Insider Threat Behavior Factors: A comparison of theory with reported incidents

Asmaa Munshi
Curtin University
a.munshi@postgrad.curtin.edu.au

Peter Dell
Curtin University
p.t.dell@curtin.edu.au

Helen Armstrong
Curtin University
h.armstrong@curtin.edu.au

Abstract

Almost all organizations and sectors are currently faced with the problem of insider threats to vital computer assets. Internal incidents can cause more than just financial losses; the costs can also include loss of clients and damage to an organization's reputation. Substantial academic research investigating internal threats has been conducted. This paper examines a number of theoretical models drawn from academic literature to identify a set of factors that are thought to be behavior factors associated with insider threats. These factors are then critiqued using empirical evidence from reported incidents, resulting in insights into areas where the theoretical perspectives of academic literature are both supported and unsupported by actual case evidence. The paper concludes with recommendations for future research directions for academic researchers.

1. Introduction

The threat posed by organizational insiders continues to be one of the main issues facing organizations and governmental institutions across critical infrastructure sectors. Internal threats have been recognized as a security problem since the 1980s [11]. Damage from internal sources is one of the most serious problems organizations face, and it is difficult to overcome [6]. This threat is associated with authorized users who abuse their privileges in ways that can cause major damage or loss to a company [38]. All employees can cause possible internal damage in some form; however, trusted employees have the most potential to harm the organization, through damage to the accumulated information or by destabilizing the operation system [27]. Some computer investigators have classified the insiders into four categories: traitors, who have a malicious intention to harm or destroy their organization; zealots, who believe that the organization is being badly run; browsers, who are curious to know everything even if it causes damage to the organization; and the well-intentioned, who are characterized by a lack of concern, and who damage the organization by downloading untrustworthy documents and/or by not activating their virus protection software [25].

Regardless of which category insiders belong to, they are better placed to harm their organizations than external agents. Insiders can avoid physical and technical security systems which are designed to prevent attacks [5]. Even though insider attacks may occur less frequently than outsider attacks, insiders have a high impact on information, as they are familiar with their targets and the security measures in place [11]. Most of the research reported on insider threats covers the problem from the researcher's individual perspective, focusing on one primary problem seen as either a technical or human factor. A recent study however, indicated that successful protection against internal threats relies on both technical and behavioral solutions [37].

Chinchani et al. define insiders as "*legitimate users who abuse their privileges, and given their familiarity and proximity to the computational environment, can easily cause significant damage or losses."[6]* Althebyan and Panda define the insider as an "*individual who has the knowledge of the organization's information system structure to which he/she has authorized access and who knows the underlying network topologies of the organization's information systems"* [1]. Another definition, given by Keeney et al. [29] states that *"internal threats are those executed by a current or former employee or contractor that intentionally exceeds or misuses an authorized level of access to networks, systems, data, or resources to harm individuals and/or an organization"*.

This study will define insider threats as *the potential harm posed by any trusted entity with inside access to the organization*. Each trusted entity will have a different level of trust assigned, appropriate to their position and role. Each trusted person will be

978-0-7695-4525-7/12 $26.00 © 2012 IEEE
DOI 10.1109/HICSS.2012.326

influenced by different factors, thus resulting in different behavior.

Several models have recently been presented to detect and prevent insider threats. Most of these have focused on technical factors and some have also discussed social, psychological and demographic factors. Selections of models that are representative of the research space are set out below:

Gonzalez and Sawicka developed a dynamic-system simulation model to discover complex security problems; their research goal was to understand the role of human factors in information security systems [22]. They used a simple case to demonstrate how system dynamics may provide insight into the security problem presented by individuals, and may help in designing robust security policies. The model focused on human factors and does not address other issues, such as technological and organizational environments.

Althebyan and Panda [1] presented a predictive model of insider threats focusing. on two components to develop their model: the insider's knowledge, and existing dependencies among objects in the system. Their model limits the possibilities for the insider to gain accesses to documents and get sensitive information from the organization. This model however, focused on cyber insiders and did not consider social insiders.

Hu, Bradford and Liu [28] developed a model for detection of insider attacks by intrusion detection systems based on the assumption that an insider is described by job function. However, the influence of social insider factors was not considered in this model.

The final model considered here, developed by Moore, Cappelli, and Trzeciak [40], presented a dynamic-system model of the insider IT sabotage problem, where the insider's main aim is to harm some parts of the organization, such as business operations, information and the system or network. Their model too, mostly focused on one primary problem, and they did not consider other types of insider threats, such as fraud or the stealing of sensitive information.

The scopes of prior studies have been limited to specialized areas, resulting in isolated findings where many factors related to insider behavior have been omitted, including such factors as gender, background and psychological factors.

Carnegie Mellon University has been conducting a variety of research projects on insider threats. One of the significant results achieved is the confirmation of the fact that insider attacks are substantial and have occurred across all organizational sectors, frequently causing potential harm to the affected organizations. Cases included a mixture of types, from low-tech attacks, such as fraud or theft of intellectual proprietary, to highly sophisticated technical crimes which damage the organization's infrastructure, damages are include financial or client loss and organization's reputation. The impact from insider attacks can be shocking, according to the 2005 E-Crime Watch Survey conducted by CERT Coordination Centre (CERT/CC), and CSO Magazine. One complex financial fraud case caused by an insider resulted in losses of around $700 million. Another incident resulted in losses of $10 million and the layoff of eighty employees [9].

This paper presents a critique of theoretical factors identified in the academic literature by comparing these theoretical perspectives with empirical evidence from actual reported incidents.

2. Method

This research involved three main activities. First, the academic literature was reviewed and studied in-depth to identify factors that are thought to influence an insider's behavior. Second, published reports on reported incidents have been analysed to determine a set of factors that have been observed in real-life cases of behavior associated with actual insider threats. Finally, the empirical information from stage two has been used to critique theoretical factors from the literature, resulting in a number of insights into areas in which the theoretical literature is lacking, and where further investigation is necessary. These insights form the basis of the recommendations made in the conclusion of the paper.

The data for this study was collected from two different sources: academic research, such as conference proceedings, journal articles and books, and published reported incidents, such as CERT's reports and journal articles. The CERT program conducted a study on internal threats in 2001, which gathered data and analyzed approximately 150 cases. The internal incident cases collected by CERT totaled 550 cases by 2011[23]. Further study of such cases can afford better insight into behavior factors associated with insider threats in actual insider crimes. This research seeks to study the internal incident cases from CERT for better understanding of the threat, and for insight into how insiders behave and the factors that influence insiders to behave in inappropriate ways. A total of thirteen reports derived from around 500 CERT's internal incident cases identified through public reporting were studied for this research. The internal incident cases in the CERT program are summarized in Table 1. According to CERT, insider threats fall into three main categories, all of which have been found important to this study. The three core categories are IT sabotage, fraud, and theft of intellectual property IP.

Table 1. CERT incident cases reports

Hanley et al.[23], Moore et al. [39] and Spooner et al.[49]	Theft of IP
Cappelli et al. [8], Keeney et al. [29], Band et al. [3] and Moore, Cappelli & Trzeciak [40]	IT sabotage
Cappelli et al. [9] and [10]	IT sabotage, fraud and Theft of IP
Randazzo et al. [45]	IT sabotage, fraud and Theft of IP in banking and finance sector.
Kowalski et al. [32]	IT sabotage, fraud and Theft of IP in Government sector
Kowalski, Cappelli and Moore [31]	IT sabotage, fraud and Theft of IP in IT and telecommunication sector

The collected data were analyzed to identify factors that are suggested or confirmed by prior rigorous academic research as well as potential factors that have been studied in reported incidents reports.

3. Review of Insider Threat Factors

Major factors contributing to insider threat behavior that emerged from the investigation of past research literature are: access and level of trust, the insider holding a technical position and/or having technical skills, motivation to carry out the abuse, outsourcing providing the opportunity, cultural factors, lack of information security policies, psychological factors, remote access facilities and gender. Each of these factors is considered in turn.

3.1. Access and Level of Trust

The academic literature surrounding insider threats suggests that insiders can cause significant harm, as they have the ability to avoid the physical and logical controls available to protect the organization. Moreover, beside their free access to the system they have a great knowledge about policies, pressures and security countermeasures in their organization [17]. Misuse of access is one of the most difficult types of attack to detect and prevent, since the insider uses his or her authorized access rights to perform illegal tasks [4]. Some organizations are now being asked to grant increased access to the database; users who need access to data include internal employees, auditors, contractors, and supply chain partners. With the increased access there is a major increase in the possibility of theft and abuse [4][12][19][21][41].

Insiders' privileged access allows them to easily abuse organizational trust for personal gain [34]. Privileged access makes it simpler for the insider to cause serious harm to the organization than it would be for someone attacking from outside. Some of this harm can be caused by inadequate defense mechanisms, but for the most part it is privileged access which allows harm to occur. Yet the privileged access which allows harm is also necessary to enable insiders to perform their proper job functions [15][17][33][51]. According to Althebyan and Pand *"Both privileges and knowledge help individuals in planning successful attacks while making it difficult for the organization to discover and/or prevent them*" [2].

Malicious insiders do not necessarily need privileged computer access to cause significant damage to their organization, since they have free physical access to some or all facilities in their organization, which allows them to access sensitive and confidential areas. This effortless access to the physical facilities allows them to make significant changes or steal vital and private data [17]. According to Walker [50] "*even the most physically or logically isolated military networks have to extend enough trust to users in order to perform the duties they are assigned. Therefore, some degree of access is usually available for utilization by a malicious insider"*.

Researchers claim that the level of trust that malicious insiders enjoy is one of the important factors that permit them to make a successful insider attack. This level of trust offers the essential privileges needed to enable internal misuse of the organization [15][36].

Insiders have free logical and physical access; they are more trusted, and have better information about their organization's internal processes and the potential weak points in the security policy; factors which permit them to easily harm their organizations [30][42].

Evidence from reported incidents supports the theoretical position developed in the academic literature, indicating that access is a significant factor in insider threats. The majority of reports regarding insider threats confirmed that access is one of the most important factors insiders usually abused when stealing information. According to Spooner et al. [49] all of the insiders in the cases they studied had some level of privileged access to the information they stole. Moore et al. [39] state in their report that the majority (67%) of insiders had authorized access to the information they stole. Moreover, Cappelli et al. [9] found that over 75% of the insiders had authorized access when they performed their theft. At the time of the incident 78% of the insiders were authorized users with active

computer accounts [45]. Almost 88% of the insiders had authorized access to the information in question, and those who did not have authorized access to the information were former employees [10]. However, other reports indicate that less than 50% of the insiders had authorized access to the system at the time of incident [24][29][31][40].

3.2. Insider Technical Position and Technical Skills

Academic literature suggests that authorized employees are usually familiar with some or all the internal process of their target systems. For example, insiders are almost always aware of the policies, procedures, security countermeasures and the associated vulnerabilities which relate to them, or they have the ability to gain that knowledge without suspicion [2][36][52].

Furthermore, employees sometimes use their IT skills to harm an organization's system through activities such as downloading and using hacker tools, gaining access to the system after termination, and the setup and use of backdoor accounts. Insiders usually have the skills which are generally limited to the systems with which they are familiar may increase their opportunity to compromise these systems. Some research considers the level of employee sophistication as a potential factor which can influence their ability to perform insider misuse. The levels of IT sophistication are set out below [12][36][52].

- Advanced: end users with a high level of sophistication, who shows the mastery of applications and system.
- Ordinary: end users with a medium level of knowledge of some applications.
- Novice: end users with a low level of IT knowledge.

While theoretical academic literature argues that employees in technical positions with technical skills are a factor in insider threats behavior, empirical evidence from reported incidents varies according to the different types of insider crime. Most of the reports studied suggest that the guilty insiders held technical positions such as system/database administrators, engineers and programmers. According to Spooner et al. [49] in all of the incidents they analyzed the insider worked as either a scientist or a computer engineer. Some reports mentioned that around 70% of the insiders were employed in technical positions, which included system administrators, programmers and engineers [10][24][29][32]. Moreover, Moore et al. [39] and Hanley et al. [23] assert that nearly 50% of the insiders had held technical positions in the incident which they studied. On the other hand, some researchers claim that less than 20% of the insiders were employed in a technical position [8] [9][31][45].

Moreover, some of the insiders used sophisticated technical means to perform their attacks. Generally they used some technical methods such as writing a script or program, included a logic bomb, or placing a virus on client computers, utilizing password crackers, and downloading remote system administration tools.

Randazzo et al. [45] and Kowalski et al. [31] assert that approximately 10% of the incidents they analyzed involved sophisticated tools or techniques. According to some insider incident reports, around 30% of the insiders used one or more sophisticated techniques to assist them in the attack, such as the ability to write a script or program, establish a backdoor account, or compromise another employee's account [9][10][24][29]. Only two reports suggest that over half of the cases involved sophisticated technical methods [8][32].

The differences in the level of importance ascribed to technical skills is not surprising given that some insider threats will require sophisticated technical skills while others will not. What is unclear from the empirical case evidence available is the relative proportions of attacks that require no particular skill, attacks that require technical skills, and those that would require certain skills where those skills can be from a third party, for example by downloading an exploit from the Internet.

3.3. Motivation

Academic literature asserts that motivation is one of the significant factors leading to insider threats. According to Furnell [19] motivations include *"greed, revenge, stress, and espionage, as well as being exacerbated by other factors*". Insiders' attack-motivation could be categorized into three main categories: IT sabotage, financial gain, and business advantage [52]. Some of the recent attacks have been motivated by financial gain: attackers hope for gain if they sell the organization's data and information that exists in the database. Most often, insiders deliberately abuse the system to gain sensitive data for financial or business gain. Whether the motivation is deliberate or accidental, it represents a significant risk of inappropriate user activity [21]. The malicious insider's motivation could involve the hope of direct personal gain, or the insider may have been recruited by competitive organizations that financially reward them for their betrayal [50].

Some researchers have discussed opportunity as a motivational factor, and how the availability of opportunity can motivate employees to abuse their organization [7][18][26]. Indeed, 'the land of

opportunity' is one of Bloombecker's eight categories of motivation [7].

Evidence from reported incidents supports the theoretical positions found in the academic literature, indicating that motivation is one of the significant factors in insider threats. Motivation has been discussed in many incidents reports, which have divided insider motivations into three main categories: financial gain, revenge and business advantages. Most insiders in the banking and finance sector were motivated by financial gain, rather than a desire to damage the information or the organization's infrastructure. Insiders stole information to sell it, and modified data to achieve financial benefits for themselves.

Financial motivation represents less than the half of insider incidents, and other motives included revenge, frustration with organization management, culture or policy dissatisfaction, and sometimes that insider's were persuaded by outsiders [8][9][24][31][32].

Researchers have suggested as many as 84% of the incidents were motivated by revenge [29][40] the second category of motivation. In Hanley et al. 80% of the incidents were motivated by a desire for revenge against their company [24]. According to Cappelli et al. over half of the incidents they analyzed were vengefully committed to retaliate for a negative event, such as transfers or termination, salary or employer dissatisfaction, new managers, and demotions [9][10]. Kowalski et al. [31] found that only around 20% of insiders were motivated by revenge, and indicated that insiders had other motives and goals, such as financial gain.

The final category of motivation is business advantages. All incidents studied by Spooner et al. [49] and Cappelli et al.[10] were cases in which insiders stole intellectual property in order to gain a business advantage. Sometime insiders stole the information to get a direct advantage at a new job or to start a new competing business. According to Moore et al [39] 32% of the insiders analyzed were acting to gain an immediate advantage at a new job.

If the insiders have a motive to harm their organization as well as having logical or physical access either authorized or unauthorized, and they are familiar with the environment of the workplace, they can represent a serious threat to the organization [48].

3.4. Outsourcing

The academic literature maintains that there are rapidly increasing numbers of third-party workers given long-term access to organizations' systems and critical information. Some researchers suggest that a single outsourcing contract can change the position of several 'outsiders' to 'insiders' and may blur the difference between a organization's employees and members of the third party. Contractor's employees may be given a level of logical and physical access equal to the organization's full time employees. The dynamics of the labor force in the market and the increased rate of worker turnover could lead to increase in the vulnerability of organizations, to loss of intellectual property and the probability to transfer the high value or high impact knowledge to a competitor or other external sources. This provides the opportunity for malicious insiders who now have access to collections of information that not previously collected to harm the organization [14].

While academic literature reviewed suggests that outsourcing is an important factor affecting behavior in insider threats, the empirical evidence from reported incidents reviewed for this study has found that outsourcing or the introduction of contractors are not major factors, as many reports did not indicate this as a significant factor; and where some reports discussed these motivations they referred to them at a very low percentage. Most of the reports studied argue that contractors were involved with less than 20% of insider incidents. According to Kowalski et al. [32] 16% of the insiders at the time of the incident were contractors, sub-contractors, or temporary employees. In all insider incidents analyzed by Kowalski, Cappelli and Moore [32] 18% only were contractors. Cappelli et al. declare that in only two out of fifteen cases they analyzed were there contractors or outsourcing employees involved, and all were current employees [8].

3.5. Cultural Factors

In the field of organizational studies and management, organizational culture is defined as the set of shared communal understandings which explain the psychology, attitudes, experiences, beliefs and values of an organization [14]. According to Royds [46] most of the data losses reported by the government of the UK since the HRMC incident show that only 5% occur because of technology issues while 95% occur as a result of cultural factors or people's behavior. Most organizations experience some kind of transformation at some stage in their development. Original corporate cultures are regularly dismantled and rebuilt, including the concepts and behaviors used to achieve security. However, if cultural changes are not addressed explicitly they can cause fear, ambiguity and doubt in employees, which can impact their attitudes regards to security [16].

Additionally, acceptable traditions for doing business differ according to region and area. For

example, some practices considered illegal in the Western world can be acceptable in other regions, such as the giving of substantial gifts. According to these differing various regional circumstances, the pressure of external sources on insiders could be easier to apply, both directly and indirectly, through sophisticated methods such as social engineering [14].

Although much of the academic literature reviewed above suggests that cultural factors are important in insider threats behavior, the empirical evidence from reported incidents reviewed in this study has found no evidence to support such assertions. According to Kowalski et al. [32] insiders did not share a common national or regional culture and also they had different demographic profiles. Insiders had come from diverse cultures: 42% were African American, 39% Caucasian, 8% Asian and 5% were Hispanic. Furthermore, Spooner et al. [49] claim that insiders come from different lands: 50% were American, and 40% were foreign nationals including Chinese and Taiwanese. Another study by Keeney et al. emphasized that insiders were demographically diverse with regard to culture and ethnic background, age, gender and marital status [29].

3.6. Information Security Policy

Researchers claim that insider threat is affected by several factors including the implementation of inappropriate policy for the information security and the technology involved in the infrastructure. However, even if the security policy is suitable and up to date, misuses of the policy are caused by human factors. Therefore, human factors are the central issue. These can be categorized into three main components: system role, reason of misuse, and the consequences of the system used [35]. The organization needs to know who has access to the data, what their own access policies are, and what actions they take to access data [44]. In general, a security policy determines what actions are authorized for a specific user and purpose. Users are able to misuse their privileges because the computer systems do not recognize people - only user accounts [6]. Therefore, organizations require a detailed security policy that focuses on both external and insider threats.

Some evidence suggests that the problems faced by organizations from internal threats are being reported along with matching evidence of insufficient security training and awareness [20]. Security training and awareness is one of the areas in which an organization must be focused on and applied for reducing the insider threats. If employees found that there is an effective security culture and their colleagues applied it this could make a difference. It would seem logical to expect that if organizations were to adopt a more responsible approach the change will reduce the insider threat risks [12]. Conversely, security culture could assist the insider to harm their organization. The bad news is that some existing security cultures are not keeping up to date and have no quick way to change [51].

Despite the fact that theoretical academic literature argues that security policy and policy culture are factors in insider threats behavior, empirical evidence from reported incidents is varied. It is noted that studies vary in terms of the scope of incidents examined, while this might explain different findings for factors such as motivation, it does not necessarily explain differences in information security policy.

Security policy, procedure, controls, guidelines and training are isolated from changes. Some executives in the EIU 2009 survey assert that their organizations have formulated IT policies to regulate the uses of the devices by employees, but that few have started to introduce these guidelines to employees: *"only 21% of surveyed firms provide training on the use of personal communications devices and only 17% do this for social networking applications. More worryingly, only 20% have plans to increase awareness in the future"* [19].

In 70% of the cases studied by Randazzo et al. [45] insiders had broken through or tried to break through systemic vulnerabilities in processes, procedures or policies to perform their attacks. In 61% of the cases these insiders exploited weaknesses inherent in the design of the hardware, software, or network. In 39% of cases the insiders were unaware of the technical security measures in their organization. Moreover, Kowalski et al. [31] claim that in half of the incidents they analyzed the insiders exploited the vulnerabilities in established business processes or controls, such as insufficiently enforced policies for separation of duties. Insiders were able to circumvent latent defects in business processes; they also exploited weaknesses in technical policies and procedures. In 22% of the incidents violations of vulnerabilities in security controls, such as poor of access control implementation, were involved [31]. Kowalski, Cappelli and Moore [32] assert that in 62% of the cases they studied, the insiders violated systemic vulnerabilities in policies, processes, procedures or applications. Most of the cases happened because of a lack of physical and technical access controls which facilitated the insider theft. In addition, 33% of incidents happened because of security policy violation [8]. Nevertheless, Spooner et al. [49] declare that none of the insiders exploited any technical vulnerability or security policies to carry out their thefts.

3.7. Psychological Factors

Some resarchers have attempted to study the psychological profile of an insider who was likely to offend before the incident. Many researchers wanted to know how to spot potential insider attackers before they attack. However, for several years the criminal justice system has unsuccessfully sought to develop a profile of the internal threat criminal. Criminologists are not yet close to discovering criminals reliably in advance. Criminals differ in their motivations and psychological makeup.

Thus, it should be possible to identify some types of very antisocial behavior, but it remains very difficult to identify other offenders because they can conceal themselves from advance detection. The presence of false positives obstructs these efforts. It is also difficult to identify internal threats in advance, because it is currently not possible to identify serious criminal intent or behavior. In addition, insiders' threat activity can gradually evolve from non-malicious intent to more malicious intent. A rigorous psychological evaluation might be sufficient to identify possible inside attackers while it might also prove to be offensive to the non-attackers who must be employed. Furthermore, the time spent to evaluate the candidate psychologically decreases the time available to consider if the employee would be beneficial to the organization or not.

As a result of this conundrum, even if a psychological exam existed its use might be counterproductive. The relative lack of cases to work with, the poor understanding of the best definition of average acceptable behavior, and the ambiguity in the identification of the boundary between acceptable and unacceptable behavior all combined to make the development of useful psychological profiles difficult [43]. However, Shaw, Ruby, and Post [47] assert that there are numerous features that, when found together, could indicate an increase in the possibility of harmful behavior on the part of the insider. These features are: computer dependency, a history of personal and social frustrations, ethical lapses, a sense of entitlement, and lack of empathy.

Another major use for psychology is positive: the development of ways to supporting good behavior. Some researchers seek ways to use psychology to keep insiders acting in positive ways. The predictions look more hopeful for this use of psychology than for profiling. The difference between profiling and motivational methods is that profiling must be precise, producing few false positives and false negatives. The risk of a false positive is that of not employing a good employee or refusing somebody who has not yet demonstrated harmful behavior; the risk of a false negative is failure to detect or prevent an attack [43].

Though the theoretical academic literature was diverse in regard to the psychological factors, empirical evidence from reported incidents argues that personal predispositions and behaviors are a common factor in internal incident cases. According to United States Secret Service and CERT, about 80% of insiders who performed attacks on their organizations had demonstrated negative behaviors before the incident, and 92% had experienced a negative occupational event, such as a demotion, transfer, warning, or termination [13]. According to Moore, Cappelli, and Trzeciak [40] the majority of the insiders in the MERIT cases who committed IT sabotage, the majority demonstrated the impact of personal predisposition. Personal predisposition is *"a characteristic historically linked to a propensity to exhibit malicious insider behavior" [40]*. Personal predispositions can be identified by some obvious characteristics, such as alcohol and drug addiction, physical partner abuse, violations arrests, hacking, and security violations. Most insiders in the studied cases had common personal predispositions which indicated an increased threat of performing malicious activities [3]. Personal predispositions may explain why some insiders perform malicious actions, while other employees exposed to the same situation do not act maliciously. Researchers emphasize that, in 97% of the IT sabotage cases, insiders came to the attention of supervisors or colleagues for concerning behavior before the incident [40]. An estimated 80% of the criminal insiders behaved in inappropriate ways prior to the incident, and 30% of them were arrested prior to an attack [29] According to Cappelli et al [8] 60% of the insiders had exhibited several incidents of concerning behavior or activity before the incident occurred, such as delays, absences and poor job performance. Their figures indicate that 55% of the criminal insiders have a noticeable concerning behavior prior the attack and 38% of the insiders had been arrested previously [32]. Kowalski et al. [31] report that about half of the cases (43%) the insiders demonstrated inappropriate behavior before the attack and about 31% of the insiders previously arrested. These individuals were arrested for: financial or fraud offenses (14%), nonfinancial offenses (6%), drugs or alcohol offenses (3%) and violent and other offenses (6%).

3.8. Remote access

Very few academic researchers investigated remote access as a factor in insider threat behaviors.

While the academic literature did not consider the consequences of remote access, security practitioners are keenly aware of its importance – it is even addressed by CERT's best practices – and empirical evidence from reported incidents also supports the significance of remote access as a factor in insider threats behavior. Employees can access the organization's networks from outside the workplace, from their homes or any another place. Several researchers claim that the number of cases which were carried out through remote access is significant. In 87% of the cases studied by Keeney et al., the victim organizations gave their employees remote access, and in 56% of the incidents the attacks were carried out through remote access [29]. Most of insiders in IT sabotage cases used remote access to committed their attack and in 30% of the fraud cases the insiders used remote access [9].

According to Moore, Cappelli, and Trzeciak [40] in 64% of the cases they studied the insiders used remote access to attack. Half of the cases used remote access to attack 24]. In about 43% of the cases the insider attacks were conducted via remote access from outside the workplace [32]. Randazzo et al. [45] report that 30% of the cases were performed from the insiders' homes via remote access and 57% of those were attacks carried out both from workplace and from home. On the other hand, some reports declare that less than 20% of the incidents were conducted via remote access [8][23][31][39][49], even though remote access is an important factor and which has been largely ignored by academic research.

3.9. Gender

There is almost no academic literature investigating gender as a factor in insider threats behavior.

In contrast to the academic literature's silence on the importance of gender, empirical evidence from reported incidents overwhelmingly supports the importance of gender as a factor in insider threats behavior.

According to Moore et al [39] in 82% of overall CERT cases the insider was male and 91% of the insiders who stole intellectual property were male. Another study indicates 94% of the insiders were male [23]. Males committed 90% of the incidents studied by Spooner and his group [49]. In another study 96% of the insiders were male [29]. Insiders who carried out IT sabotage were mainly male and males constituted 80% of the insiders who stole secret proprietary information [8]. The majority of the insiders were also male in the research by Capelli [10] and Hanley [24]. However, some reports indicate that the numbers of males and females were equal; in a study presented by Kowalski et al [31] 50% of the insiders in cases were male and 50% were female. Cappelli et al [9][10] support the contention that half of the insiders were male and the other half female in cases of fraud and theft for financial gain.

4. Conclusions

In its identification of factors which affect insider threat behaviors, this paper presents a focused view of the perspectives offered in associated academic literature, with or without the evidence of actual cases. The comparison with empirical reported incidents evidence has shown that theoretical academic research has overlooked gender as an important factor. Evidence clearly suggests that male gender is a factor in most CERT cases; therefore, further academic investigation in male-gender related issues is needed. It is noted that such research would need to be mindful of legal constraints, particularly regarding workplace discrimination. Similarly, academic research has overlooked remote access as a factor in insider threat behavior, and thus more research is also required in this direction. Without research into these two possible factors, theoretical models of insider threat are potentially incomplete.

Second, it is possible that theoretical emphases of the importance of technical positions held within an organization actually restate the importance of access: those with technical positions almost by definition have access. While employees in technical positions may have technical skills, the presence of such skills may be coincidental in many internal incident cases. In future research it will be important to investigate the extent to which technical skills are a factor in and of themselves; it may well be the case that such skills are not necessary in an age where exploit tools can be freely obtained via the Internet.

Third, although much of the academic literature suggests that outsourcing and cultural factors are important in insider threats behavior, there is very little empirical evidence from reported incidents to support this belief. Outsourcing and cultural factors therefore need more clarification to determine their importance. This could require more empirical studies to support the theoretical assertions.

The empirical support for academic assertions that security policy and policy culture are factors in insider threats behavior was varied; it is not particularly common, but there are some reports that consider policy as a contributing factor to aid insider attacks. Time may be a factor in this regard: the importance of a good security policy framework is well-known today and it is less likely that recent cases will find poor policy as a factor than in the past. However, future

research to confirm or disconfirm this would be beneficial.

Academic literature is not unanimous in regard to the importance of psychological factors; some authors have argued that the psychology of the insider is an important factor, while others declare that it is difficult to control for such factors. Nevertheless, empirical evidence from reported incidents suggests that personal predisposition and behaviors are common factors in internal incident cases and therefore further investigation regarding psychological factors is definitely needed.

Finally, evidence from reported incidents supports the theoretical perspective that an insider's motivation is a factor; it is obvious that the majority of insiders who stole intellectual property were motivated by business advantages. Continuing to spend research efforts in this direction is not necessary, given that other areas appear less well understood.

Understanding the insider threat is an important academic research direction and a sound theoretical model of insider threat behavior will enable security professionals to better protect their organizational assets. Providing specific models of the insider threat without making a holistic contribution adds to the obstacles to preventing insider threat. The scope of many prior studies has been limited to specialized areas, and this is understandable in the quest to gain deeper knowledge of specific aspects of insider behavior. Whilst on one hand this provides more insight into specific types of behavior it also presents a fragmented approach to the overall problem. There is a need for a holistic approach in order to understand the nature and breadth of the insider threat within the context of the organizational structure, its goals, activities, threats, risks and vulnerabilities. To be beneficial such a holistic model would need to consider character, social, technical and organizational factors. Research is needed to develop such a holistic conceptual model, encapsulating a broader perspective of the insider situation that more closely reflects empirical experience

5. References

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

[2] Althebyan, Q., and B. Panda. 2008. A Knowledge-Based Bayesian Model for Analyzing a System after an Insider Attack. In *Proceedings of The IFIP TC 11 23rd International Information Security Conference*, ed. S. Jajodia, P. Samarati and S. Cimato, 557-571. Springer Boston.

[3] Band, S., D. M. Cappelli, L. Fischer, A. Moore, E. D. Shaw, and R. Trzeciak. 2006. *Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis* CERT Program and Software Engineering Institute.

[4] Bellovin, S. M. 2008. The Insider Attack Problem Nature and Scope. In *Insider Attack and Cyber Security*, ed. S. J. Stolfo, S. M. Bellovin, A. D. Keromytis, S. Hershkop, S. W. Smith and S. Sinclair, 1-4. Springer US.

[5] Besnard, D., and B. Arief. 2004. Computer Security Impaired by Legitimate Users. *Computers & Security* 23 (3): 253-264.

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

[7] Bloombecker, J. 1984. *In Computer Security: a Global Challenge Introduction to computer crime* North-Holland, Amsterdam: Elsevier Science Publishers(accessed

[8] Cappelli, D., T. Caron, R. Trzeciak, and A. Moore. 2008. *Spotlight On: Programming Techniques Used as an Insider Attack Tool*

[9] Cappelli, D., A. Moore, T. Shimeall, and R. Trzeciak. 2006. *Common Sense Guide to Prevention and Detection of Insider Threats- Version 2.1* CyLab.

[10] Cappelli, D., A. Moore, R. Trzeciak, and T. Shimeall. 2009. *Common Sense Guide to Prevention and Detection of Insider Threats – Version 3.1* CERT Program, Software Engineering Institute and CyLab.

[11] Chinchani, R., A. Iyer, H. Ngo, and S. Upadhyaya. 2005 Towards a theory of insider threat assessment. In *IEEE International Conference* Washington, DC. IEEE Computer Society

[12] Cohen, F. 2001. The New Cyber Gang -- A Real Threat Profile. *Network Security* 2001 (5): 15-17.

[13] Cole, E. 2008. *Correlating SIM information to Detect Insider Threats A SANS Whitepaper* SenSage. http://www.sans.org/reading_room/analysts_program/SIMInfo_June07.pdf (accessed 8 Mar 2011).

[14] Colwill, C. 2010. Human factors in information security: The insider threat - Who can you trust these days? *Information Security Technical Report* In Press, Corrected Proof:

[15] Contos, B. 2007. Insider threat monitoring is enhanced by asset relevance. *Infosecurity* 4 (2): 47-47.

[16] Crinson, I. 2008. Assessing the insider-outsider threat' duality in the context of the development of public-private partnerships delivering choice' in healthcare services: A sociomaterial critique. *Information Security Technical Report* 13 (4): 202-206.

[17] Dallaway, E. 2008. You're only human. *Infosecurity* 5 (6): 7-7.

[18] Forester, T., and P. Morrison. 1994. *Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing* 2 nd ed. Cambridge: MIT Press.

[19] Furnell, S. 2004. Enemies within: the problem of insider attacks. *Computer Fraud & Security* 2004 (7): 6-11.

[20] Furnell, S. 2006. Malicious or misinformed? Exploring a contributor to the insider threat. *Computer Fraud & Security* 2006 (9): 8-12.

[21] Fyffe, G. 2008. Addressing the insider threat. *Network Security* 2008 (3): 11-14.

[22] Gonzalez, J., and A. Sawicka. 2002. A framework for human factors in information security. In *2002 WSEAS Int. Conf. on Information Security*. Rio de Janeiro, Brazil.
[23] Hanley, M., T. Dean, W. Schroeder, M. Houy, R. Trzeciak, and J. Montelibano. 2011. *An Analysis of Technical Observations in Insider Theft of Intellectual Property Cases*. CERT Program and Software Engineering Institute.
[24] Hanley, M., A. Moore, D. Cappelli, and R. Trzeciak. 2009. *Spotlight On: Malicious Insiders with Ties to the Internet Underground Community*. Software Engineering Institute and CyLab.
[25] Hayden, M. 1999. *The insider threat to U. S. government information systems*. National Security Telecommunications And Information Systems Security Committee.
[26] Hitchings, J. 1995. Deficiencies of the traditional approach to information security and the requirements for a new methodology. *Computers & Security* 14 (5): 377–383.
[27] Ho, S. M. 2008. Behavorial parameters of trustworthiness for countering insider threats. In *The Third Annual iConference*.
[28] Hu, N., P. G. Bradford, and J. Liu. 2006. Applying role based access control and genetic algorithms to insider threat detection. In *Proceedings of the 44th Annual ACM Southeast Regional Conference (ACM-SE)*. New York, USA. ACM.
[29] Keeney, M., D. Cappelli, E. Kowalski, A. Moore, T. Shimeall, and S. Rogers. 2005. *Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors*. CERT Program and Software Engineering Institute.
[30] Kemp, M. 2005. Barbarians inside the gates: addressing internal security threats. *Network Security* 2005 (6): 11-13.
[31] Kowalski, E., D. Cappelli, and A. Moore. 2008. *Insider Threat Study: Illicit Cyber Activity in the Information Technology and Telecommunications Sector*. U.S. Secret Service and CERT/SEI.
[32] Kowalski, E., T. Conway, S. Keverline, M. Williams, D. Cappelli, B. Willke, and A. Moore. 2008. *Insider Threat Study: Illicit Cyber Activity in the Government Sector*. U.S. Secret Service and CERT/SEI.
[33] Liu, D., X. Wang, and J. Camp. 2008. Game-theoretic modeling and analysis of insider threats. *International Journal of Critical Infrastructure Protection* 1: 75-80.
[34] Liu, D., X. Wang, and L. Camp. 2009. Mitigating Inadvertent Insider Threats with Incentives. In *Financial Cryptography and Data Security*, ed. R. Dingledine and P. Golle, 1-16. Springer Berlin / Heidelberg.
[35] Magklaras, G. B., and S. M. Furnell. 2001. Insider Threat Prediction Tool: Evaluating the probability of IT misuse. *Computers & Security* 21 (1): 62-73.
[36] Magklaras, G. B., and S. M. Furnell. 2005. A preliminary model of end user sophistication for insider threat prediction in IT systems. *Computers & Security* 24 (5): 371-380.
[37] Martinez-Moyano, I., E. Rich, S. Conrad, D. Andersen, and T. Stewart. 2008. A behavioral theory of insider threat risks: a system dynamics approach. *ACM Transactions on Modeling and Computer Simulation* 18 (2): 1-27.
[38] Martinez-Moyano, I., M. Samsa, J. Burke, and B. Akcam. 2008. Toward a generic model of security in an organizational context: exploring insider threats to information infrastructure. In *Proceedings of the 41st Hawaii International Conference on System Sciences*. Hawaii, USA. IEEE Xplore.
[39] Moore, A., D. Cappelli, T. Caron, E. Shaw, and R. Trzeciak. 2009. *Insider Theft of Intellectual Property for Business Advantage: A Preliminary Model*. CERT Program, Software Engineering Institute and CyLab at Carnegie Mellon University.
[40] Moore, A., D. Cappelli, and R. Trzeciak. 2008. *The "Big Picture" of Insider IT Sabotage Across U.S. Critical Infrastructures*. CERT Program and Software Engineering Institute.
[41] Nykodym, N., R. Taylor, and J. Vilela. 2005. Criminal profiling and insider cyber crime. *Digital Investigation* 2 (4): 261-267.
[42] Okolica, J., G. Peterson, and R. Mills. 2006. Using PLSI-U To Detect Insider Threats from Email Traffic. In *Advances in Digital Forensics II*, ed. M. Olivier and S. Shenoi, 91-103. Springer Boston.
[43] Pfleeger, C. P. 2008. Reflections on the Insider Threat. In *Insider Attack and Cyber Security*, ed. S. J. Stolfo, S. M. Bellovin, A. D. Keromytis, S. Hershkop, S. W. Smith and S. Sinclair, 5-16. Springer US.
[44] Pramanik, S., V. Sankaranarayanan, and S. Upadhyaya. 2004. Security policies to mitigate insider threat in the document control domain. In *Proceedings of the 20th Annual Computer Security Applications Conference (ACSAC'04)*. Washington, DC, USA. IEEE Computer Society
[45] Randazzo, M., M. Keeney, E. Kowalski, D. Cappelli, and A. Moore. 2004. *Illicit Cyber Activity in the Banking and Finance Sector*. U.S. Secret Service and CERT/SEI.
[46] Royds, J. 2009. Virtual battlefield. *CIR Magazine*.
Schultz, E. E. 2002. A framework for understanding and predicting insider attacks. *Computers & Security* 21 (6): 526-531.
[47] Shaw, E., K. G. Ruby, and J. M. Post. 2005. *The insider threat to information systems1. the psychology of the dangerous insider*. Security Awareness Bulletin, No. 2-98.
[48] Shaw, E. D. 2006. The role of behavioral research and profiling in malicious cyber insider investigations. *Digital Investigation* 3 (1): 20-31.
[49] Spooner, D., D. Cappelli, A. Moore, and R. Trzeciak. 2009. *Spotlight On: Insider Theft of Intellectual Property inside the U.S. Involving Foreign Governments or Organizations*. CERT Program, Software Engineering Institute and CyLab.
[50] Walker, T. 2008. Practical management of malicious insider threat - An enterprise CSIRT perspective. *Information Security Technical Report* 13 (4): 225-234.
[51] Walton, R., and W.-M. Limited. 2006. Balancing the insider and outsider threat. *Computer Fraud & Security* 2006 (11): 8-11.
[52] White, J., and B. Panda. 2009. Automatic Identification of Critical Data Items in a Database to Mitigate the Effects of Malicious Insiders. In *Information Systems Security*, ed. A. Prakash and I. Sen Gupta, 208-221. Springer Berlin / Heidelberg.