The Threats that Insiders Pose to Critical Infrastructure – A South African Perspective

D. Heneke, J. Ophoff and A. Stander

Dept. of Information Systems, University of Cape Town, Cape Town, South Africa
e-mail: hnkdar002@myuct.ac.za; {jacques.ophoff; adrie.stander}@uct.ac.za

Abstract

Insider threat is reported less frequently than cyber-attacks yet remains an important information security risk in organisations. It is arguably more difficult to handle due to the access and knowledge of the insider. We report the results of a qualitative study across four critical infrastructure (defence, telecommunications, energy, and financial) organisations in South Africa on the perception and management of insider threat. The results show that the organisations have various cyber-security related plans in place, yet these are only not always enforced, monitored, or updated as the threat landscape changes. Within organisations insider threat is not always considered to be of strategic importance at the executive management level, leading to a lack of funding to mitigate risks. In order to reduce the risk of insider threats it is vitally important to create a culture of security compliance among all employees of the organisation. This should be driven by a top-down management approach. Where managers have taken responsibility, and were driving the awareness and compliance with security policies, the understanding and reduction of insider threats was clearly evident.

Keywords

Critical Infrastructure, Insider Threat, Information Security, Cyber Security

1. Introduction

Information systems and data are a strategic resource and must be protected against theft or damage, whether accidentally or maliciously (Posthumus & Von Solms, 2004; Siponen & Oinas-Kukkonen, 2007). The international trend over many years has been to protect against external cyber threats. The insider threat has grown exponentially, but most organisations do not have adequate defensive mechanisms in place to defend themselves against these threats (Schultz, 2002). Employers generally assume that the trust and integrity of employees can be accepted. However, the extent of insider threat damage from a financial, reputational, or operational perspective indicates that this is a serious problem requiring strategic attention (Jaffe, 2010; Cappelli, Moore, & Trzeciak, 2012).

This paper examines current understanding of insider threat in critical infrastructure organisations in South Africa. This includes awareness of insider threat, the potential implications of security breaches, and how these are managed. Identifying commonality between critical infrastructure organisations could be beneficial if they collaborated regarding insider threats (National Infrastructure Advisory Council,

2015). This paper lays a foundation for further studies on the insider threat phenomenon, which is currently lacking within a developing country context.

Critical infrastructure is considered to encompass the core services which are vital to a country and its people (US Department of Homeland Security, 2014). In the South African context this paper will address the defence, telecommunications, energy, and financial sectors. The majority of these are parastatal institutions; however, each one has different IT systems, infrastructure, and security policies. Each one also has specific differences in vulnerabilities and counter measures.

The main research question is: How is insider threat perceived and managed within critical infrastructure organisations in South Africa? The question is addressed through primary data collection in the form of surveys with top management, and users in various roles, in critical infrastructure organisations. The results of data analysis point to several issues in the research context, which is the main outcome of the study.

2. Background

An insider threat has the potential to put an organisation's data, processes, or resources at risk in a disruptive or unwelcome way (Pfleeger, Predd, Hunker, & Bulford, 2010). Theoharidou, Kokolakis, Karyda, and Kiountouzis (2005) define the term insider threat as the misuse of privileges and violation of the organisation's IT security policies by users who have been given system access rights. There are two main categories of insider threats: malicious (e.g. information theft) and unintentional or accidental. Unintentional threats refer to users who put the organisation at risk by not complying with the security policies due to ignorance, carelessness, or negligence. A difficulty is that it is not always possible to differentiate between these two categories of threats (Vroom & Von Solms, 2004).

Insider threat research has focused on a variety of areas, including behavioural issues, management, mitigation and theoretical perspectives (Ophoff, Jensen, Sanderson-Smith, Porter, & Johnston, 2014). Due to its inherent complexity the insider threat is difficult to manage and generic security controls have not proven to be completely effective and reliable to mitigate the threat. One of the main reasons for this is the nature of an insider, who has trusted access to systems and information.

Insiders can be defined as any person who has legitimate access to an organisation's IT systems, networks and infrastructure. Such 'trusted' persons may include, current employees, former employees, contractors, and service providers (Silowash, 2012). Insider roles are commonly dictated by the organisation's IT usage policies, which consist of "a set of laws, rules, practices, norms and fashions that regulate how an organisation manages, protects, and distributes the sensitive information and that regulates how an organisation protects system services" (Caelli, Longley, & Shain, 1991). Insider threats occur when insiders do not adhere to such policies.

Insiders have an advantage as attackers because they know the systems, procedures and general operational functioning of the organisation. This includes former employees who no longer have physical access to the organisation, because they still retain knowledge of the systems and their vulnerabilities (PWC, 2013). From previous research it is clear that there is a lack of awareness from within critical-infrastructure sectors of the potential threats that insider's pose, as well as the severe consequences of not putting strategies in place to mitigate these risks (Gelles, Brant, & Geffert, 2008; Ponemon Institute, 2013). Without a clear understanding of the problem, it will not be possible to effectively reduce insider threats.

3. Research Methodology

The purpose of this research is both descriptive and exploratory as it firstly analyses the threats posed by insiders, secondly attempts to determine why these are prevalent, and thirdly proposes improvements regarding policies, best practices and user awareness programs for organisations. The research adopts an interpretive philosophy to address the research question. A survey consisting of a questionnaire and interview guide was developed, based on an initial literature review, and adapted to suit the South African environment.

Interviews were conducted with the Chief Information Officer (CIO) and Chief Security Officer (CSO), or equivalent security expert, within each of the four targeted critical infrastructure organisations (eight interviewees in total). To supplement the interview data users in various roles were targeted with a questionnaire. Roles included finance, logistics, human resources, and senior IT support. A non-probability sampling technique based on the snowball sampling method was used to identify stakeholders (Saunders, Lewis, & Thornhilll, 2016). 31 completed questionnaires were received and analysed. Full ethics approval was obtained from the University's Research Ethics Committee.

All interviews were conducted face-to-face and participation was voluntary. Interviews were recorded and transcribed before analysis. The transcriptions were analysed through thematic and axial coding using CAQDAS software (NVivo and QDA-Miner). In the analysis questionnaire data is linked to a 'respondent' while interview data is linked to an 'interviewee'.

4. Data Analysis

4.1. Understanding of the insider threat phenomenon

The majority (87%) of the questionnaire respondents consider that insiders are potentially a threat to their organisations. This is based on those respondents who answered either definitely or possibly. The deduction can therefore be made that the majority of respondents recognise that this threat exists in their organisations. However, an indicative comment came from Respondent 29 who stated that *"there is very little understanding of this threat within our organisation"*. During one of the interview sessions, Interviewee 6 stated: "*The Insider Threat is, to a large extent,*

limited to accidental incidents which are not malicious, caused through user ignorance and/or non-compliance with policy, resulting in minor threats", which points to a subset of the overall problem. Both comments illustrate that in some organisations the insider threat is either not understood, or it is considered to be an inconsequential problem and therefore a manageable risk to the organisation. In contrast, research conducted internationally has shown that the insider threat is definitely not something to be underestimated (Cappelli et al., 2012).

4.2. Perception of insider vs. external threats

An important finding was that the insider threat is generally not very high on the list of priorities for organisations within the critical infrastructure sectors. As Interviewee 3 stated: "In South Africa, the external threat is still perceived to be far greater and as such very little time and effort is spent on protecting against the insider threat. This can potentially result in financial losses, disruption of services and loss of customers/market share within our organisation". A similar sentiment was expressed by Interviewee 5 who indicated that "the perception is that the external threat is still by far the greatest problem facing any organisation in SA. I believe that if the international trends are studied, we will find that the insider threat may be less than 10% of the incidents which occur, but the financial impact in many cases is extensive. In SA, this aspect is not really understood or considered as a major factor. In all possibility, research of this nature may help to create awareness".

One of the organisations participating in this research admitted that the "insider threats represents 99% of all security incidents. Our network is, supposed to be a closed network, making it more difficult for outsiders/hackers to access our systems and information" (Respondent 27). Further discussion revealed that many organisations have a false sense of security in believing that their 'closed' systems/networks have eliminated almost all potential security incidents. This false sense of security has the potential to result in extremely serious consequences from which recovery could be a lengthy process. The effects on critical infrastructure organisations, which provide essential services, may have far reaching consequences, not only for the organisation, but for South Africa as well.

Interviewee 8 provided a relevant summary of these issues, stating that "the external threat is still considered to be the far greater threat, however, as new methods evolve within criminal syndicates and a culture evolves of reduced loyalty to the organisation, this threat has the potential to escalate dramatically". A question that needs to be asked is whether South Africa is ready for such an escalation? Based on the results of this research South Africa is relatively prepared to manage the external threat, however the country still has a long road to travel in understanding, managing, and significantly reducing the insider threat.

4.3. Perceived threat posed by insiders

The majority of respondents were of the opinion that fraud constituted the most damaging implication of an insider action, followed by sabotage, theft of intellectual

property, and unintentional actions. Due to the nature of critical infrastructure sectors in South Africa the market share and loss of customers rated very low in terms of implications. This could be attributed to the fact that the energy sector, and to an extent the telecommunications sector, are controlled by parastatal organisations.

By the very nature of an insider's legitimate access to the systems and information within an organisation, Interviewee 5 stated that *"it would be foolish to assume that the insider threat does not have the potential to escalate"*. International research has shown that where the insider threat is not managed and controlled, the consequences for organisations could be disastrous. Based on this research the most common threats, as identified by a large percentage of the respondents, appear to be fraud, sabotage of IT systems, and information-espionage by administrators and users with excessive rights. Interviewee 5 further commented that *"users have started breaching the trust of employers for different motives"*. This research also highlights the perceived threats created by malicious and unintentional insiders. Analysis indicated that the unintentional insider threat can be effectively managed and eliminated on condition that policies and procedures are enforced and a culture of security awareness and education, at all levels of the organisation, is implemented and continuously maintained and updated.

An aspect not previously considered as a priority focus area, but which became clear during some of the interviews, was that insiders are normally the easiest target from whom sensitive information can be obtained. Respondent 23 indicated that *"insiders can legally gain access to various areas of information resources and are mostly influenced through social-engineering, bribery, or extortion"*. These insiders effectively become an intermediary providing access to critical systems or sensitive information. The insider threat has the potential to become a large problem based on the opportunities that are available to them. The traditional security paradigm is to try and keep outsiders from the network and systems and insufficient attention is focused on the threat within the organisation. Insiders may also be coerced into allowing outsider access to the internal systems, either because of money or some other threat.

The following comments are representative of the problem facing organisations. Respondent 31 stated that *"people are complex creatures to manage. Trust is always a problem"*. Interviewee 6 highlighted the fact that *"an insider normally acts from behind the traditional security barriers, and can do more harm without being noticed"*. These comments clearly illustrate a few of the complexities when dealing with the insider threat.

4.4. Factors considered important to secure critical infrastructure

Implementation and enforcement of security policies and procedures. The adoption of IT security standards within an organisation should follow a top-down approach from executive management to the lowest functioning employee and not, as was evident during this research, from middle management up and down. It is of no significance if all the policies and procedures are in place, but are not strictly

enforced, and insiders seize the opportunity to commit cybercrimes with little or no fear of reprisal. Without regular monitoring having a standard in place is inconsequential. Respondent 31 highlighted the complexity when commenting that *"policies and procedures alone are not necessarily going to improve the situation. Insider attacks are usually launched by few individuals who will behave badly regardless of the policy. The trick/difficulty is identifying them and dealing with them"*.

An important aspect identified during this research was that IT security policies and procedures can assist in reducing the insider threat but only if they are relevant, applicable, implementable, measurable, reviewed and updated regularly, and most importantly that these are monitored and enforced. If the standards and policies do not adhere to these requirements, they are of absolute no value and will not reduce the threat. It is also important to consider that since every organisation is unique, with regards to threats, vulnerabilities, culture, etc. the protection mechanisms should be tailored accordingly where required.

Monitoring and conducting security assessments on a regular basis seems to be an effective method and first step in establishing a secure organisation. Respondent 22 confirmed this viewpoint stating that *"having an IT security standard in place without regular monitoring is as good as having nothing in place"*. In virtually all the organisations communication channels for the reporting of incidents was in place and generally considered acceptable. However, as Interviewee 7 indicated, *"due to top management being reluctant to take severe action against transgressors, I do not think that the effectiveness is satisfactory. The conviction rate for incidents is fairly low and as a result, this has not really reduced the number of incidents"*. The majority of organisations who participated in the survey have well established IT security policies. The problem is that these policies, and procedures, seldom receive support and enforcement from executive management. The perception appears to be that once the policies and procedures are published the task is complete and no further action is required. For IT security policies to be effective Interviewee 5 and 6 both indicated that *"without the monitoring, enforcement, training and reviewing of these policies and procedures, they are not worth the paper they are written on"*.

Cooperation between HR and IT (security) departments. In the majority of the critical infrastructure organisations participating in this survey it was established that the recruitment of employees is either handled by the HR department or an external recruitment agency. There appears to be a serious lack of communication between the HR and IT security departments in that an IT specialist is recruited for a specific position without proper understanding of the detailed job specifications and personal profile. There should be a greater interoperability between HR and IT security when it comes to the recruitment of IT specialists and specifically system administrators. It was also established that the retention of skilled IT security personnel and system administrators is extremely difficult, as there doesn't to be much loyalty to the organisation. Interviewee 5 and 6 supported this theory when it was stated that *"retention of skilled IT security expertise is a major area of concern. We cannot*

compete with other industries when an employee receives a substantially better offer".

An additional problem identified was that in the majority of the organisations there are no automated systems between the HR and IT departments. In certain cases, it is only by accident that the IT department becomes aware of an individual having transferred or left the organisation. In one of the organisations, Interviewee 8 stated that the procedure when an employee is transferred, resigns, retires or whose employment is terminated, requires that the relevant department provides these details to the IT department. This is the theory, but in reality participants reported that this rarely happens. The implication of an automated system not being in place to manage this, results in the unacceptably high number of invalid or orphaned user accounts, which creates a serious vulnerability for any organisation, especially if an employee left the organisation unwillingly or with a grievance.

Management's role. The best way to detect a potential malicious or unintentional insider isn't usually a software security system. It is an alert manager who realises that an employee is disgruntled and may be capable of taking things too far, or a co-worker who overhears a threat being made by a specific employee against the organisation. These human observations can lead to reducing threats posed by insiders, however, there must be a culture of reporting such incidents as well as management being willing to listen and take appropriate action. Failure to take cognisance of these human observations may result in an insider security incident such as sabotage of IT systems or the loss of confidential information.

The perception within middle and lower levels within the organisation is that cyber-security is not taken seriously enough by top management. Based on factors identified during this research, one of the main reasons for this is believed to be because of a lack of understanding of the insider threat as well as the implications of these threats. Interviewee 5 clarified this aspect by stating that *"economies of scale are relevant when dealing with insider security threats. Where risks are not critical, funding will not be provided by executive management"*. Limited financial budgets for IT security are one of the critical factors which reduce the ability for protection against insider threats. Financial decisions are often connected to the insider vs. external threat debate, as illustrated by Respondent 18: *"the external threat is still considered to be the greatest threat and consequently most funding is pumped into this area of protection. The internal threat is not considered serious enough to warrant major financial investment"*.

In analysing this aspect numerous respondents repeated that without the prerequisite financial support, protection of systems and information becomes very difficult to achieve. The dilemma facing security specialists is illustrated by Interviewees 3 and 7, who stated that *"it is often very difficult to convince the executive management to invest more money into security systems/controls unless the potential losses exceed the expenditure required to implement such systems"*. In the majority of situations, the IT department found it extremely difficult to convince executive management to

invest additional money into security controls unless the potential losses far exceed the expenditure.

5. Discussion

The general opinion is that South Africa is not a threat in the international arena, and therefore will not be a target for colluded insider threats. The vast majority of respondents at least recognise that this threat potentially exists in their departments (section 4.1); however, it does not appear that measures are in place to protect their organisations adequately. The insider threat is generally speaking, not very high on the list of priorities for organisations within the critical infrastructure sectors. In South Africa, the external threat is still perceived to be far greater and as such very little time and effort is spent on protecting against the insider threat (section 4.2). Perceptions should be changed regarding the insider vs. external threat – our participant views point to a lack of understanding and awareness regarding the consequences of insider threat as well as what constitutes an insider (section 4.3).

Perhaps as a consequence of the above, there are very few critical infrastructure organisations with effective policies and procedures to manage insider threat. In many cases this aspect is acknowledged but not enough has been done to manage it proactively. It is evident that policies and procedures need to be revised and that stricter enforcement should be applied, which is currently lacking (section 4.4). Regular security risk assessments should be conducted to help mitigate the threat. Lack of top management support and funding are barriers to achieving this (section 4.4). Top management should be fully informed and a top-down approach should be implemented (Posthumus & Von Solms, 2004).

There is a critical lack of IT, cyber-security, and system administrator expertise within the critical infrastructure organisations, as well as within South Africa as a whole (Humphries, 2015). The consequence of this is that personnel are appointed into jobs, where they are expected to ensure the security of IT systems and information, when they do not have the necessary experience or knowledge to be able to fulfil this role effectively (section 4.4). Furthermore the retention of such specialists appears to be extremely difficult, mainly due the supply-demand problem as well as a situation where loyalty is no longer a factor amongst employees. An effective recruitment practice was identified in some organisations, where candidates are referred by peers in the industry and then subjected to a rigorous interview process and comprehensive background checks. It is critical that IT (security) and HR departments cooperate in this regard.

Due to the shortage of skilled personnel, as well as the ability of the organisation to retain these skills, some of the critical infrastructure organisations have resorted to outsourcing the management of cyber threats (internal and external). The concern is that outsourcing takes a degree of control away from the organisation and they become reliant on the outsourced business partner to effectively manage this threat. This appears not to be the best option, but in certain cases there is little alternative due to the unavailability of suitably skilled personnel.

Employee well-being appears to be less important today than it was in the past. This poses a risk because unhappy employees are more inclined to become a threat to the organisation. Our data points out several of the 'human' problems facing organisations today: difficulty in understanding the motives of malicious insiders (section 4.3), vulnerability of users to social engineering attacks (section 4.3), and a lack of organisational loyalty (section 4.4). Behavioural information security research has long acknowledged the difficulties in dealing with the human aspect of security (e.g. Vroom & Von Solms, 2004). This is something organisations should not neglect as part of a holistic management plan.

6. Conclusion

In South Africa very little research has been conducted on the insider threat. The insider threat is a global phenomenon and consequently South Africa should participate with international organisations in order to improve and mitigate the threats. In a few of the critical infrastructure organisations the responsibility for managing the IT systems security is an 'over and above' task and there is no specialist career path for this function. Consequently, less than ten percent of the daily job addressed security related concerns. The insider threat should be recognised and placed into perspective in order to ensure that the correct protective measures are implemented and enforced by proper management of all resources including contractors and sub-contractors.

The findings indicate that the unintentional insider threat can be effectively managed and eliminated on condition that policies and procedures are enforced and a culture of security awareness and education, at all levels of the organisation, is implemented and continuously updated. It was seen that well established IT security policies and procedures are in place, but that these policies and procedures are generally focused on preventing external threats and seldom receive support and enforcement from the executive management level.

There appears to be a culture within organisations of deemphasising insider security threats as well as carelessness regarding the safeguarding of equipment, systems and information. Employees aren't always aware of security threats and the consequences thereof. Future research should examine how this culture can be changed. Another area for future research is to examine how legislation should provide strategic guidance regarding the insider threat phenomenon (e.g. the planned National Cybersecurity Policy Framework for South Africa does not cover insider threat). Researchers need to consider legislation and existing empirical data to develop effective and practical strategies. In support of this the current study lays a foundation for future research.

This study targeted specific types of organisations and knowledgeable participants (in particular the interviewees). However, due to the small number of participants, questions around the transferability of results may arise. Future studies can address this by including more organisations in a similar survey.

7. References

Caelli, W., Longley, D., & Shain, M. (1991). *Information Security Handbook*. New York: Stockton Press.

Capelli, D., Moore, A., & Trzeciak, R. (2012). *The CERT Guide to Insider Threats*. Westford, Massachusetts: Pearson Education Inc.

Gelles, M. G., Brant, D. L., & Geffert, B. (2008). *Building a Secure Workforce - Guard against insider threat*. Deloitte Consulting.

Humphries, F. (2015). *Cyber security skills shortfall a 'national emergency'*. Retrieved June 1, 2016 from: http://www.itweb.co.za

Jaffe, B. (2010). *IT Manager's Handbook*. San Diego: Morgan Kaufmann Publishers.

National Infrastructure Advisory Council. (2015). *NIAC Insider Threat to Critical Infrastructures: Final Report and Recommendations*. Retrieved April 15, 2016 from: https://www.dhs.gov/publication/niac-insider-threat-final-report

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).

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

Ponemon Institute. (2013). *Managing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age*. Ponemon LLC.

Posthumus, S., & Von Solms, R. (2004). A framework for the governance of information security. *Computers & Security*, 23(8), 638-646.

PWC. (2013). *Key findings from the 2013 US State of Cybercrime Survey*. Retrieved April 15, 2016 from: http://www.pwc.com

Saunders, M., Lewis, P., & Thornhill, A. (2016). *Research methods for business students (7th Edition)*. United Kingdom, UK: Pearson Education Limited.

Schultz, E. (2002). A framework for understanding and predicting insider attacks. *Computers & Security*, 21(6), 526-531.

Silowash, D. (2012). *Common Sense Guide to Mitigating Insider Threats*. Software Engineering Institute.

Siponen, M., & Oinas-Kukkonen, H. (2007). A Review of Information Security Issues and respective research contributions. *The DATA BASE for Advances in Information Systems*, 38(1), 60-80.

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.

US Department of Homeland Security. (2016). *What Is Critical Infrastructure?* Retrieved April 15, 2016 from: http://www.dhs.gov/what-critical-infrastructure

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security*, 23(3), 191-198.