J., Cappelli, D. M., Moore, A. P., Trzeciak, R. F., Shimeall, T., & Flynn, L. (2012). *Common sense guide to mitigating insider threats*. Published by CERT, Software Engineering Institute, Carnegie Mellon University, http://www. cert. org.

Steele, S., & Wargo, C. (2007). An introduction to insider threat management. *Information Systems Security, 16*(1), 23-33.

Theoharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799. *Computers & Security, 24*(6), 472-484.

Verizon Business. (2011). *Data breach investigations report*. Verizon Business.

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly, 26*(2), xiii-xxiii.

Widup, S. (2010). *The leaking vault–Five years of data breaches*. Digital Forensics Association.

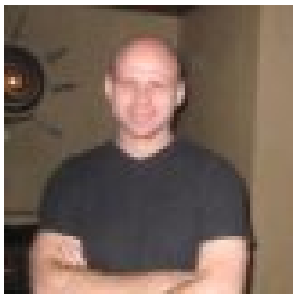
Willison, R., & Siponen, M. (2009). Overcoming the insider: Reducing employee computer crime through situational crime prevention. *Communications of the ACM, 52*(9), 133-137.

Willison, R., & Warkentin, M. (2006). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly, 37*(1), 1-20.

Wolfswinkel, J. F., Furtmueller, E., & Wilderom, C. P. M. (2013). Using grounded theory as a method for rigorously reviewing literature. *European Journal of Information Systems, 22*(1), 45-55. doi:10.1057/ejis.2011.51

Biographies

Jacques Ophoff is a Senior Lecturer in the Department of Information Systems at the University of Cape Town (UCT), South Africa. He obtained his doctorate in Information Technology from the Nelson Mandela Metropolitan University, South Africa. Before joining UCT he was an IT Product Manager at an online startup company. His research interests include information security, mobile technologies, and education.



Adrian Jensen is an Infrastructure Specialist in the Financial Services industry. He also has many years of experience as a Systems Administrator. Adrian is a graduate of the University of Cape Town, and holds a Bachelor of Commerce (Hons) degree specializing in Information Systems.

Jonno Sanderson-Smith is a Consultant in the IT and Services sector. He has an interest in identity and access management. Jonno is a graduate of the University of Cape Town, and holds a Bachelor of Commerce (Hons) degree specializing in Information Systems.

Michael Porter is an IT professional specializing in IT Service Management in the Financial Services industry. Michael is a graduate of the University of Cape Town, and holds a Bachelor of Commerce (Hons) degree specializing in Information Systems.

Kevin Johnston is an Associate Professor in the Department of Information Systems at the University of Cape Town. He worked for 24 years for companies such as De Beers, Liberty Life, Legal & General and BoE. Kevin's main areas of research are ICT Strategic Management, IS educational issues, IS-related social issues and Open Source Software.