Australian Government
Department of Defence
Defence Science and
Technology Organisation

Preventing and Profiling Malicious Insider Attacks

Agata McCormac, Kathryn Parsons and Marcus Butavicius

Command, Control, Communications and Intelligence Division
Defence Science and Technology Organisation

DSTO-TR-2697

ABSTRACT

This report examines previous research on malicious insiders with particular emphasis on the social and psychological factors that may have influenced the attacker and their behaviours. This research also draws on corresponding studies into fraud and espionage in non IT scenarios. A range of preventative measures is presented that approach the problem from personnel, policy and technical perspectives. Given the relative scarcity of research into non-technical aspects of malicious insider attacks, further recommendations are also made to study malicious insiders, involving both government and academic stakeholders. Such research has the potential to provide further preventative measures.

Published by

Command, Control, Communications and Intelligence Division
DSTO Defence Science and Technology Organisation
PO Box 1500
Edinburgh South Australia 5111 Australia

Telephone: (08) 7389 5555
Fax: (08) 7389 6567

AR-015-286
April 2012

APPROVED FOR PUBLIC RELEASE

Preventing and Profiling Malicious Insider Attacks

Executive Summary

Insider threat presents an ever increasing problem within Australian government agencies and organisations. The financial repercussions, losses in productivity and damage to public and consumer confidence may result in far reaching negative consequences.

A review of recent literature has revealed that limited research has been conducted into this area. Due to the nature of the problem, previous research has been based on retrospective accounts that examine the details of the insider attacks. However, organisations are often hesitant to reveal details of their experiences with insider attacks.

The aim of this report is to provide specific information about the individuals who commit insider attacks. This includes motivating factors, personality traits and observable behaviours that may assist organisations in the detection and profiling of insiders. In conjunction with this, the identification of technical precursors may prove to be a valuable tool in the detection of an insider threat.

There are certain preventative measures that organisations can implement to improve their overall security and to significantly reduce their chances of becoming targets of insider attacks. For a holistic approach, it is recommended that preventative measures be designed to incorporate three major areas; personnel, policy, and technical aspects.

It is strongly recommended that further research be undertaken within Australia to enhance our understanding of the threat. This may include an analysis of previous attacks to obtain details of any psychological and motivating factors. These factors should also be examined within the incident response to gain insight from information gathered at the time of the attack. Future research should also have an empirical basis to enhance our understanding, which may lead to further preventative measures.

This page is intentionally blank

Authors

Agata McCormac
Command, Control, Communications and Intelligence Division

Agata McCormac joined DSTO in 2006. She is a research scientist with the Human Interaction Capability Discipline in C3ID where her work focuses on cognitive and perceptual psychology, information visualisation and interface design. She was awarded a Master of Psychology (Organisational and Human Factors) at the University of Adelaide in 2005.

Kathryn Parsons
Command, Control, Communications and Intelligence Division

Kathryn Parsons is a research scientist with the Human Interaction Capability Discipline in C3ID where her work focuses on cognitive and perceptual psychology, information visualisation and interface design. She obtained a Graduate Industry Linked Entrepreneurial Scheme (GILES) Scholarship in 2005, with Land Operations Division, where she was involved in human factors research, in the Human Sciences Discipline, specifically in the area of Infantry Situation Awareness. She completed a Master of Psychology (Organisational and Human Factors) at the University of Adelaide in 2005.

Marcus Butavicius
Command, Control, Communications and Intelligence Division

Marcus Butavicius is a research scientist with the Human Interaction Capability Discipline in C3ID. He joined LOD in 2001 where he investigated the role of simulation in training, theories of human reasoning and the analysis of biometric technologies. In 2002, he completed a PhD in Psychology at the University of Adelaide on mechanisms of visual object recognition. In 2003 he joined ISRD where his work focuses on data visualisation, decision-making and interface design. He is also a Visiting Research Fellow in the Psychology Department at the University of Adelaide.

This page is intentionally blank

Contents

This page is intentionally blank

1. Introduction

"Insider threat" is a term that can be broadly used to describe employees, contractors and consultants, who intentionally misuse their computer network access or violate security policy (Schultz, 2002). This report will focus on individuals who exploit a system to commit computer sabotage, extortion, fraud or to steal confidential information.

Insider attacks are a major concern for organisations; they arguably pose a far greater risk than outsider attacks. Colloquially, network security can be described as having a "hard outer coating [with] a soft chewy middle" (Schulz, 2002, p527). Most network security measures focus on preventing access from outside the network. However, there is traditionally far less emphasis placed on securing elements against malicious access from inside the network itself. An employee with authorised internal access has already surpassed the more difficult challenge of gaining external access into a network. In addition to this they are also familiar with the systems and networks of the organisation and know where the important information can be found (Spitzner, 2003).

It has been estimated that insider attacks cost organisations hundreds of thousands of dollars in lost revenue and productivity every year (AusCERT, 2006; Association of Certified Fraud Examiners, 2008). This figure is, of course, only a conservative estimate; it is believed that the figure is significantly higher, as many incidents of insider attack go unreported and are dealt with internally to avoid the repercussions of negative publicity.

In order to deal with and minimise the risks associated with insider threat it is crucial for organisations to have the appropriate tools to identify and detect signs of insider threat and to also implement strategies to prevent insider attacks from occurring. These warning signs are not only technical signs that can be traced through system logs and internal audits, but also include observable behaviours and individual and personality predispositions.

The aim of this report is to determine what personality factors, personality predispositions and motivators may predispose individuals to commit insider attacks and what differentiates this group of people from other employees. The report also aims to provide an overview of preventative measures that may reduce the threat of insider attacks. These warning signs and preventative measures and tactics will be described in greater detail in this report.

1.1 Insider Versus Outsider Attacks

Organisations are likely to experience more outsider attacks than insider attacks. However, the consequences of insider attacks may be more serious, and the attack patterns observed in an insider attack are different from those observed in an outsider attack. Therefore, organisations need to have specific strategies to deal with each type of threat (Schultz, 2002).

Outsider attacks are often intercepted by firewall technology and other access control mechanisms, such as encryption and intrusion detection measures (Schultz, 2002). These attacks tend to be orchestrated by individuals with very high levels of technical expertise, but

they are easier to identify and are more likely to be successfully intercepted using technical strategies (Schultz, 2002). In contrast, the benefit of having physical access to a computer system means that insider attacks do not have to be as technically advanced as outsider attacks. Therefore, insider attacks are often committed by a different group of individuals (Schultz, 2002). Defending against insider attacks is much more challenging, and technical defence measures on their own are often unable to successfully identify an attack (Bellovin, 2008).

Shaw, Ruby and Post (1998) speculate that the insider became all the more dangerous as a result of two changes in information systems: first, consolidation, and second, the elimination of the need-to-know principle. The aim of these changes was to facilitate and improve the sharing of information; however, it has also created more opportunities for damage by removing many obstacles to insider attacks.

An investigation of 959 cases of organisational fraud was conducted by the Association of Certified Fraud Examiners (2008). This study revealed that in the United States alone, organisations reported an average 7% loss of revenue as a direct result of fraud. This figure represents approximately $994 billion in annual losses.

There is also concern that the frequency of insider incidents may be far higher than estimated. Of great concern, was that on average, an act of fraud, which was eventually detected, would avoid detection for a two year period. The detection of these fraud cases was usually the result of a tip rather than an audit or through the use of other detection strategies (Association of Certified Fraud Examiners, 2008). Similar findings were reported by Porter (2003) who found that the majority of insider fraud was detected by either a tip or by accident. Porter (2003) also reported that most cases of insider fraud were not detected until 18 months later. These findings suggest that the number of cases of such fraud that are officially reported is only a lower bound estimate of the actual figure.

Interestingly, the organisations that did implement strategies to reduce the threat of insider attack experienced significantly lower financial losses. For example, organisations that conducted surprise audits reported an average loss of $70,000, in comparison, organisations that did not conduct unexpected audits reported average losses of over $200,000 (Association of Certified Fraud Examiners, 2008).

The impacts of insider activity are not limited to financial losses. In reality the consequences are far reaching and also include the public exposure of sensitive and personal staff and customer information, and negative media attention and publicity. These factors often have a costly effect on reputation and consumer and business confidence (Cappelli, Moore, Shimeall & Trzeciak, 2006). In fact, it is these very concerns which also hamper research into insider threats because organisations are ill inclined to advertise the fact that they have been victims of an internal attack. It is certainly not in their business interest, and may make them appear to be vulnerable and lacking in appropriate security measures. Studies of insiders themselves can only be conducted after the fact, which means that they are all retrospective in nature, and therefore, very few detailed studies of this kind have been successfully conducted.

1.2 Previous Research

There are a small number of insider studies that have had a substantial impact on enhancing our current level of knowledge of observable insider behaviours. These major studies will be briefly described in this section, and specific content will be reinforced in the following sections of this report. Although the studies all revolve around the problem of insider threat, some focus more on the individuals responsible, and other studies focus more on preventative measures that may reduce the threat of an attack.

A retrospective study into insider threat was conducted by researchers at the CyLab at Carnegie Melon University (Cappelli et al., 2006). A team of researchers collected and coded 116 cases of documented insider threat attacks. They first divided the cases into the type of malicious insider activity, categorising the attack as fraud, IT sabotage or theft of information. Each type of attack was then further analysed by focusing on different aspects of the attack. This included gathering information about the insiders and factors that motivated them to commit the attack. Technical aspects, about how the attack was conducted, were also documented. Researchers also determined how each attack was discovered and how the insider was identified. Finally researchers measured the impact of the crime, including the financial and business outcomes and non-monetary consequences (Cappelli et al., 2006).

The authors of the report outline 13 practices that may prevent an attack from occurring or may lead to earlier detection. These practices involve the implementation of organisation wide policies that incorporate risk assessment and security training. A clear outline of security policies and practices is crucial and is supplemented by auditing and monitoring of employee computers and online activities. Using a multi-layered approach is encouraged, and in conjunction with technical strategies and education, it is also important to monitor employee behaviours, and to respond promptly and appropriately to suspicious behaviours. The recommended practices have been summarised in greater detail in following sections of the report. All of the practices are important since a combined strategy can prove to be a stronger tool against insider attacks (Cappelli et al., 2006).

A more recent study by Moore, Cappelli and Trzeciak (2008) was able to take the results of the study conducted by Cappelli et al. (2006) and delve further into the threat of insider IT sabotage. In this study, the authors outline seven predominant observations that were common in cases of insider IT sabotage. The first three observations relate directly to the psychological, behavioural and situational factors that were present, while the other observations are organisational and technical limitations that unintentionally helped to facilitate a successful attack (Moore et al., 2008).

Another study conducted by researchers at Carnegie Mellon focused on insider threat, specifically conducted within the IT and telecommunications sector (Kowalski, Cappelli & Moore, 2008). The study focused on the characteristics, motives and behaviours of the insiders and the consequences for both the insiders and the organisations. Some recommendations for the prevention of insider attacks for the IT industry were provided. This study was also retrospective in nature and was based on 52 documented attacks that occurred within the IT and telecommunications sector between 1996 and 2002 (Kowalski et al., 2008). The size of targeted organisations varied greatly. The majority of organisations had fewer than 500

employees (62%); however 30% were large organisations with over 10,000 employees. All of the organisations were private sector businesses. In half of the instances where intellectual property was stolen, the insider was employed by a company that had confidentiality policies in place (Kowalski et al., 2008).

The growing threat of the malicious insider has given rise to a number of long term research projects. Research conducted through The Personnel Research Centre (PERSEREC) has focused on the creation of an Espionage Database, in an effort to collect valuable information about specific espionage case studies (Fischer, 2008). Espionage is now viewed to be comparable to other illegal acts such as computer crime, embezzlement and corruption (Fischer, 2008). In fact, in financially motivated cases of espionage, the only difference may be that the actions may directly benefit a third party. Therefore, information concerning cases of espionage may be highly relevant to cases pertaining to insider attacks and vice versa; it is hypothesised that there are many similarities between these two populations of individuals (Fischer, 2008). The aim of this data collection was to better understand motivations and personal characteristics, and to gauge reliable predictors of such behaviour (Fischer, 2008). The Community Research Centre, located in Virginia, has also conducted similar research, under the name 'Project Slammer'. This project employs a qualitative research approach to explore why people commit acts of espionage. It is through interviews with perpetrators that researchers are able to delve into a variety of factors including personality, behavioural and situational variables (Fischer, 2008).

This report aims to bring together the findings from a variety of perspectives on the insider threat problem. Despite some very diligent research efforts, insider threat remains an area of research that still holds many unanswered questions and warrants further investigation. Details of these particular studies will now be expanded upon in following sections of this report.

2. Profiling and Detecting Insider Attacks

The complex and dynamic structure of organisations makes profiling of insider threats more difficult. For example, organisations consist of full-time and part-time employees; there are also contractors, temporary employees, consultants and partners, along with former employees, who still may have access to information and systems (Shaw et al., 1998). This has two major implications for profiling insider threats. First, the loyalty expressed by these groups may differ. Second, the processes used to hire individuals from these groups may also vary greatly, particularly in regards to the levels of background checks conducted. Therefore, it is fair to assume that these groups may experience different motivators when it comes to insider attacks (Shaw et al., 1998).

Kowalski and colleagues (2008) concluded that age, race and ethnic background varied widely among insiders. However, although there was no one profile that could best describe an insider, there were certainly some distinct characteristics that emerged from their case studies. For example, insiders were predominantly male, most were single at the time of the attack and had not previously been married, and 38% had a prior arrest on their record. Approximately half of the insiders were current employees at the time of the attack and half were previous employees. The majority of insiders were employed in technical positions within their organisation (Kowalski et al., 2008). Interestingly, the Association of Certified Fraud Examiners' (2008) study of occupational fraud found that the vast majority of offenders did not have previous convictions.

Cappelli et al. (2006) explored three types of insider attacks, namely, fraud, IT sabotage and theft of information. Although the three types of attacks occurred with similar frequency, it was discovered that the profiles of the individuals who committed these attacks did differ across the type of attack. For instance, incidents of fraud were largely committed by employees who used their own passwords and usernames, and there was an equal distribution of male and female offenders. System irregularity most commonly alerted the organisation to a problem and system logs were used to trace the offender (Cappelli et al., 2006).

In the cases where confidential information or proprietary information was stolen, the majority of attackers were current employees. However, one third of this group consisted of previous employees that were still able to access the network. Importantly, over 50% of these individuals held technical positions within the organisation (Cappelli et al., 2006). In fact, cases of IT sabotage were generally orchestrated by male employees who held technical positions. They used highly sophisticated techniques that were only detected as a result of system failure or system irregularity, and once again, system logs had to be used to identify the perpetrators (Cappelli et al., 2006).

A significant portion of the research has an emphasis on insider attacks instigated by IT specialists. This group is of particular interest given their high level of expertise; they usually have system administrator or privileged access, and therefore, they are a group of individuals that require close monitoring because of their knowledge and skills base (Moore et al., 2008).

A particular focus will be placed on this group of insiders as part of the following sections of this report.

2.1 Observable Behaviours

The information gathered by Kowalski et al. (2008) does suggest that insider attacks occur after careful consideration and preparation, with the majority of insiders planning their attack in advance. This research indicated that, in the majority of cases, behavioural warning signs were observable prior to an attack.

Observable behaviours of concern included absenteeism, arguments with co-workers and poor performance, and in 70% of cases, individuals were actually reprimanded for inappropriate behaviours in the workplace (Kowalski et al., 2008). Kowalski and associates (2008) recommend that in these situations access rights should be reviewed for individuals who are displaying any behaviour that is deemed to be threatening to the security of the organisation. This response may prevent the successful completion of an attack.

A significant behavioural warning sign, which was present in 52% of insider cases, was the presence of noticeable online activities (Kowalski et al., 2008). These activities included sabotaging backups, creating false client accounts and downloading malicious code or materials (Kowalski et al., 2008). Many of these online activities could have been detected by automated security programs and through logging, monitoring and auditing of employee's online actions. The challenge in this instance was that over half of the insiders possessed a high level of technical skills making them harder to detect. However, the prevalence of this behaviour does highlight the importance of increased monitoring, particularly of individuals with high technical skills and administrative and privileged access (Kowalski et al., 2008).

Another vulnerability that is commonly observed in insiders is computer dependency. Computer dependency is defined as an addictive attachment to a computer system (Shaw et al., 1998). An individual who is dependant on their computer will spend a significant amount of their time on their computer and this behaviour interferes with everyday lives and social interactions. It is an observable behaviour that may alert an organisation to a potential problem.

Interestingly, Kowalski and colleagues (2008) provided a breakdown of time and location of when insider incidents were executed, and in 43% of cases, remote access from outside the workplace was used to commit a malicious act. What is of great concern is that, of those individuals who used remote access, 88% of them were former employees. This means that the organisations failed to disable all access following termination. Having an appropriate and detailed procedure in place to deactivate all access points may have significantly reduced the chances of an attack from a previous employee (Kowalski et al., 2008).

In these examples, the majority of cases were only detected due to system failures and irregularities. In fact, 74% of cases were discovered not by security staff, but by other employees, supervisors and even customers. After the identification of an attack, system logs were predominantly used to identify the responsible individual (Kowalski et al., 2008).

Research has also found that in a staggering 46% of cases, other individuals had some degree of knowledge and information about an imminent attack (Kowalski et al., 2008). This included co-workers, acquaintances, family members and friends. Often individuals failed to acknowledge the seriousness of any statements of intent or threat, and unusual behaviours were often dismissed. In other words, warning signs were observed but they were not acted upon. This is why appropriate and detailed education programs are a necessity. Once employees are given the knowledge and information about what to do when they observe such behaviours, they are empowered to act appropriately (Kowalski et al., 2008). Similar findings and conclusions were reached by researchers working on Project Slammer. It was observed, in their research cases, that there was often either an inability for other employees to identify an *at risk* colleague, or alternatively, employees had noticed *at risk* behaviours, but failed to act on these behaviours (Fischer, 2008).

This theme of an inability to act on observable risk behaviours was also communicated in the study conducted by Moore and colleagues (2008). Their research focused specifically on IT insiders and they determined that although many behavioural precursors were observed in insider IT sabotage cases, they were largely ignored by the organisation. In fact, in a staggering 97% of cases, management was fully aware that the employee was displaying behaviours that were serious and of great concern. Despite this knowledge, no action or formal process of mediation was undertaken to intervene prior to an attack (Moore et al., 2008).

Therefore, as a preventative measure, Fischer (2008) suggests that organisations have appropriate programs in place to assist vulnerable employees. If employees are experiencing any form of personal crisis or difficulty, it is recommended that employees are encouraged to use Employee Assistance Programs. The feedback provided by the perpetrators of acts of espionage delivered the strong message that early intervention may have prevented the act occurring in the first instance (Fischer, 2008).

A very pertinent reoccurring theme during the Project Slammer interviews was the decision by individuals to commit these acts because they knew that the probability of being reported by a co-worker was negligible. This finding emphasises the importance of co-worker responsibility and educating staff about potential warning signs and observable behaviours that should be reported in an effort to facilitate early intervention (Fischer, 2008).

In support of this, the findings of the Project Slammer study suggest a relationship between personal stress and risk of attack; they also lend support to the connection between adverse social climate and the heightened risk of attack (Fischer, 2008). What is being strongly suggested to organisations is the need to be aware of disgruntled employees and to provide immediate management intervention at the very first observable sign of discontentment (Fischer, 2008).

The findings of these studies support the necessity to be alert and responsive to unusual and unexpected behaviours and actions, and to be able to act decisively on these observable warning signs. This recommendation is strongly dependant on having a training program that gives employees the tools to be able to effectively detect behavioural precursors (Kowalski et

al., 2008). Subsequent sections of this report will elaborate in greater detail on the strategies that can be used to achieve these goals.

2.2 Motivating Factors

It is important to try to understand why certain individuals commit insider attacks, and a number of studies have explored the motivating forces driving these illegal behaviours.

Research conducted by Kowalski et al. (2008) investigated the motivations of insiders and, although there were multiple motivating factors, the strongest was revenge (56% of cases). Other motivating factors included financial gain, dissatisfaction with company policies, and a desire to take information to a new place of employment. The primary goals of insider attacks were sabotage (47%), along with financial gain and theft of information and property (42%).

Some of the insiders who stole confidential or proprietary information were also disgruntled and motivated by revenge (Willison, 2009). However, this particular group were more likely to be financially motivated. They also often felt that they were entitled to the information. This was particularly evident for insiders who were either changing jobs or were starting their own businesses (Cappelli et al., 2006).

The most perplexing group of insiders were those who committed acts of fraud. Cappelli et al. (2006) found that although some of these individuals were motivated by money, debt and drug related problems, the vast majority of them did not have a financial need, nor were they disgruntled or dissatisfied with their employer. Therefore, their motivation remains unclear and difficult to categorise and understand.

As mentioned previously, a large proportion of research focuses on IT insiders, who often have different motivations. A motivating factor that was particularly evident for IT insiders was a feeling of disgruntlement that resulted from unmet expectations. An individual's expectation may not have been met in various areas of their employment. For example, this may include poor relationships with co-workers, lack of promotion or demotion and diminished responsibilities. It was also observed that a high proportion of IT insiders (84%) were also motivated by revenge (Moore et al., 2008). The theme of revenge was also observed in the Cappelli et al. (2006) study. A number of insiders who committed IT sabotage were motivated by revenge following a negative incident. These negative incidents included termination, demotion and disputes with employers. In addition to this, Moore and colleagues (2008) observed that the individuals' environment and current personal situation had a strong motivating impact. In many of their case studies, stressful events, such as the imposition of organisational sanctions, contributed to the subsequent act of insider IT sabotage. In fact, the majority of cases of IT sabotage occurred as a direct result of employment suspension or termination (Moore et al., 2008).

Most of the insiders did not seem to grasp the severity of their actions and were not prepared for the consequences of their behaviour. Formal criminal charges were laid in 90% of cases, and punishments included jail time, probation and financial restitution. Of course, other losses were incurred, including termination of employment, the stigma of a criminal record, travel restrictions and computer restrictions (Kowalski et al., 2008).

The literature indicates many similarities between individuals who commit espionage and those who commit insider attacks. The creation of the Espionage Database has resulted in the collection, coding and statistical analysis of 117 cases of espionage, and as part of the analysis of these case studies, researchers have looked at motivations for espionage (Fischer, 2008).

Motivations were linked to whether the individual was a volunteer or a recruited offender. Many volunteers were financially motivated, and this is despite the fact that very few actually received any substantial amount of monetary compensation. Financial compensation was low and often non-existent; this was because the espionage was either detected prior to any exchange of money, or because the money was due to be paid over an extended period of time. For the individuals who were recruited, particularly those who were recruited by family or friends, the major source of motivation was the desire to satisfy or please. Other sources of motivation included ideology (including political ideology), coercion, intrigue and also a desire for revenge (Fischer, 2008). These motivators are comparable to those observed in insider attacks.

2.3 Personality Traits

Many insiders exhibit personal predispositions that contribute to their risk of committing insider attacks. What this means is that there are observable personality characteristic that may be common to individuals who commit malicious acts and comparatively rare in other employees (Moore et al., 2008). The identification of these characteristics suggests that, with further research, they may be used to predict future malicious attacks.

Moore et al. (2008) outline three primary predispositions. First, serious mental health disorders, such as panic attacks and drug and alcohol addictions. Second, individuals may also display inappropriate social skills, such as bullying and poor hygiene. This is in conjunction with poor decision making strategies, which are often observed in individuals that have difficulty conforming to workplace rules and expectations. Third, insiders often present with a history of rule violations, which may range from the misuse of organisational resources to multiple arrests (Moore et al., 2008).

Personal and cultural vulnerabilities are also outlined by Shaw et al. (1998) in an effort to try to present a profile of malicious insiders. Although further empirical research and analysis is needed to confirm these variables, they do indicate patterns of personality and vulnerability that warrant further investigation. The personal and cultural vulnerabilities that have been identified include introversion, social and personal frustrations, ethical flexibility, reduced loyalty, entitlement and lack of empathy. It is suggested that the combination of several of these factors should alert employers to a potential danger (Shaw et al., 1998).

Computer specialists who commit insider acts tend to be introverted individuals (Pocius, 1991). Introverts are individuals who are reserved, prefer solitary activities and are less assertive in social situations. Approximately 40% of the general population can be classified as introverted individuals. It is a trait that is prevalent and over represented in computer technology specialists and therefore it is not a characteristic that on its own indicates that an

individual may be an insider (Pocius, 1991). Instead, combined with other factors and behaviours, it may indicate a vulnerable subgroup (Shaw et al., 1998).

Social and personal frustrations are frequently observed in insiders. Insiders display a history of conflicts with family members, peers and co-workers, and because of their social history, they prefer the structure and predictability of working with computers as opposed to working with people (Coldwell, 1993). These social experiences mean that these individuals may become isolated and less socially skilled. This in turn can create an inclination towards anger, which can lead to disgruntlement, and disgruntlement has been shown to be a powerful motivator for insider attacks (Shaw et al., 1998).

Ethical flexibility is a term used to describe a code of ethics that is observed in the information security culture. Ethical boundaries are often much less stringent and more elastic within this subgroup of IT specialists. The philosophy of this subgroup is essentially that if an information system is not appropriately secured, then they are entitled to access that system (Shaw et al., 1998).

Interestingly, this paradigm is more evident in younger age brackets, which suggests a generational change in thinking and may become more of an issue as younger employees enter into the workforce. It has been hypothesised that a lack of appropriate ethical training specific to computer usage is a contributing factor to this behavioural trend. The authors also strongly suggested that mixed messages from the information security industry itself are of grave concern. The industry is well known for hiring former hackers in esteemed positions which clearly communicates to the younger generation that hacking behaviour may be an incentive for future job opportunities (Shaw et al., 1998).

In relation to this issue reduced loyalty is another observable trait. A high demand for computer skills, coupled with high turnover rates has contributed to a lack of loyalty shown to an employer. It has been observed that, although some computer professionals are loyal to the employer who pays them for their work, other computer professionals are loyal to their profession. A lack of loyalty may confound tension within the work environment and this can, at times, generate a great deal of conflict that may make an individual vulnerable to committing an attack (Shaw et al., 1998).

A sense of entitlement, in conjunction with anger directed at authority, is also present in many cases of insider attack. This strong sense of entitlement is often observed alongside the perception that employers and colleagues fail to acknowledge and affirm their exceptional skills. This combination results in feelings of entitlement that are used to justify consequent behaviours and actions (Shaw et al., 1998).

This sense of entitlement is often associated with individuals who have Narcissistic Personality Disorder. According to the Diagnostic and Statistical Manual of Mental Disorders (American Psychiatric Association, 1994) individuals who are diagnosed with Narcissistic Personality Disorder display an excessive sense of self importance. There is an observed pattern of grandiosity and a strong need for admiration, and this is coupled with a lack of empathy. Although the aetiology of this disorder is unknown, these patterns of behaviour are observed by early adulthood. It is important to understand that these traits are also observed

in normal development and they appear along a spectrum of severity, and vary from one individual to another. Therefore, an individual may display elements of narcissism without meeting the criteria for a diagnosis of Narcissistic Personality Disorder.

As explained, a common trait of individuals with narcissistic personality is a lack of empathy, which is the final personal vulnerability described by Shaw et al., (1998). A lack of empathy presents a recurring theme in many individuals who have committed insider acts; these individuals seem unable to consider the implications of their actions on others (Shaw et al., 1998).

As previously mentioned, research suggests that there are many similarities between individuals who commit acts of espionage and individuals who commit insider attacks (Fischer, 2008). Therefore, by looking at the personality predispositions of individuals who committed acts of espionage we may gain further insight and understanding of the personality traits observed in insiders. For example, in the case studies of individuals who had committed acts of espionage, a very high percentage of the individuals were substance abusers, with drug or alcohol addictions (Fischer, 2008).

Fischer (2008) describes the data collection process that was used for each of the case studies. As part of this data collection process, a substantial amount of time was spent gathering information about childhood experiences and behaviours. The aim of this approach was to enrich our understanding of psychological and emotional development, in conjunction with mental health (Fischer, 2008).

The psychological testing and interviewing process conducted during Project Slammer has revealed two types of offenders (Fischer, 2008). One type of individual is described as manipulative, dominant and self-serving, and the other in total contrast is described to be passive, easily influenced and with very low self-esteem. Many of these personality characteristics are similar to those presented in the insider threat research domain, and they include selfishness, lack of empathy and lack of loyalty (Fischer, 2008). Hence, although there are many differences between the two populations, they also have certain characteristics in common.

Of course individuals may display these personality traits and predispositions without committing an insider attack or an act of espionage. What we really need to know is what makes individuals who commit an offence different from those who do not. Researchers have observed that these individuals tend to be psychologically vulnerable, and often display impaired judgement in highly stressful situations (Fischer, 2008). Many were victims of child abuse and suffered severe self-esteem problems, while others were never taught about moral boundaries or did not experience positive role models. This is certainly a complex issue and a definitive answer will continue to elude researchers for some time, but the hope is to be better able to identify at risk individuals to facilitate more rapid and effective intervention strategies (Fisher, 2008).

2.4 Technical Factors

Evidence also suggests that organisations were not only overlooking behavioural warning signs, but were also failing to detect technical indicators of malicious activity (Moore et al., 2008). Basic computer security was not being maintained and this included not creating backups, and failing to monitor internet access and downloads. In some instances individuals were downloading and using specific hacker tools at work. In an astounding 87% of cases, evident technical precursors were not detected (Moore et al., 2008).

A pattern of behaviour was observed with IT insiders. This group would often create their own access paths to initiate an attack, and to conceal their identity (Moore et al., 2008). In most instances, they would then use these access paths to attack after termination. This observation highlights the importance of very stringent and responsive security measures pertaining to terminated employees. In these cases of IT sabotage, 59% were conducted by previous employees (Moore et al., 2008).

A recurring theme that organisations need to take very seriously is electronic and physical access controls. It was found that a lack of electronic and physical access controls facilitated cases of IT sabotage. In fact, in 93% of cases the insider took advantage of this lack of security (Moore et al., 2008). Further information pertaining to access controls can be found in Parsons, McCormac & Butavicius (2009).

A high proportion of insider attacks can be detected and intercepted much earlier if organisations are willing to implement certain strategies and procedures. These will be described in detail in the following sections.

3. Preventative Measures

There are many potential indicators of internal attacks, and evidence suggests that no single indicator provides a conclusive warning of a likely attack (Schultz, 2002). Generally speaking, the methods of detecting and preventing insider attacks can be categorised as personnel related measures, policy related measures and technical measures. These measures will be detailed in this section.

3.1 Personnel Related Preventative Measures

Within organisations employees play a vital role in information security. Therefore, individual behaviours and actions can have strong repercussions in mitigating the insider threat.

3.1.1 Suspicious behaviours

As detailed in the previous section, there are certain behaviours that may provide an indication of a possible threat. Therefore, it is necessary to be aware of changes in behaviour, specifically any erratic or out of character behaviours or any overt signs of stress (Shaw et al., 1998).

Employers need to be especially attuned to any financial problems that their staff may be experiencing as these can precipitate an attack. This is particularly important because research has shown financial gain to be a strong motivating factor in some cases of insider attack (Kowalski et al., 2008).

All staff should be encouraged to be vigilant and attentive to any threats that other employees may make against the organisation. Any threats or boasts that individuals may express concerning harm to the company should be treated seriously and investigated (Cappelli, Moore, Trzeciak and Shimeall, 2009).

Given that feelings of disgruntlement often precipitate an attack, formal processes should also be in place to deal with any grievances that may arise. It is crucial to ensure that these grievances are not allowed to fester and become a greater issue than they are, as this too may trigger an attack motivated by revenge (Cappelli et al., 2009).

Individuals will usually provide behavioural cues that indicate an imminent attack, but they will also often leave deliberate technical markers to make a statement. Therefore, it is also important to be alert for any indicators of this nature (Schultz, 2002). These specific behaviours can often be detected using technical strategies and will be discussed in following sections of the report.

What is evident is that in certain instances, network access rights need to be reconsidered and revoked for any employees who are being disruptive or who pose a viable security risk (Cappelli et al., 2009).

3.1.2 Security awareness training

Compulsory security training packages, provided to all employees, need to be reviewed periodically by the training team responsible for their content and administration. This training also needs to be reinforced on a regular basis (Wilson & Hash, 2003). The training should cover all aspects of computer security, paying close and specific attention to insider threat. According to Warkentin and Wilson (2009), organisations should have a strong emphasis on training and motivating employees to act securely.

Employees need to be made aware that insiders may use social engineering strategies in an attempt to gain information to help enable a malicious act. Parsons et al. (2009) provide a comprehensive review of current research in social engineering. They describe how social engineering attacks are orchestrated, what makes individuals susceptible to attacks, and the strategies that are used by perpetrators to increase susceptibility. Along with this information, the authors describe how organisations and individuals can defend against attacks, and how education and training can be used to specifically combat the problem (Parsons et al., 2009).

Employees also need to understand that there is certainly no one profile to describe insiders. Rather employees ought to receive descriptions and examples of what behaviours and personality predispositions they should treat cautiously and with suspicion (Cappelli et al., 2009). Case studies have been shown to be a very effective tool in communicating a message and leaving a lasting impression (McIlwraith, 2006). These behaviours and personality traits have already been discussed in previous sections of this report, and they include such factors as conflicts with co-workers, poor performance, computer dependency and drug and alcohol abuse to list just a few.

Once employees are able to identify behaviours and activities of concern, their training also needs to incorporate detailed procedures for reporting these suspicious behaviours or activities. As part of this process confidentiality needs to be ensured to encourage staff to communicate any concerns (Cappelli et al., 2009).

Training should not only focus on how to identify a possible insider, but it should also incorporate general information about individual behaviours that can improve the overall and everyday computer security within the organisation (Cappelli et al., 2009). An increase in information security will lead to an increase in security specific to the insider threat. For more information on security awareness and training see Parsons et al. (2009).

3.1.3 Restriction of Access

Security awareness and training provides a solid foundation for education. However, to make it more difficult for insiders to commit a malicious act, organisations can restrict access to employees via mechanisms such as separation of duties and least privilege (Cappelli et al., 2009).

Separation of duties occurs when tasks need to be completed by two or more employees; each employee is responsible for ensuring that procedures and practices have been completed

correctly. This practice is likely to be effective given that research has shown that insiders are more likely to act alone in committing an attack (Cappelli et al., 2009).

The principle of least privilege is quite simple; it involves restricting employees to only have access to the resources that they require to complete their defined roles and responsibilities. This means restrictions in both technical and physical access to resources. By enforcing this principle, organisations can limit the potential damage that may occur as a result of an insider attack (Cappelli et al., 2009).

3.1.4 System administrators and privileged users

Extra caution and surveillance needs to be applied to system administrators and privileged users. These individuals are technically more advanced and experienced than other employees, and their technical knowledge means that they are able to hide their actions, making it harder to detect a threat (Kowalski et al., 2008). They are able to use more sophisticated methods of committing an insider attack, such as using backdoor accounts, changing system logs, creating viruses and using logic bombs (which are computer viruses that remain hidden until they are activated by predetermined conditions) (Cappelli et al., 2009).

Separation of duties is crucial for this group of employees. It is also suggested that as an extra precaution sensitive files should be encrypted to ensure that access will be granted only when it is appropriate. Finally, extra precaution is required when a system administrator or a privileged user either has their employment terminated or resigns. All access needs to be promptly disabled and the process needs to be well documented to ensure that no access point has been overlooked (Cappelli et al., 2009).

3.2 Policy Related Measures

Research also suggests that appropriate policies and procedures can minimise the likelihood of insider attacks (Kowalski et al., 2008). Organisations should create a document that clearly outlines all policies and procedures pertaining to insider threat controls (Kowalski et al., 2008), and all employees should have a copy of the document. This document should detail the behavioural warning signs and technical indicators associated with insider threats. Furthermore, the policy should also specify formal procedures for recording and responding to insider threats (Kowalski et al., 2008).

Cappelli and colleagues (2009) also recommend that all employees officially acknowledge and sign that they have read the document and are aware of the consequences of any behaviours that violate stated policies and procedures. This document should be incorporated as part of the ongoing and periodically reviewed information security training sessions.

Implementing effective policy and procedures can be very powerful as it can communicate a strong commitment to computer security and can therefore act as a strong deterrent. Individuals are less likely to pursue an action where there is a high possibility that they will be caught. A proactive organisation will undoubtedly reduce the risk of becoming a victim of an insider attack (Cappelli et al., 2009).

3.2.1 Password management

Related to this, Cappelli and colleagues (2009) also suggest that organisations should implement strict password and account management policies and practices. This should reduce the likelihood that employee accounts can be compromised, and should therefore ensure that the threat of unauthorised access is minimised. To ensure that employees are obeying these policies and practices, it is necessary to log and monitor the system.

It is also necessary to educate employees regarding how to select a strong password; they should be aware that they need to change their passwords on a regular basis, and they should ensure that their workstations are locked when they are away from their computer. Most importantly, employees should be aware that they should not share their password under any circumstances (Cappelli et al., 2009). It is, however, vital to ensure that employees' work practices are taken into account. Procedures that are not developed with an emphasis on usability are likely to result in low security motivation and insecure work practices (Adams & Sasse, 1999; Parsons et al., 2009).

3.2.2 Employee access

As alluded to earlier, a vast number of insider threat attacks are perpetrated by former employees (Cappelli et al., 2009). Hence, it is extremely important to ensure that all computer access is promptly deactivated when an employee leaves. Since research has indicated that revenge is often a primary motivation for computer sabotage, the deactivation of accounts is particularly important in situations where an individual's employment has been terminated (Cappelli et al., 2009). This procedure needs to be detailed, up to date, and clearly specified so as to not overlook any potential access points (Kowalski et al., 2008). This includes remote access accounts and shared accounts. It is also important to disable the employees' access to all points before they are notified of their termination (Moore et al., 2008). Once system access has been removed, the organisation is also responsible for ensuring that physical access to all premises has been disabled.

Similar policies and procedures should also be in place for the demotion or transfer of employees (Moore et al., 2008). It is important to examine the roles and responsibilities of all employees to ensure that access controls and authorisation levels remain appropriate. Such policies can, in fact, act as a deterrent against insider attacks (Moore et al., 2008).

3.2.3 Risk assessments

To minimise the likelihood of insider threat attacks, organisations are also urged to conduct an enterprise wide risk assessment (Cappelli et al., 2009). This risk assessment will facilitate the identification of essential organisational assets that need to be protected. These may include sensitive information, such as financial data, employee and customer data, and confidential and proprietary information. Once the crucial assets have been identified, the next step is for organisations to determine both the external and the internal threats to those assets (Cappelli et al., 2009).

It is important to note that an enterprise wide risk assessment is an ongoing process that needs to be reviewed periodically. This is vital because, as organisations change and develop, so does information technology, which in turn results in changes to the threats to valuable assets (Cappelli et al., 2009).

3.2.4 Hiring policy

Finally, since evidence indicates that many insider attacks are committed by employees with a previous criminal record, it is also necessary for organisations to be vigilant and committed to having a comprehensive and detailed hiring policy (Theoharidoua, Kokolakisb, Karydaa & Kiountouzisa, 2005; Reid & Gilbert, 2007). To increase the possibility that the right individuals are hired to fill positions, an organisation needs to conduct thorough background checks, including checks for any criminal convictions (Cappelli et al., 2009). By conducting detailed checks, employers have a greater understanding of the character and personality of any potential employees.

Once an individual has been employed by an organisation, a substantial amount of time should be devoted to training and educating the new employee regarding security policies and procedures (Cappelli et al., 2009). Particular attention should also be focused on explaining the consequences of behaviour. Employees need to be clear as to the consequences should they fail to comply with security expectations. However, it is important to not only monitor the behaviour of new recruits, but to also be vigilant in observing the behaviours of all staff.

3.3 Technical Measures

Given that there are numerous technical precursors that have been observed in insider cases it is important to ensure that technical knowledge and skills are integrated into preventative strategies. These technical measures, especially when combined with personnel and policy measures, can act as an effective deterrent against insider attacks.

3.3.1 Technical Safeguards

Many organisations do have strong firewalls and antivirus software in place to guard against outsider attacks, but for many organisations increased security is required to protect against insider attacks. To facilitate this, organisations are encouraged to catalogue software and hardware configurations (Cappelli et al., 2009).

This catalogue system can be used in conjunction with file integrity checkers, which automatically check systems. This will assist in identifying anything unusual, and these unusual occurrences can then be investigated to determine if they are malicious in nature. These recommendations require continual updating as computer configurations and software are constantly changing (Cappelli et al., 2009).

3.3.2 Auditing of online activity

It is by logging, monitoring and auditing employees' online activities that organisations are able to detect the early warning signs of an imminent threat. If employees are informed that the organisation will conduct both regular and random checks of their computer activities this information may in itself act as a strong deterrent to some individuals (Cappelli et al., 2009). However, Schultz (2002) states that it is important to minimise reliance on this, as many insiders have the ability to disable or otherwise interfere with any auditing measures.

3.3.3 Restrictions on remote access

There is debate as to whether remote access should even be an option for organisations serious about eliminating a vast range of security threats (Cappelli et al., 2009). Conducting an attack is certainly much easier for an insider when it is done in the privacy of their home than at work with the constant threat of someone discovering what they are doing.

In circumstances where remote access is necessary it is suggested that organisations limit the amount and type of information that can be accessed from outside the workplace (Cappelli et al., 2009). Strict regulations are also needed to limit remote access to only those individuals who require the access to fulfil their job requirements. Remote access accounts do need to be more closely monitored and logs checked on a regular basis. This is much easier to manage when only a limited number of individuals have been approved to use remote access in the first instance (Cappelli et al., 2009).

3.3.4 Maintain evidence of an insider attack

In the event of an attack, it is essential that information and equipment be collected and maintained as evidence of an illegal activity. It is crucial to ensure that accurate logs of information are maintained from various sources in conjunction with phone records and physical access records (Walker, 2008). If an insider attack is identified it is recommended that experts be contacted to conduct a through investigation (Cappelli et al., 2009).

3.3.5 Backup and recovery processes

All necessary steps should be taken to ensure that the organisation has sufficient and secure backup of all critical information along with tested recovery processes (Cappelli et al., 2009). This is of course a practice that needs to be reviewed often to ensure that information and processes are current. Multiple copies stored at different off site premises may in fact deter attackers. The consequences of an attack would be minimal provided that operations could be quickly and efficiently restored and resumed (Cappelli et al., 2009).

4. Further research and recommendations

Of the research reviewed in this report, very little has been based in Australia. In addition, the international research into the human factors of malicious insiders is still in its infancy. To address these issues, this section outlines avenues for future research into malicious insiders.

4.1 Incident response team

After a malicious insider has been detected, there is normally a fast technical response to the attack. For example, an investigation is launched into what the attacker did, what systems were affected and how, if possible, the damage might be contained. However, an analysis of the underlying psychology of the attacker, their background and their observed behaviours before and during the attack is normally only investigated, if at all, long after the attack has occurred. In addition, such investigation is normally only conducted as part of an academic exercise and is not part of the official government response to the incident.

This deficiency could be rectified via the implementation of an incident response program, whereby a specialist government response team investigates the attacker and their background immediately after the incident. This investigation would take the form of interviews with the attacker, their co-workers and other friends, as well as psychological testing and profiling as appropriate. In many instances interviewing the attacker may be difficult as they would be unlikely to want to incriminate themselves prior to the conclusion of any associated legal proceedings. However, a great deal of relevant information may be gathered from other individuals. Part of this process could be likened to a security vetting procedure; however, it would be deployed on all malicious insider attackers, and not just those who may have already undergone a high level security clearance.

This type of investigation could provide vital information into the social and psychological background of malicious insiders in Australia. Furthermore, it could also identify triggers and behavioural warning signs that could, in future, prevent a similar attack on government networks. This investigation would run in parallel with, and would complement the findings of, the technical assessment of the insider's attack.

4.2 Analysis of known attacks in Australian government agencies

Previous attacks against Australian government agencies could also be assessed. In the first place, this would take the form of interviews with senior management and technical and security staff of government agencies, where malicious insider attacks or other critical incidents have occurred. This first series of interviews may also lead to further interviews with the staff who worked directly with the attacker at the time of the incident and, where possible, interviews with the attackers themselves.

At the present time there has been no known systematic analysis of such incidents in these organisations. The purpose of this type of investigation is to first, reveal insights into the psychological and behavioural factors associated with the attack, and second, to examine the organisational factors that may have impacted on its success. This research would be conducted in a confidential manner, and although general, unclassified findings would be presented to a wider audience, specific findings at the security-in-confidence level would be fed back to senior management of the organisation involved.

4.3 Empirical study of the psychology of malicious insiders

The research cited in this report, which looked at the psychological factors behind malicious insiders, was based on interviews and the application of psychological theory to the problem of profiling insiders. However, there is very little research in the existing literature looking at specific psychological profiling and psychological factors.

A dedicated research initiative, such as a key centre or centre of excellence involving both public and private sector organisations may prove to be beneficial. The aim of such a proposed key centre would be to investigate, in an empirical manner, the psychology of malicious insiders. This research would draw, initially, on the areas of forensic psychology, especially as it relates to white-collar fraud, before progressing to controlled studies on personality and cognitive factors of malicious insiders. This research program could also be extended to look at general human factors issues surrounding information security behaviours. This research program would run in parallel with the interview-based incident analyses and could complement these findings.

5. Conclusion

In conclusion, insiders pose a serious and sobering threat, costing organisations hundreds of thousands of dollars in lost revenue. This is a challenging problem to define and study. Insiders cannot be easily profiled and insider attacks are often difficult to detect with incidences usually only uncovered 18 to 24 months after they occur.

However, despite these difficulties this report has detailed strategies and techniques from the existing research literature to not only identify potential insiders, but to also combat and reduce the insider threat to an organisation. Simply put, there are a number of observable behaviours, motivating factors, personality traits and technical factors that can reveal a possible and imminent threat.

In combination with these, there are specific strategies that can successfully prevent or warn of a likely attack. These preventative measures can be grouped in three major categories. The first category relates to personnel related tactics, such as security awareness training. The second category consists of policy related measures, such as conducting regular risk assessments and abiding by strict hiring regulations. The final category consists of technical measures, such as auditing employee activities and restricting remote access.

A combination of these approaches, together with strategies to detect vulnerable individuals is highly recommended. Without this line of attack an organisation is knowingly taking a risk that has serious and far reaching consequences.

This report has also proposed a number of initiatives that may be implemented to further investigate, predict and prevent malicious insider attacks. These involve the formation of a joint government and academic research program, a study of the organisations, in the Australia government, that have been subject to such attacks, and the creation of a formal malicious insider response strategy. The aim of this response strategy would be to investigate such incidents from a psychological and social perspective, immediately after they occur. This would provide valuable and unprecedented insight into insider threats specific to the Australian organisational environment.

6. References

Adams, A. & Sasse, M.A. (1999). Users are not the enemy. *Communications of the ACM, 42(12)*, 41-46.

American Psychiatric Association. (1994). *Diagnostic and statistical manual of mental disorders* (4th ed.). Washington, DC.

Association of Certified Fraud Examiner (2008). Report to the Nation on Occupational Fraud and Abuse.

AusCERT (2006). *Australia Computer Crime and Security Survey*. Retrieved July 2009, from http://www.auscert.org.au/images/ACCSS2006.pdf

Bellovin, S.M. (2008). The insider attack problem nature and scope, In S. Stolfo, S.M. Bellovin, A.D. Keromytis, S. Sinclair, S.W. Smith & S. Hershkop (Eds.) *Insider Attack and Cyber Security: Beyond the Hacker (Advances in Information Security)*, Vol. 39, New York: Springer.

Cappelli, D. M., Moore, A. P., Trzeciak, R. F., Shimeall, T. J. (2009). *Common Sense Guide to Prevention and Detection of Insider Threats, Version 3.1*, Carnegie Mellon University/CyLab.

Cappelli, D. M., Moore, A. P., Shimeall, T. J., Trzeciak, R. F. (2006). *Common Sense Guide to Prevention and Detection of Insider Threats, Version 2.1*, Carnegie Mellon University/CyLab.

Coldwell, R. A. (1993) University students' attitudes towards computer crime. *Computer Society. 23*, 1–2, 11–14

Fischer, L.F. (2008). *Espionage: Why Does it Happen?* Retrieved June 2009, http://www.hanford.gov/oci/maindocs/ci_r_docs/whyhappens.pdf

Kowalski, E.F., Cappelli, D.M., and Moore, A.P. 2008. *Insider Threat Study: Illicit Cyber Activity in the Information Technology and Telecommunications Sector*. Joint SEI and U.S. Secret Service Report, January 2008.

McIlwraith, A. (2006). *Information Security and Employee Behaviour: How to Reduce Risk Through Employee Education, Training and Awareness*. Aldershot, UK: Gower Publishing Limited.

Moore, A.P., Cappelli, D.M., & Trzeciak, R.F. (2008). *The "Big Picture" of Insider IT Sabotage Across U.S. Critical Infrastructure*. CERT Technical Report, CMU/SEI-2008-TR-009, May 2008.

Parsons, K., McCormac, A. & Butavicius, M. (2009). *Human Factors and Information Security: Individual, Culture and Security Environment.* Manuscript submitted for publication.

Pocius, K.E. (1991), "Personality factors in human-computer interaction: a review of the literature", *Computers in Human Behavior*, Vol. 7 pp.103-35.

Porter, D. (2003). Insider Fraud: Spotting The Wolf In Sheep's Clothing. *Computer Fraud and Security, 4*, 12-15.

Reid, R.C. & Gilbert, A.H. (2007). Managing security from the perspective of the business executive, *Proceedings of the 4th annual conference on Information security curriculum development*, September 28-28, Kennesaw, Georgia.

Schultz, E.E. (2002). A Framework for Understanding and Predicting Insider Attacks, *Computers and Security, 21(6)*, 526-31.

Shaw, E.D., Ruby, K.G., & Post, J. M. (1998). The insider threat to information systems. *Security Awareness Bulletin, 2–98*, 27–46.

Spitzner, L. (2003). Honeypots: Catching the insider threat. *Proceedings of the 19th Annual Computer Security Applications Conference, IEEE Computer Society*.

Theoharidoua, M., Kokolakisb, S., Karydaa, M., & Kiountouzisa, E. (2005). The insider threat to information systems and the effectiveness of ISO17799. *Computers & Security 24(6)*, 472-484.

Walker, T. (2008). Practical management of malicious insider threat – An enterprise CSIRT perspective. *Information Security Tech. Report, 13(4)*, 225-234.

Warkentin, M. & Wilson, R. (2009). Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems, 18*, 101-105.

Willison, R. (2009). *Motivations for employee computer crime: understanding and addressing workplace disgruntlement through the application of organisation justice*. Working Paper No. 1, Copenhagen Business School, Department of Informatics.

Wilson, M. & Hash, J. (2003). *Computer Security: Building an Information Technology Security Awareness and Training Program*. Information Technology Laboratory National Institute of Standards and Technology, Gaithersburg, MD 20899-8933.

DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION
DOCUMENT CONTROL DATA

1. PRIVACY MARKING/CAVEAT (OF DOCUMENT)

2. TITLE

Preventing and Profiling Malicious Insider Attacks

3. SECURITY CLASSIFICATION (FOR UNCLASSIFIED REPORTS THAT ARE LIMITED RELEASE USE (L) NEXT TO DOCUMENT CLASSIFICATION)

Document	(U)
Title	(U)
Abstract	(U)

4. AUTHOR(S)

Agata McCormac, Kathryn Parsons and Marcus Butavicius

5. CORPORATE AUTHOR

DSTO Defence Science and Technology Organisation
PO Box 1500
Edinburgh South Australia 5111 Australia

6a. DSTO NUMBER	6b. AR NUMBER	6c. TYPE OF REPORT	7. DOCUMENT DATE
DSTO-TR-2697	AR-015-286	Technical Report	April 2012

8. FILE NUMBER	9. TASK NUMBER	10. TASK SPONSOR	11. NO. OF PAGES	12. NO. OF REFERENCES
2009/1090433/1	07/012	ASINFOSEC	28	24

13. DOWNGRADING/DELIMITING INSTRUCTIONS

To be reviewed three years after date of publication

14. RELEASE AUTHORITY

Chief, Command, Control, Communications and Intelligence Division

15. SECONDARY RELEASE STATEMENT OF THIS DOCUMENT

Approved for public release

OVERSEAS ENQUIRIES OUTSIDE STATED LIMITATIONS SHOULD BE REFERRED THROUGH DOCUMENT EXCHANGE, PO BOX 1500, EDINBURGH, SA 5111

16. DELIBERATE ANNOUNCEMENT

No Limitations

17. CITATION IN OTHER DOCUMENTS Yes

18. DSTO RESEARCH LIBRARY THESAURUS http://web-vic.dsto.defence.gov.au/workareas/library/resources/dsto_thesaurus.shtml

Human Factors, Information Security and Insider Threat

19. ABSTRACT

This report examines previous research on malicious insiders with particular emphasis on the social and psychological factors that may have influenced the attacker and their behaviours. This research also draws on corresponding studies into fraud and espionage in non IT scenarios. A range of preventative measures is presented that approach the problem from personnel, policy and technical perspectives. Given the relative scarcity of research into non-technical aspects of malicious insider attacks, further recommendations are also made to study the malicious insiders, involving both government and academic stakeholders. Such research has the potential to provide further preventative measures.