School of Information Systems

A Study of Insider Threat Behaviour: Developing a Holistic Insider Threat Model

Asmaa Mahdi Munshi

This thesis is presented for the Degree of
Doctor of Philosophy
of
Curtin University

December 2013

DECLARATION

To the best of my knowledge and belief this thesis contains no material previously published by any other person except where due acknowledgment has been made. This thesis contains no material which has been accepted for the award of any other degree or diploma in any university.

Asmaa Munshi
10 December 2013

ACKNOWLEDGEMENTS

I would like to take this opportunity to express my sincere gratitude to my supervisors, especially Dr Peter Dell who dedicated more of his time and effort for helping me during this study. He has directed me through the hardest times as he encouraged me to always focus on the prize, "the doctoral degree". I am very thankful for his support, cooperation, open door policy and for leading me to the right way in my study. Moreover, I would like to thank Dr Tomayess Issa for her prompt response and immediate feedback. She worked patiently and diligently with me throughout my whole journey. Finally, I would like to extend my sincere thanks to Dr Helen Armstrong for guiding me to the right decision in the beginning of this thesis and for sharing her extensive knowledge in the field of security.

I would like to give my deepest expression of love and appreciation for all those who provided me the possibility to complete this thesis. Firstly, without the support of my husband Dr Talal Qadah and my children Muhammed and Deyaa, I would never have succeeded. Thanks my beloved husband without your encouragement, support, understanding, patience, caring and listening, writing this thesis would not have been possible. Muhammed, my little instructor, you always care about my study even if I am too busy to care about yours. 'How many chapters left mum?' was the inspired question that enlightened my heart to achieve my work. Muhammed your mum finally finished her biggest homework, thanks for being a great instructor for me. My little angel Deyaa, you were my smile during the busiest and hardest time. No words in any language can express my heartfelt thanks to my lovely family for their kindness and thoughtfulness during this long journey.

My special words of thanks should also go to my father, Mr. Mahdi Munshi who always believed in me. His unlimited love and support gave me the confidence in myself, helped me see what I could be. He has given me strength to strive for my goals, to be independent and never settle for less. His support and encouragement guided me throughout this academic journey. He will always be my role model in

life. I would like to extend my thanks to my mother Mrs. Fiqah Jamal Hariri for everything she gives me in my life; thanks for everything I learnt from you since my childhood. I would not have been here without your guidance and blessing. Thanks a lot my parents for today, yesterday and tomorrow, for all that made me stronger.

ABSTRACT

Over the last decade, the number of insider threat cases has increased by 500%. However, although this costs the world a great deal, very little academic research has been devoted to investigating the problem. One of the most recent security violations was committed by Edward Snowden in June–July 2013. Snowden, an American infrastructure analyst, leaked some of the National Security Agency's (NSA) top-secrets. In one of the worst NSA security breaches in United States history, Snowden, who was a technical contractor at NSA, disclosed highly critical information. . This incident illustrates that the prospect of insider threats is still a real and present danger threatening the security of organisations and indeed nations around the world; this study investigates the factors that influence insider threat behaviour and develops a holistic view of insider threat behaviour and ways to manage it.

This research adopts an Explanatory Mixed Methods design approach for the research process. Firstly, the researcher collects the quantitative data and then the qualitative data is collected in two sequential phases. In the first phase of this study, the holistic insider threat model is developed; in the second phase, best practices are developed to manage the threat.

In the first phase, the literature review identified the need for a holistic approach to address all insider threat factors. After it was established that no holistic model exists that adequately addresses the issue of insider threat behaviour, a candidate holistic insider threat model was developed to incorporate all the factors that had been identified in the literature. The candidate model was then evaluated, via a survey, by 100 security specialists. The collected data were analysed using the Exploratory Factor Analysis technique and the candidate model was modified based on the results, leading to a further eight factors being included in the enhanced insider threat model.

The quantitative data collection stage was followed by the qualitative stage, the aims of which were twofold: to evaluate the enhanced model, and to gather information about ways to manage each factor in the model. The data were collected from 11 Chief Information Security Officers (CISOs). The semi-structured interview data were analysed using a two-stage content analysis technique. The results from the interviews were taken into account for the final holistic insider threat model. Finally, in the second phase a set of best practices were developed to manage the factors in the final holistic insider threat model.

This study makes both theoretical and practical contributions. The theoretical contribution lies in the holistic conceptual insider threat model that successfully combines a range of factors that may influence the insider to behave inappropriately in terms of an organisation's security. These factors were derived from three sources: academic research, published legal cases and IT industry publications. Regarding its practical contribution, the findings of this study, especially the best practices, will assist organisations to better manage the insider threat behaviour, thereby mitigating the risk of insider threat. .

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE: INTRODUCTION

1.1 Background

Any security system will have to rely on its operators even if it is designed and implemented in a perfect manner. Organisations face ongoing threats from external and internal attacks (Cappelli, Moore, and Trzeciak 2012; Willison and Warkentin 2013; Guo 2013; Zafar 2013). Insider attacks, which have been recognised as a potential security problem since the 1980s (Chinchani et al. 2005), are associated with legitimate users who abuse their privileges and can easily cause significant damage or loss to an organisation (Cappelli, Moore, and Trzeciak 2012; Sasaki 2011; Sarkar 2010; Liu, Wang, and Camp 2009; Martinez-Moyano et al. 2008b). Almost all organisations and sectors are currently faced with the problem of insider threats to vital computer assets (Willison and Warkentin 2013). Internal incidents can cause more than just financial losses; the costs can also include loss of clients and damage to an organisation's reputation.

Part of this chapter has been presented and published in the following conferences:

1- Munshi, Asmaa, Peter Dell, and Helen Armstrong. 2012. "Insider Threat Behavior Factors: A Comparison of Theory with Reported Incidents". In *45th Hawaii International Conference on System Science (HICSS), Maui, HI* 2402-2411. IEEE.

2- Munshi, Asmaa, and Tomayess Issa. 2012. "Insider Threat: A Critical Review of the Literature". In *IADIS International Conference - Internet Technologies and Society 2012, Perth, WA*: IADIS press.

3- Munshi, Asmaa. 2010. "A Study of Insider Threat Behaviour: Developing a Holistic Framework". In *IADIS International Conference - Internet Technologies and Society 2010, Perth, WA*: IADIS press.

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 organisational sectors, frequently causing potential harm to the affected organisations. 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 organisation's infrastructure; damages include financial or client loss and organisation's reputation (CERT 2006).

The impact from insider attacks can be shocking, according to a CERT study on organised insider threat crime; the average costs of these crimes exceed $3M, with some cases resulting in $50M in losses (King 2012). Moreover, according to the 2005 E-Crime Watch Survey conducted by CERT 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 lay-off of eighty employees (CERT 2006). Cybercrime appears as one of the most important challenges to law enforcement as computer crime causes many problems to daily business operations and information. According to an Australian computer crime and security survey, computer fraud cost nearly $1,000,000 between 2005 and 2006, which caused the biggest financial loss to Australian businesses since 2003 (Mubarak and Slay 2010). A Computer Crime and Security Survey conducted in 2008 found that the average financial loss to an organisation as a result of fraud was US $500,000 per year (Mubarak and Slay 2010).

Problems related to security and insider threat issues are not restricted to specific organisations; almost all organisations face the same problems. Therefore, a comprehensive model needs to be adopted to minimize the insider threat problem by controlling the factors which assist the insiders to behave inappropriately towards both the organisations and their computer systems. Such a model should place equal emphasis on people, tools, technology, environment and behaviour.

Although most organisations pay great attention to outsider attacks and expend significant efforts in securing information systems, actually very few take an efficient approach to minimizing insider attack (Hu and Panda 2009). The insider threat is one of the most serious problems affecting security systems and one that is difficult to overcome (Bishop et al. 2008). The threat is associated with the authorised users who misuse their access and trust to cause significant damage to an organisation (Martinez-Moyano et al. 2008b). Trusted employees have the most potential to harm the organisation by damaging the information or stability of the operation system (Ho 2008). Understanding employee actions is a principal goal for insider threat protection and detection. The differences between "acceptable normal" and "unacceptable abnormal" employee behaviour varies among organisations. Understanding the special restrictions and concerns affecting an organisation's security policy could help to determine the inappropriate behaviour of the employees (Hu, Bradford, and Liu 2006). Although most employees can pose a potential insider threat in some form, not all insiders pose insider threats; in fact, most employees can be trusted to protect the information of the organisation. Even though most of the existing literature refers to the insider as malicious in insider threat researches (Wood 2000), not all insider cases of abuse of organisations' systems, networks or information are based on malicious intents. Insider threats can also arise by accident (Magklaras and Furnell 2002; Carroll 2006).

Unintentional insider threat could be the result of either accidental deletion or policy violation. Accidental deletion occurs when an authorised employee accidentally accesses sensitive information and by mistake changes or erases this information. Unintentional policy violation is not malicious security policy circumvention. A good example of this is when an employee creates an unauthorised copy of sensitive data in order to take work home. This sensitive data now exists in a storage device which, if compromised, could lead to an unintentional security policy violation (Fyffe 2008).

One challenge of the insider threat is how to discriminate between authorised and unauthorised actions. Once an authorised employee has access to internal resources, it could be difficult to recognize activities that are malicious. This is particularly difficult in the case of an outsourced employee or contractor who has been granted some access to complete a job. Furthermore, the increase in employee turnover and changing roles adds more complexity to the overall problem (Bhilare, Ramani, and Tanwani 2009).

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

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

1.2 Insider Definitions

According to Pfleeger et al. (2010), the concept of "insider" represents assumptions about who is under consideration, the trust level the insider had, the insider knowledge about the organisation's systems, and the system's perimeter. The problem of insider threats has been investigated by many researchers, most of whom

do not offer a comprehensive definition of an insider. For example, a RAND Corp. report defines an insider as *"an already trusted person with access to sensitive information and information systems"* (Brackney and Anderson 2004, xi), while on another position it defines the insider as *"someone with access, privilege, or knowledge of information systems and services"* (Brackney and Anderson 2004, 10). Ignoring the 'trusted person' in the first definition, this second definition assumes the insider is trusted not to abuse the information of the system. In fact who is considered as an insider might be different among organisations (Predd et al. 2008). According to Bishop (2005, 75), an insider is *"someone with access, privilege, or knowledge of information systems and services".* And also *"Anyone operating inside the security perimeter".* Chinchani et al. (cited in Bishop et al. 2008, 9) define insiders as *"legitimate users who abuse their privileges, and given their familiarity and proximity to the computational environment, can easily cause significant damage or losses".* Another definition by Butts, Mills, and Baldwin (2005, 413) states that an "*insider is any individual who has been granted any level of trust in an information system".* Althebyan and Panda (2007, 240) define the insider as an "*individual who has the knowledge of the organisation's information system structure to which he/she has authorised access and who knows the underlying network topologies of the organisation's information system".* According to Carroll *(2006, 156), "insider is any persons who have access to an organisations information including people such as contractors, temporary employees and the like".* Other definitions simply include anyone operating inside the security perimeter (Patzakis 2003), ignoring factors such as trust and knowledge of the systems. Such different definitions exclude insiders who are not trusted, which results in a binary distinction whereby a person is either an insider or not an insider. Blackwell (2009) define an insider *" as one who has legitimate access to an organisation , its systems, information or other resources".* The final definition of the insider was offered by Gabrielson (2006, 1) who regards the insider as *"any entity (person, system, or code) authorised by command and control elements to access network, system, or data".* Each definition could be suitable for a particular organisation, situation, or concern. Even though defining the authorised insider is better to identified by the business and

organisation's needs, it is fundamental to have a general preliminary point for considering insiders and addressing their inappropriate behaviours. The basic definition should be common and free from assumptions about system's perimeter and the nature of authorised access. Therefore, Pfleeger et al. (2010, 170) propose a common insider definition they define the insider as ***"****A person with legitimate access to an organisation 's computers and networks".*

1.2.1 Insider Taxonomy

Many researchers classify insiders according to different categories based on role or level of access. This section describes insider classification in more detail.

The first attempt to categorize insider abuse of organisation systems was made by Anderson (1980). He describes three types of malicious insiders namely: masqueraders, misfeasors and clandestine users. Masqueraders are insiders with full access to the computer system who exploit its weakness in order to obtain the identity of another authorised employee. Misfeasors are insiders who misuse their authorised access so as to abuse the system. Finally, the clandestine insider is the one using his authorised access to avoid audit, control and access resource mechanisms in a particular computer system.

Magklaras and Furnell (2002) established three classifications of insiders: system masters, advanced users and application users.

- System masters: includes all authorised employees such as network administrators with full administrative privileges access to most of the organisation's resources. As a result of their increased level of access and trust, this category of authorised employees presents a significant threat to the organisation's resources and infrastructure.
- Advanced users: includes all authorised employees who have a significant knowledge about the organisation's internal process and system. This category includes: system programmers and database administrators, in addition to

previous system masters and the current shift operator. Even if they do not have a high level of access to the organisation's system, they are aware of any system vulnerability.

- Application users: this category includes all remaining authorised employees in the organisation who use standard applications, such as World-Wide-Web (WWW) browsing, email and a database of clients. Generally, they have only the access required for them to run their application without any extra access to system resources. These employees can misuse the application to which they have access.

Furthermore, Cole and Ring (2005) categorise insiders according to their levels of access; they established four categories as follows:

- Pure insider: is an employee with all the privileges and access associated with being employed by the organisation. In general, s/he has access to the facilities, devices and networks. This category of insider can cause great harm since they have almost all the access they need. An elevated pure insider is an employee who has additional privileged access, such as system administrators who are given greater access, such as route access to the network, in order to do their jobs. Nevertheless, in some cases, these employees are given greater access than is actually required. In general, when organisations attempt to minimize the insider threat risk, they start to limit the access of the elevated pure insider. Organisations should give their employees only the amount of access they require to carry out their jobs, and remove the additional access that they do not need.
- Insider associate: is an employee such as a contractor, guard or cleaner with limited authorised access. This category usually has limited access, the insider having physical access to the facility and building but not privileged access to the network. Some employees leave sensitive data on their desks and lock their office doors, although locking a door actually does not protect the data. Employees must remember that there are other individuals such as cleaning staff who need to access all offices every night for cleaning;

therefore, sensitive data must always be well secured. User awareness and control of access are required to minimize the harm caused by an insider associate. Increasing awareness is supposed to change employees' behaviour, whereas training is intended to teach employees new skills. Many employees believe that their building and office are well secured and they can leave systems logged in and sensitive information lying about without any concern. User awareness sessions can assist employees to understand that locks do little to secure information. All employees should recognize that many people could have potential access and that they must consistently and adequately secure sensitive information and log out from the systems before they leave.

Pure insiders and insider associates have an authorised reason to access the organisation's recourses. The following two categories of insider do not.

- Insider affiliate: is a partner or friend who uses the employee's identification to obtain access. The most damaging insider affiliate is an individual who directly acts as an employee using the employee's ID. For instance, the partner of an employee may need to browse the Web and borrows the employee's laptop to do so. Using the employee's user ID and password, he not only can log on and access the internet, but also he can access sensitive information. Moreover, some employees give their access card for the building and PIN number to their partner to pick up some sensitive papers from the office. To avoid insider affiliates, the best measure is to adopt consistent policies and procedures. Organisations should have written policies, procedures and regulations which all employees should read and sign off that they understand them. After that, any violation or ignoring of policy can be considered as a deliberate action on the part of an employee.
- Outside affiliate: is an untrusted outsider who exploits open access in order to use an organisation's resources. A good example is wireless access - an organisation sets up an unsecured wireless access point which allows an outsider to connect to its network. This is similar to leaving the building door

unlocked with no access controls and allowing anybody to get in. Even if the outside affiliate threat seems obvious, it is frequently ignored by some organisations. For protection against the outside affiliate, organisations need to implement an appropriate access control protocol for all sorts of access, including logical and physical access.

1.3 Insider Threat Definitions

Most of the existing definitions focus on the insider's abuse of trust or access rather than on the consequential risk to the organisation. Moreover, some definitions suggest that the threat is always malicious while others include accidental behaviour.

Einwechter (cited in Pfleeger et al. 2010, 170) defines the insider threat as *"someone entrusted with authorised access who manipulates system access to exploit it"*. Brackney and Anderson (2004, xi) define the insider threats as *"malevolent (or possibly inadvertent) actions by an already trusted person with access to sensitive information and information systems"*. Carroll (2006, 1):*"Insider threats can be either intentional or unintentional".* Anderson et al. (2000, 36): *"Any authorised user who performs unauthorised actions that result in loss of control of computational assets"*. Schultz and Shumway (2001, 189) describe the insider threat as *"the intentional misuse of computer systems by users who are authorised to access those systems and networks"*. According to Blackwell (2009), insider threat is *"a risk that an insider can misuse their access or knowledge to cause harm to the organisation"*. The problem of insider threat definition is further complicated because the boundary is not clear-cut, as someone inside it naturally is an insider. This is further complicated by the increased use of outsourced and contract employees. Even after defining the boundary of the insider threat, many definitions do not address physical boundaries, and instead focus mainly on the technology boundaries (Bishop et al. 2008).

According to Bishop et al. (2008) handling the insiders rather than defining the problem is another complication in understanding the concept of insider threats. This point has been addressed by many studies, although they do not adequately describe the problem. Another definition given by Keeney et al. (2005b, 10) states that *"insider threats are those executed by a current or former employee or contractor that intentionally exceeds or misuses an authorised level of access to networks, systems, data, or resources to harm individuals and/or an organisation"*. These definitions however, while addressing the cyber insiders, do not consider social insiders. This definition characterises the insider as an entity which includes not only people but also systems and code, which is very important as no other definitions have addressed these elements. Pfleeger et al. (2010) define the insider threat as the insider's undesirable or inappropriate action which poses a risk to an organisation's data, processes, or resources.

Establishing a definition is important if researchers are to find an effective means of minimizing the insider threat problem. Without a comprehensive definition of the insider threat, each researcher defines it according to his/her own assumptions and perspective, which may lead to complications if their model is used for other applications. Therefore, a comprehensive definition of insider threat will allow flexible movement and translation between several domains under one model and thus assist in reducing the insider threat problem.

This research uses this definition of insider threat: *"the potential harm posed by any trusted entity with inside access to the organisation"* (Munshi, Dell, and Armstrong 2012, 2402). Each trusted entity will have a different level of trust assigned that is appropriate to their position and role. Each trusted person will be influenced by different factors, thus resulting in different behaviour. Insider behaviour refers to human attempts to obtain self-satisfaction. According to Calandrino, McKinney, and Sheldon (2007, 1) *"Undesirable insider behaviour involves any wilful or negligent misuse of resources in an organisation's information systems"*. This research will investigate insider threat behaviour resulting not only from a person's actions, but

also controlled and guided by organisational policies, procedures, security restrictions, as well as external factors such as laws.

1.4 Insider Behaviour

Most information security specialists suggest that information security within organisations can be made more effective by encouraging good employee behaviours and limiting bad employee behaviours (Schultz 2002; Stanton et al. 2005; Möller et al. 2011). The crucial success of information security in any organisation relies on suitable end-user behaviours (Rhee, Kim, and Ryu 2009). Insider threat *"refers to intentionally disruptive, unethical, or illegal behaviour enacted by individuals who possess substantial internal access to the organisation 's information assets"* (Stanton et al. 2005, 125). Due to the significance of employees' security-related behaviours, studying the different types of behaviour that employees engage in could assist managers, auditors and information technologists to measure and influence employee behaviour (Stanton et al. 2005).

Stanton et al.(2005) conducted a research study to illustrate the helpful and harmful behaviours that information technology employees perform within organisations, which might influence the information security. They determined six categories of security behaviour, focusing on two factors: intentionality and technical expertise. The intentionality factor relates to whether the behaviour is intentionally malicious, intentionally beneficial, or in between. The technical expertise factor focuses on the level of computer or information technology knowledge and skill that the users require in order to execute the behaviour. Table 2.2 shows the six categories arranged according to these two dimensions (Stanton et al. 2005, 126).

Table 1.1: Two-factor taxonomy of security behaviours

adapted from (Stanton et al. 2005, 126).

Expertise	Intentions	Title	Description
High	Malicious	Intentional destruction	Behaviour requires technical expertise together with a strong intention to do harm to the organisation's IT and resources. Example: employee breaks into an employer's protected files in order to steal a trade secret.
Low	Malicious	Detrimental misuse	Behaviour requires minimal technical expertise but nonetheless includes intention to do harm through annoyance, harassment, rule breaking, etc. Example: using company email for SPAM messages marketing a sideline business.
High	Neutral	Dangerous tinkering	Behaviour requires technical expertise but no clear intention to do harm to the organisation's IT and resources. Example: employee configures a wireless gateway that inadvertently allows wireless access to the company's network by people in passing cars.
Low	Neutral	Naïve mistakes	Behaviour requires minimal technical expertise and no clear intention to do harm to the organisation's information technology and resources. Example: choosing a bad password such as ''password.''
High	Beneficial	Aware assurance	Behaviour requires technical expertise together with a strong intention to do good by preserving and protecting the organisation's information technology and resources. Example: recognizing the presence of a backdoor program through careful observation of own PC.
Low	Beneficial	Basic hygiene	Behaviour requires no technical expertise but includes clear intention to preserve and protect the organisation's IT and resources. Example: a trained and aware employee resists an attempt at social engineering by refusing to reveal her password to a caller claiming to be from computer services.

1.4.1 Insider Attack Classification

This section discusses several classifications of the insider attacks that have been identified in the previous literature.

In the literature, one finds several classifications of insider attacks. Usually, malicious insiders intentionally misuse the system and information. Because of their

malicious intents they are ready to pose a risk to the organisations by following a specific process and engaging in various activities to achieve their targets (Wood 2000). To mount a successful attack, the insider generally follows an essential process: insiders are motivated to attack, they identify their goals, plan their attack and finally launch the attack.

- Insider motivated to attack: could be either the results of the insider's discontent, or somebody employed by either an internal or external party to harm the organisation.
- Insider identifies target: Either the insider spots the target as a means to fulfil a personal need, or an outsider suggests a target to the insider.
- Insider plans operation: The insiders perform some investigation of their target. They plan the attack and might even employ somebody else to assist them in carrying out the attack.
- Insiders launch the attack: Once the attack has been launched by the insider, subsequent actions are not obvious. Several possibilities include: damage assessment, escape in a hurry, escape when suitable, or launch the attack again until they are either successful or caught.

According to Schultz (2002), there are several indicators that can point to future malicious insider attacks. These include:

- Deliberate markers: insiders sometimes leave deliberate markers to make a "statement", which can differ in scale and obviousness.
- Meaningful errors: insiders can make several errors in the process of preparing for or executing the attacks. These mistakes could have been saved even if the insiders try to erase related evidence.
- Correlated usage patterns: are patterns of computer usage that are consistent from one system to another. An insider can use a command to search on many systems for records with particular words in them.
- Verbal behaviour: Both spoken or written could present a sign that an attack is imminent.

- Personality traits: This indicator refers to the psychological profile of the offenders. Some personality factors such as introversion, stress handling capability and frustration could be used in predicting insider attacks.

Butts, Mills, and Baldwin (2005) mention four types of actions that malicious insiders could execute:

- Alteration: a malicious insider modifies an organisation's information, or another employee accesses it in an unauthorised manner.
- Elevation: a malicious insider gains unauthorised access to the system, for instance when someone tries to get administrative privileges. This could be achieved by social engineering.
- Distribution: a malicious insider transfers confidential information to someone who is not supposed to have this information. The insider transfers secure information to an unauthorised individual; this happens when the insider has appropriate access to the system and the need to know.
- Snooping: a malicious insider obtains unauthorised information about a user or object. This action can occur when a malicious insider is given authorization by the system but this will violate the organisation's policy.

Furthermore, Bellovin (2008) suggest that there are three different types of attack: misuse of access, defence bypass, and access control failure.

- Misuse of Access: Misuse of privileges access is considered to be probably the most difficult type of attack to detect or prevent. Usually, insiders use their authorised access rights to perform an authorised task. For instance, university professors can request that marks be changed after the end of the semester. Normally, this occurs in order to correct clerical errors. However, if professors request a change to the grades in response to a bribe, then this would constitute insider misbehaviour. It is very difficult to stop or spot abuse by insiders only through technical means.
- Defence Bypass: Insiders normally have a main advantage over outsiders since they are already past some defence layers. One of these defences is

firewalls which numerous organisations depend upon as a component of their cyber security. Typically, insiders are not blocked by the firewall because they are inside it, and therefore out of it range. Likewise, insiders normally have some kind of login access to an organisation's computer systems which allows them to perform local attacks rather than network attacks. It is hard to detect this attack by means of only technical defences. Insiders are inside the organisation and therefore have better opportunities to carry out misbehaviour.

- Access Control Failure: By contrast, access control failures are considered to be a technical issue. The ideal solution is to correct the problem. Insider attack detection is often more complex, particularly when a configuration error occurs, because by definition the system is not declining inappropriate access requests. Good solutions require looking for misbehaviour by other applications.

Another classification is given by Blackwell (2009) and Serdiouk (2007) who suggest three classes of insider attacks based on their actions: sabotage, fraud and theft. These attacks cause unwelcome consequences by violating the basic security services of integrity, confidentiality and availability. Moreover, problems can also occur as a result of unintended failures or external attacks which are facilitated by internal weaknesses. These three types of attack are detailed as follows:

- Sabotage: can cause loss of availability and integrity of the targeted resources with potential significant impacts on the organisation's ability to execute its usual business activities.
- Fraud: can cause major financial losses to the organisation since illegal transactions are carried out.
- Theft: includes intellectual property, logical assets (e.g. Information) and physical assets (e.g. equipment). The leaking or theft of confidential information frequently has a much more serious consequence than the loss of physical assets.

Likewise, the third CERT guide to insider threats classifies an insider attack according to the purpose of the attack, which can be one of three: sabotage, financial gain or business advantage (CERT 2009).

Other researchers classify the insider actions that cause direct or indirect threats to organisational assets into two categories (Willison and Warkentin 2013; Crossler et al. 2013):

- Intentional (deviant behaviour): includes sabotage, theft, and industrial espionage
- Unintentional (misbehaviour): includes using an organisation's computers to browse non-work related Websites, posting secure information onto untrusted Websites by accident, or carelessly opening phishing links on emails and Websites

According to Cole and Ring (2005), all types of attacks carried out by an insider produce significant damage and financial loss to the organisation.

The next section will discuss the problems posed by insiders, comparing the impacts of their activities with those of external attackers and will also present statistics which reflect the current problem.

1.5 Purpose of the Study and Research Questions

The problem of insider threat has become a major issue in the security field as many challenges have arisen and are increasing. *"The challenges of preventing, detecting, and responding to insider threats, is among the most difficult facing security researchers and professionals today"* (Huth et al. 2013, 1). According to Huth et al. (2013, 1) there is no definitive description of insider threat problems and solutions: *"one of the most important elements in any field of research is the common vernacular researchers use to describe problems and solutions. Unfortunately, insider threat and data leakage research has yet to fully mature in this respect".*

Most of the researches relating to insider threat cover the problem from the researcher's perspective to match his/her situation which focuses on one primary problem as either a technical or human issue. The models used in such research may be suitable for their particular case but not for other cases covering different aspects. Moreover, most of the models focus largely on technical issues without considering the behavioural aspects. A recent study however, indicated that successful protection against insider threats relies on both technical and behavioural solutions (Martinez-Moyano et al. 2008a).

A holistic approach is essential to address the whole picture of the insider threat problem and provide further solutions as stated by Huth et al. (2013, 2) *"an approach is necessary to provide holistic solutions to the problem of insider threats".* 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 organisational structure, its goals, activities, threats, risks and vulnerabilities. To be beneficial, such a holistic model would need to consider character, social, technical and organisational 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.

The purpose of this study is to develop a holistic model that includes all factors that influence the insider to behave inappropriately, and ways to manage these factors. It will examine the threat posed by any insider within the organisation and includes current, former or contractors employees. The primary research questions of this study are as follows:

> *RQ_1: What are the factors that influence the insider to behave inappropriately with regard to security?*
>
> *RQ_2: How can organisations manage the security-abusive behaviour of insiders?*

1.6 Outline of the Thesis

This section provides an overview of the thesis structure. The thesis has eight chapters. Chapter One (this chapter) briefly discusses the background of the study, the research problem and the purpose of the study. The focus of the study and the research questions research are presented.

Chapter Two reviews the literature related to the insider threat behaviour from three different sources: academic research, IT industry publications and published reported incidents. The scope of the literature search and selection criteria is justified, and the risk of insider threat is detailed. The chapter then provides a critical review of the insider threat contributing factors from the three sources in order to develop the candidate holistic insider threat model. In addition, some of the previous insider threat models that represent the research scope are described to provide further theoretical support for the conceptual model. Finally, Chapter Two highlights the research gaps.

Chapter Three starts with a description of the research objectives followed by the research questions. The theoretical and practical significance is explained. Next, the factors in the candidate holistic insider threat model are explained in detail. This research will assist in the development of the candidate holistic insider threat model by combining all factors identified in the three sources of the literature. Finally, the candidate holistic insider threat model is presented as the initial research model.

Chapter Four describes the research methodology and research process. First, the selection of research paradigm and mixed method design will be explained and justified. Second, the sample selection and the quantitative and qualitative data collection are discussed. Finally, the various phases of the research are described.

Chapter Five gives a general overview of the quantitative data collection that has been used to test the candidate holistic insider threat model. This chapter discusses

the survey design, target population and the Web-based survey. Furthermore, survey distribution and analysis are described. Finally, the enhanced holistic insider threat model is presented.

Chapter Six provides a general overview of the qualitative data collection that has been used to validate the enhanced holistic insider threat model. The interview decisions, design, the process of obtaining interviewees, data analyses and coding are described in detail. The results from the interviews and the new information obtained from the security specialists as well as the participants' feedback regarding the proposed model are discussed. The chapter concludes with the presentation of the final insider threat holistic model.

Chapter Seven describes the management and controls for the factors produced in the final holistic insider threat model using the best practices. This chapter discusses the method used to develop these best practices which comprises two steps: first, understanding CERT best practices and addressing the gaps in the CERT best practices; second, using interviewees' suggestions and several academic sources to address the shortcomings found in CERT best practices. Finally, this chapter presents a list of extra guidelines that complement CERT best practices, which can be used to minimise insider threats.

Chapter Eight summarizes this study. This chapter provides answers to the research questions. The theoretical and practical contributions are presented. Finally, the limitations of the study and the future research opportunities are detailed.

CHAPTER TWO: LITERATURE REVIEW

2.1 Introduction

This chapter reviews the literature related to insider threat behaviour from three different sources: academic research, IT industry publications and published reported incidents. This review indicates that, to date, no insider threat model has been proposed that comprehensively addresses the issue of insider threat. This literature review describes in detail the risk of insider threat followed by an in-depth analysis of the factors (from the three sources) contributing to insider threat. Previous insider threat models are also explored.

In addition, the gaps in the research are noted and the key contributions of the present research are discussed. The literature review identified a range of factors from the academic sources, published reported incidents and IT industry publications. This chapter presents a critique of theoretical factors identified in the academic literature by comparing these with actual reported incidents and IT industry publications. This comparison resulted in a number of insights gained into areas in which the theoretical literature gaps. Thus, further investigation is necessary in order to identify the main contributing factors to insider threat behaviour.

Part of this chapter has been presented and published in the following conferences:

1- Munshi, Asmaa, Peter Dell, and Helen Armstrong. 2012. "Insider Threat Behavior Factors: A Comparison of Theory with Reported Incidents". In *45th Hawaii International Conference on System Science (HICSS), Maui, HI* 2402-2411. IEEE.

2- Munshi, Asmaa, and Tomayess Issa. 2012. "Insider Threat: A Critical Review of the Literature". In *IADIS International Conference - Internet Technologies and Society 2012, Perth, WA*: IADIS press.

2.2 Scope of the Literature Search

The data for this study have been collected from three different sources: academic research, IT industry publications and published reported incidents. The literature review follows a systematic approach as shown in section 2.2.1 below.

2.2.1 Selection Criteria and Justification

The first step of a literature study is to locate relevant academic literature through online database as a primary literature collecting approach. Conventionally, this is done by targeting related books, journals and conferences. Given the limited number of IS security researches, especially relating to insider threat research papers published in the leading IS journals suggested by Schwartz & Russo (2004), some additional IS security-specific journals were included. According to Siponen & Willison (2007) the three journals which include major publications on security are: *Computers & Security, Information Management and Computer Security and Information Systems Security*. In addition to these three journals this research also studies other security journal such as *Information Security Technical Report, Computer Fraud & Security, Network Security and Infosecurty*. Furthermore, five important online scholar databases were targeted: ACM Digital Library, IEEE Xplore, ProQuest, ScienceDirect and SpringerLink. These databases cover almost all of the ISWorld's top 50 IS journals which include the aforementioned journals and most of the top 10 IS conferences (Schwartz and Russo 2004; Levy and Ellis 2006). Thus, these databases are comprehensive enough to produce a literature set which can represent the current status of insider threat in IS research literature. Several search terms were determined for this research, and several synonyms and combinations of different words were utilized such as: 'insider threat', 'internal misuse', 'insider attack', 'insider threat factors ', 'managing insider threat', 'insider threat behaviour', 'addressing insider threat', 'internal threat', 'information theft', 'data leakage' and 'insider threat detection and protection'. Figure 2.1 shows that after the eighth term, the search produced almost the same articles which indicate

that the majority of the articles were covered by those search terms. The search aimed to find books, journal articles and conference proceedings. The initial search resulted in finding 50 articles from ACM, 69 articles from SpringerLink, 160 articles from IEEE Xplore, 50 articles from ProQuest (computing) and 80 articles from ScienceDirect, in total 409 articles (see table 2.1).

The 409 articles were then analysed. This was done firstly by scanning the title and abstract of the articles and excluding irrelevant articles; this left 191. Secondly, the full text of each article was reviewed and those which were not focused on insider threat were discarded; this left 90 articles.

The systematic academic literature search resulted in 90 papers which address the insider threat issue, describe the contributing factors, and propose solutions to this problem. The academic literature review results show that more than the half of the papers found were actually conference proceedings and only around 34 papers were from journals.

Table 2.1: Summary of the literature search

Scholar databases	Number of articles	Search terms
ACM Digital Library	50	'insider threat', 'internal misuse', 'insider attack', 'insider threat factors ', 'managing insider threat', 'insider threat behaviour', 'addressing insider threat', 'internal threat', 'information theft', 'data leakage' and 'insider threat detection and protection'
IEEE Xplore	160	
ProQuest	50	
ScienceDirect	80	
SpringerLink	69	

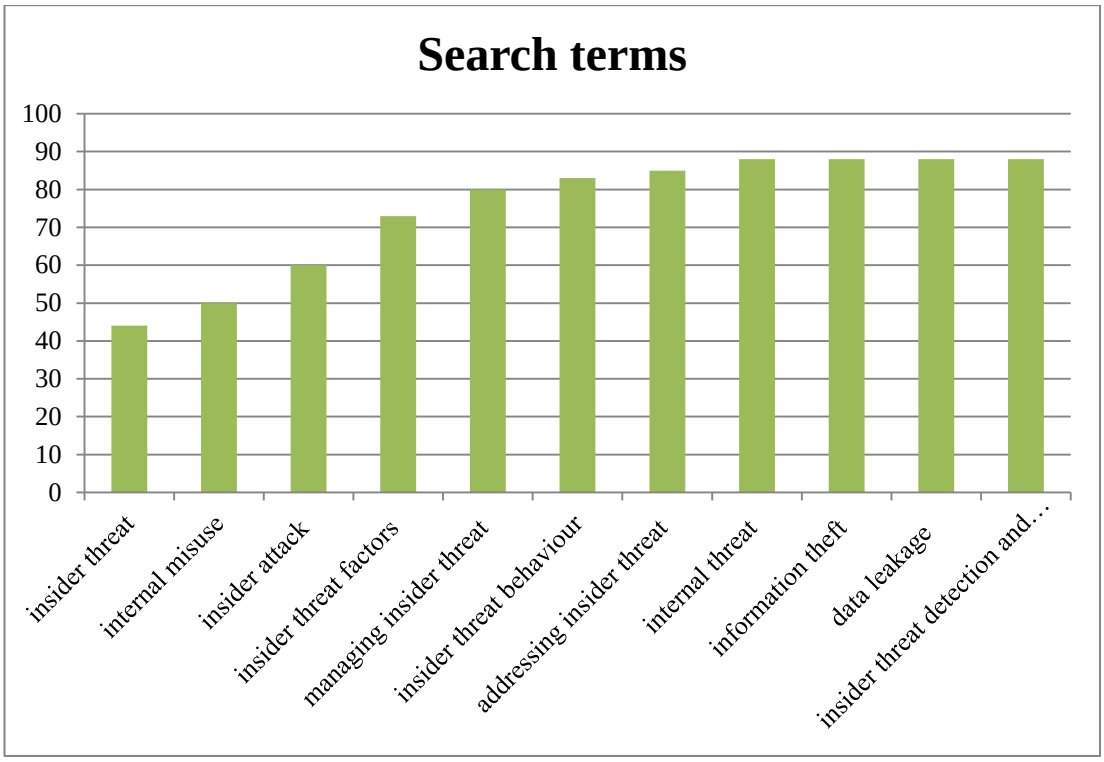


Figure 2.1: Search terms and number of articles

The second step in a literature review is to study IT industry publications. Several important business online databases were targeted including Emerald, Factiva, Business Source Premier, JSTOR, ABI/Inform Complete, Business Source Complete and ProQuest, ACM Digital Library; these were the main data bases that were examined for data published during past ten years. Furthermore, several IT magazines were consulted including *Network World, SC Magazine: For IT Security Professionals, Security Director's Report, Computerworld, InfoWorld and Communications of the ACM*. The same key words used in the first step of the literature study were used in this step, including: 'insider threat', 'internal misuse', 'insider attack', 'insider threat factors', 'managing insider threat', 'insider threat behaviour', 'addressing insider threat', 'internal threat', 'information theft', 'data leakage' and 'insider threat detection and protection'. The search of magazines articles initially yielded 81 relevant items. The title and full text of each article were examined and any articles that not related to this study were discarded, leaving 30 articles that discussed the risk of insider threat, several insider threat cases and the insider threat factors.

The third step is to study published reported incidents. According to Cappelli, Moore, and Trzeciak (2012), CERT has the largest number of detailed insider threat cases in the world. CERT conducted a research on the insider threat during the last decade and established a comprehensive database. This database contains technical, behavioural, and organisational details of every insider threat case. In 2001, the CERT program analysed about 150 cases and this number increased to 550 by 2011 (Hanley et al. 2011). By 2012, the number had expanded to more than 700 insider threat cases (CERT 2012; Cappelli, Moore, and Trzeciak 2012). Thus, in this phase of the literature review, the reports generated by CERT are studied and analysed.

According to CERT, insider threats fall into three main categories: IT sabotage, fraud and theft of intellectual property IP (Cappelli, Moore, and Trzeciak 2012), all of which are important to this study. The three core categories are *(CERT 2012, 4):*

- IT sabotage: *"an insider's use of IT to direct specific harm at an organisation or an individual"*
- Fraud: *"an insider's use of IT for the unauthorised modification, addition, or deletion of an organisation's data (not programs or systems) for personal gain, or theft of information that leads to an identity crime (e.g., identity theft or credit card fraud)"*
- Theft of intellectual property IP: *"an insider's use of IT to steal IP from the organization. This category includes industrial espionage involving outsiders"*

Figure 2.1 (adapted from CERT (2012, 6)) illustrates the sectors most affected by insider fraud, sabotage, and theft of IP. The differences among sectors are interesting and expected. For example, information technology is the sector that has suffered the most from theft of IP, followed by the commercial facilities sector. While, banking and finance sector experienced the most fraud cases, followed by the government sector. The IT sector also experienced the most IT sabotage attacks, followed by the

commercial facilities sector. The high percentage in the IT sector is possibly due to the advanced technical skills of the employees in this sector.

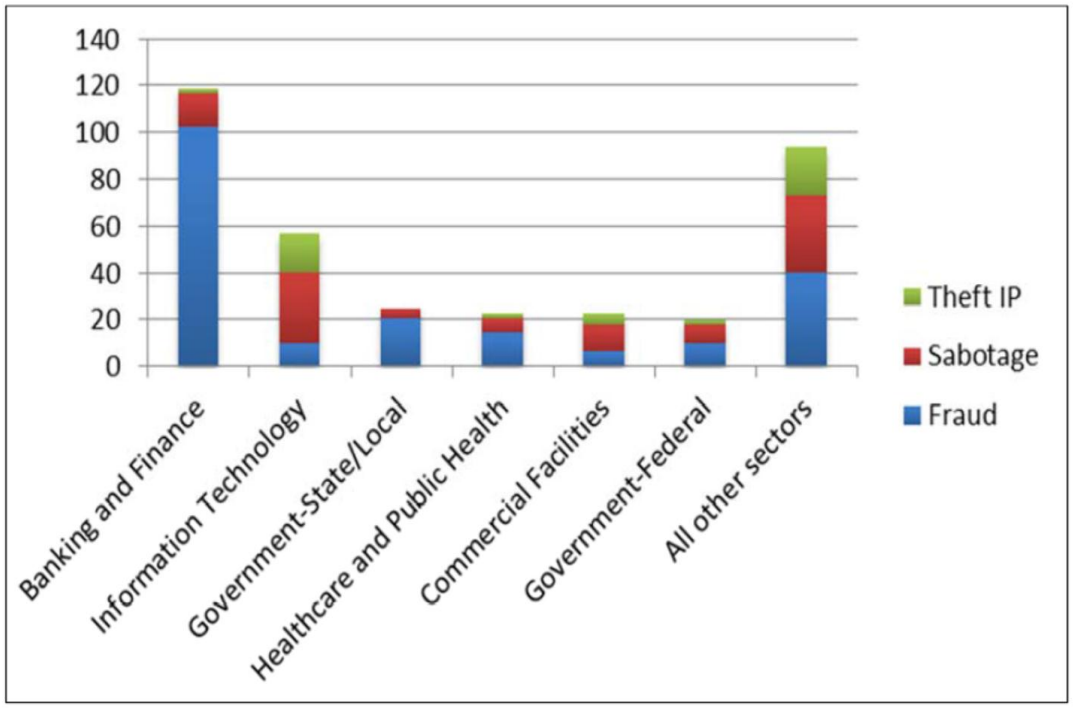


Figure 2.2: Top Six Infrastructure Sectors for Fraud, Sabotage, and Theft of IP

Further study of such cases in each sector can afford better insight into behaviour factors associated with insider threats in actual insider crimes. This researcher sought to study the internal incident cases from CERT to better understand the threat, and to gain insight into how insiders behave and the factors that influence insiders to behave in inappropriate ways. A total of fifteen reports derived from around 700 of CERT's internal incident cases identified through public reporting were studied for this research. The insider incident reports provided by CERT program are summarised in Table 2.1.

Table 2.2: CERT incident cases report

Reports	Insider threats categories
Hanley et al. (2011), Moore et al. (2009) and Spooner et al. (2009)	Theft of IP
Cappelli et al. (2008), Keeney et al. (2005a), Band et al. (2006) and Moore, Cappelli, and Trzeciak (2008)	IT sabotage
King (2012)	Fraud
Cummings et al. (2012)	Fraud in banking and finance sector
CERT (2006), CERT (2009) and Lewellen et al. (2012)	IT sabotage, fraud and Theft of IP
Randazzo et al. (2004)	IT sabotage, fraud and Theft of IP in banking and finance sector.
Kowalski et al. (2008)	IT sabotage, fraud and Theft of IP in Government sector
Kowalski et al. (2008)	IT sabotage, fraud and Theft of IP in IT and telecommunication sector

The reviewed literature is comprehensive and includes both theoretical and empirical literature.

2.3 Risk of Insider Threats

The incidence of insider threats has continued to increase each year, and according to Brdiczka et al. (2012) there are indications that this trend will continue. The protection of confidential data and information such as intellectual property, customer data and patient records from unauthorised access by employees is a major concern for all organisations. Since employees need to access such information in order to carry out their daily tasks, the detection and prevention of unauthorised employee access are very challenging tasks (Gafny et al. 2010). Although insider attacks may occur less frequently than external ones, insiders have a high impact on information since they are familiar with their targets and security countermeasures in place (Chinchani et al. 2005). Almost all definitions of the insider maintain that the insider has free access, is more trusted and has better information about internal processes and procedures, and are always more aware of the vulnerable aspects of

the security than is an outsider. As a result, the insider attack can cause significant harm to an organisation (Probst, Hansen, and Nielson 2007).

According to Cole and Ring (2005), both types of attack -insider and outsider- can cause harm to an organisation, although the insider threat is usually worse for the following reasons:

- Insider threat is easier to implement: Insiders who pose the threat have all or most of the access they require. In addition, insiders have good knowledge of their target which allows them to succeed in the attack with less chance of being caught. On the other hand, the external attacker has less idea about what is going on at the other end, has little knowledge about the internal security countermeasures, and does not have authorised access to the system. Hence, the outsider is carrying out an almost blind attack which makes the attack more difficult than it is for the insider. Although some inside attacks are sophisticated, many of them are very basic and simple because in most cases the attacker has enough knowledge and access required to commit the attack.
- Current solutions do not scale: Most organisations' security devices such as firewalls and intrusion detection/ prevention systems are designed to prevent an outsider attack. Firewalls are designed to block access to selected ports, which can prevent an outsider attack but does not prevent the insider attack. If the insider requests access to some data to perform his job, the firewall will permit it which simply allows the insider to transfer the data to an unauthorised party. Intrusion detection/prevention systems get rid of known signatures of attack. While most signatures of the external attacks are known, those of most internal attacks are not. Moreover, organisations have minimal internal protection measures. Most of them perform poorly in terms of controlling access and do an even poorer job of establishing reliable policies. Limiting access and implementing consistent policies is the essential key to minimizing or even preventing the insider threat.

- Insider threats have a high chance of success: Insiders have practically all of the information and access they need which almost guarantees their success. Even though organisations might have appropriate access control and reliable policies in place, the insider threat will have a higher chance of success than does the external threat for the predictable future.
- Less chance of being caught: Since the insiders are familiar with the environment and have access, they are technically not violating the organisation's rules. Hence, the chances of being detected are much less. Even if attackers access data which they are authorised to access but use it inappropriately, this is much harder to detect.

All insider attacks such as sabotage, fraud and theft, can lead to financial loss to the organisation, financial instability, reduced competitive advantage, loss of employees, loss of clients and loss of consumer confidence (Cole and Ring 2005). Gonzalez and Sawicka (2002) found that human factors contributed to 80 – 90% of organisational accidents. Many industry statistics have confirmed the riskiness of the insider threat:

- According to a US Federal Bureau of Investigation survey conducted in 2004, the average losses resulting from successful external attacks was $56,0000. While the average losses from a successful insider attack was $2.7 million, almost 50 times greater. Moreover, since 2000, approximately 80% of information security incidents have been the result of insider attacks (Thompson, Whittaker, and Andrews 2004**).**
- Another survey of insider incidents conducted of banking and financial institutions showed that 30% of incidents had resulted in losses in excess of $500,000 each (Randazzo et al. 2004).
- CERT, a centre of Internet security expertise, reports that 22,716 vulnerabilities (from 1995-2005) and 319,992 incidents (from 1988-2003) were caused by insiders who had authorised access to the organisation's system (Martinez-Moyano et al. 2006).

- A U.S. Secret Service study and CERT focus on insider cybercrimes and indicate than when managers make deliberate decisions to improve organisational performance and productivity, they often produce the unintended result of increasing the organisation's exposure to insider attacks (Randazzo et al. 2004; Martinez-Moyano et al. 2008a).
- Insider threat is an extremely serious problem as indicated in Blackwell (2009)'s study which demonstrates that 68% of respondents believed that insiders present a major threat to their intellectual property and sensitive information. Insiders not only can cause direct harm to an organisation's assets, but by providing them with an access route, the organisations are gradually becoming more responsible for the activities of workers who violate policy and regulations (Martinez-Moyano et al. 2008a).
- Another study was conducted by the British Department of Trade and Industry (DTI) in association with PriceWaterhouseCoopers (PWC). In their survey, published in 2004, around 33% of the respondents claimed that their worst security incident came from insiders. Moreover, DTI and PWC demonstrate that the incidence of insider abuse cases has doubled since 2002, mainly after organisations' adoption of internet-related technologies (Magklaras and Furnell 2005).
- Furthermore, Computer Crime and Security Survey CSI's conducted in 2007, 2008 and 2011 all acknowledged the increase in the number of insider crimes. In 2007, CSI reported that 59% of respondents had experienced insider misuse of organization resources and 26% of respondents had in excess of 40% of their total financial losses from insider attacks (Hunker 2008). Moreover, a 2008 survey demonstrated that there are four categories which present as the highest. The incidence of insider abuse was the second most common occurrence in organisations at 44% (Richardson 2008). A Computer Crime and Security Survey CSI conducted in 2011 confirmed significant trends in computer crimes such as an obvious increase in the sophistication of insider crimes (Cummings et al. 2012).

- A Cyber Security Watch Survey conducted in January 2011 showed that around 43% of participants had experienced an insider attack incident between 2004 and 2010, and 46% of the participants stated that insider attacks were more costly than other attacks (Holmlund et al. 2011; CERT 2012).
- According to a CERT study on organised insider threat crime, the average costs of these crimes exceeded $3M, with some cases resulting in $50M in losses (King 2012).

The insider threat is an extremely serious problem since it has grown quickly and could happen at any time. The following section discusses the different models for insider threat detection and prevention, and describes the area and factors that each model focuses on in dealing with the insider threat.

2.4 Factors that Influence Insider Threat Behaviour

The major factors contributing to insider threat behaviour 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, insider knowledge, cultural factors, lack of information security policies, psychological factors, remote access and gender. Each of these factors is considered in turn.

2.4.1 Access and Level of Trust

The academic literature relating to insider threats suggests that insiders can cause significant harm as they can avoid the physical and logical controls available to protect the organisation. Most organisations give their employees more access than what they essentially need to do their job (Cole and Ring 2005). Misuse of access is

one of the most difficult types of attack to detect and prevent, since the insider uses his or her authorised access rights to perform illegal tasks (McNamara 1998; Cohen 2001; Furnell 2004; Nykodym, Taylor, and Vilela 2005; Bellovin 2008; Fyffe 2008; Willison and Warkentin 2013). Sarkar (2010, 126) stated that *"The abuse of system access and privileges are common. Most insider attacks generally start with abusing the system, and then violating security policies*". Some organisations are now being asked to grant increased access to data. With the increased access there is a major increase in the possibility of theft and abuse (McNamara 1998; Cohen 2001; Furnell 2004; Nykodym, Taylor, and Vilela 2005; Fyffe 2008; Bellovin 2008). Therefore, organisations should limit the employees' access to confidential data to minimise negative financial impacts and regularity consequences (Sarkar 2010).

Insiders' privileged access allows them to easily abuse organisational trust for personal gain (Liu, Wang, and Camp 2009). Wood (2000, 1) claim that the *"insider should have no problem getting the privileges they need to mount an attack"*. In particular, because insiders may have privileged access to their target, they can sometimes switch to an unauthorised privileged mode to mount a specific attack. Quite simply, the knowledgeable insider may employ somebody who has privileged access to launch an attack and the insider might be the person who is responsible for monitoring or enforcing the security policy of the target organisation (Wood 2000). Privileged access makes it simpler for the insider to cause serious harm to the organisation than other insiders with ordinary access. Some of this harm can be caused by inadequate defence 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 (Walton and Limited 2006; Contos 2007; Dallaway 2008; Liu, Wang, and Camp 2008) According to Althebyan and Panda (2008, 558) *"Both privileges and knowledge help individuals in planning successful attacks while making it difficult for the organisation to discover and/or prevent them".* System masters include all authorised employees within the organisation who have managerial privileges access to the majority of the system's resources. Top system and network administrators are typical examples of system masters. The increased level of access and trust this

category of authorised employee is given clearly constitutes a significant level of risk to the organisation (Magklaras and Furnell 2002) .

As discussed previously in section 1.3, it is important to consider physical access as well as system access. Malicious insiders do not necessarily need privileged computer access to cause significant damage to their organisation, since they have free physical access to some or all facilities in their organisation, 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 (Dallaway 2008). According to Walker (2008, 288) "*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"*. Swartz (2007) suggests that organisations should monitor their employees' access to sensitive information and detect unauthorised access in order to provide better protection for their sensitive information.

Academic researchers claim that the level of trust that malicious insiders enjoy is one of the important factors that permits them to launch a successful insider attack. This level of trust offers the essential privileges needed to enable internal misuse of the organisation (Magklaras and Furnell 2005; Contos 2007). An insider's position is an important factor which allows damage to be done to the organisation, since insiders are in a good position to do so in comparison with outsiders (Kemp 2005). Insiders have free logical and physical access; they are more trusted, and have better information about their organisation's internal processes and the potential weak points in the security policy - factors which permit them to easily harm their organisations (Okolica, Peterson, and Mills 2006).

Similarly, IT industry publications highlight the importance of the access factor in insider threats. These publications concur that granting access to staff creates a degree of exploitation of vulnerable knowledge across the organisation's network (Secret Service, Cert Analyze Insider Computer Sabotage 2005; Khanna 2005;

Lynch 2006; Roberts 2007; Chickowski 2009; Blades 2010). Employees may have access to customers' and employees' data and more vulnerable production and financial data can also be made available to employees in a company. Such data may be easily transmitted through simple access of the internet. For example, without the right policy and tools in place, it can be very easy for any staff member to send out confidential customer data to a competitor through email, or for an engineer to send out a source code to another company, or for an administrative employee to leak out company earnings or shares by means of a simple instant phone call or message (Ansanelli 2005).

Organisations should be aware of all access paths to the information available to all employees. An access path is a way into the organisation's information via an access point that leads into the system. This includes swipe cards, accounts and private virtual networks. An access path that is anonymous to management is not necessarily prohibited; however, organisations should moderate unknown access paths ways by recognizing them and frequently reviewing their validity in terms of their business needs (How to Weed out the New Insider Cybersecurity Threat 2007; Addressing the Insider Threat 2007). Organisations must be cautious of who has access to their information, and should ask themselves: is our company's data secure or can it be easily pasted into a flash drive or photographed with a phone? (Castle 2009).

In addition, organisations face a big challenge when trusted employees who have authorized access abuse their trust, as organisation cannot control when such trusted employees become malicious (Ortega 2006). If employees abuse the trust placed in them, it could potentially cost their organisations millions of dollars (Khanna 2005). Cybercrimes are often committed by trusted insiders, who use their authorized access to breach security (Bauch 2011). According to Thompson and Ford (2004, 3) state: *"The problem of insider threat is trust. Insiders must be trusted to perform their work duties. The problem occurs when insiders intentionally or unintentionally extend trust inappropriately"*.

Furthermore, system administrators and other users with privileged access pose a greater threat than do other employees. Most of the detected insider threats occur through such accepted privileged access protocols (Chickowski 2009). The main concern regarding privileged access is how to guarantee that IT personnel have suitable access only to the information they require (Messmer 2010; Addressing the Insider Threat 2007).

Passwords are crucial to one being granted access to an organisation's information. Therefore, it is important to frequently monitor the process of changing passwords to grant access to a company's information. It is also vital that upon termination of contracts or after layoffs, passwords too should be terminated (Messmer 2008). However, although it is crucial to disable password access after termination, that is not the last of it. Organisations should have full knowledge of who remains with access to their information, and the pathways still available into their information (How to Weed out the New Insider Cybersecurity Threat 2007; Kirkpatrick 2008).

One of the decisive tasks facing all establishments today is that of "Access Management". This is an important protection measure to ensure that granted access is limited only to those employees who require such information to do their jobs. This is a challenge that must be addressed by incorporating human resources systems with primary access control systems. There is also rapid development of single sign-on and multi-factor verification. These guidelines for granted access can contribute to further security measures that protect the organisation's infrastructure from outside and inside threats (Financial Institution Security Risks and Concerns: The Top Eight 2007). Although one person should be authorised to have full access to a company's system, experts recommend dividing an approved level of access among employees according to their duties. Hence, instead of granting access to the entire IT staff, access should be limited and divided among IT personnel according to departments and systems. For instance, engineers responsible for maintaining e-mail servers should not be granted access to the accounting systems (Ortega 2006; Wehrum 2009).

Evidence from reported incidents supports the theoretical position developed in the academic literature and IT industry publications: 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. (2009), all of the insiders in the cases they studied had some level of privileged access to the information they stole. Moore et al. (2009) and King (2012) state in their report that the majority of insiders had authorised access to the information they stole. Moreover, CERT (2006) found that over 75% of the insiders had authorised access when they committed their theft. In approximately 71% of the cases, the insiders relied on some form of authorised access (Cummings et al. 2012). At the time of the incident, 78% of the insiders were authorised users with active computer accounts according to a study by (Randazzo et al. 2004). Almost 88% of the insiders had authorised access to the information in question, and those who did not have authorised access to the information were former employees (CERT 2009). However, other reports indicate that less than 50% of the insiders had authorised access to the system at the time of incident (Keeney et al. 2005a; Moore, Cappelli, and Trzeciak 2008; Kowalski et al. 2008; Hanley et al. 2009).

2.4.2 Insider Knowledge

Academic literature suggests that employees normally have great knowledge about their organisation, and are usually familiar with some or all of the internal processes of their target systems (Dallaway 2008). Some researchers refer to an insider as *"anyone who has intimate knowledge of internal operations and processes"*(Steele and Wargo 2007, 20). In addition to their free access to documents and data, insiders have wide knowledge of their organisation's system and procedure (Wood 2000). 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 acquire that knowledge without arousing suspicion (Magklaras and Furnell 2005; Althebyan and Panda 2008; White and Panda 2009). According to

Neumann (2010, 23) *"Some differences are likely to exist in the knowledge available, the knowledge required, and the knowledge actually used in perpetrating various types of insider misuse. Understanding these differences may be useful in analyses associated with detected misuses".* For instance, insiders have the ability to locate valuable information since they have greater knowledge of what to look for.

IT industry publications also support the importance of insider knowledge factor in insider threats. According to Neumann (1999, 160), *"Insiders may have various advantages beyond just allocated privileges and access, such as better knowledge of system vulnerabilities and the whereabouts of sensitive information, and the availability of implicitly high human levels of trust within sensitive enclaves".* Employees use the knowledge obtained from their legitimate tasks for illegitimate gain (Willison and Siponen 2009).

Insiders can be anyone in a company: an employee, an administrator or a contractor; whoever it may be, it is important to note that the more knowledge they have, the more sabotage they can do (Khanna 2005; Castle 2009). Despite the fact that the attacks committed by external hackers are more likely to occur, employees inside an organisation often pose silent but more harmful threats than those outside the organisation, due to their close knowledge about the organisational systems and the permissions they receive either appropriately or inappropriately for their work activities (Hu et al. 2011). Organisations must be aware that all employees know the organisation's vulnerabilities and how to best take advantage of such weakness to meet their objectives (Kirkpatrick 2008). The e-crime Survey and Ponemon Institute's Cost of Cyber Crime Study 2010 reveal that insider incidents are often far more costly than outsider breaches. This is likely because of the insider's knowledge - they are aware of the organisation's vulnerabilities and weaknesses and their security measures. Hence, insiders know what areas to target and how to obtain the information required (Blades 2010). Although, outsider attack may occur more frequently than insider, it is not as costly as an insider threat. This is because outsider threats face cracking codes, firewalls, intrusion prevention systems, email anti-virus and anti-spam. This weakens outsider attempts to attack. However, insider

knowledge is a resourceful asset he/she has to their advantage (Kirkpatrick 2008). Insider attack show planned targeted areas which an insider knows have weak security measures or vulnerable information. Perhaps a more direct approach is to launch an attack that targets theft of credit card details, or specific vulnerabilities. Targeted attacks are expected to have a bigger influence (Castle 2009). Moreover, the knowledgeable insider often has the ability to bypass established access controls. For example, an administrator with account creation and management privileges can easily masquerade as another user or administrator in order to conceal his or her activities (Ortega 2006; Buckley 2010).

Although much of the academic literature and IT industry publications reviewed above suggest that the knowledge held by employees is an important factor in insider threat behavior, the empirical evidence from reported incidents reviewed in this study has found no evidence to support such assertions.

2.4.3 Insider Technical Skills

Academic literature suggests that the insiders' technical skills and position in the organisation gives them a significant influence on cyber-crime. Attacks committed by employees in a technical position such as system administrator can result in a major financial loss to the organisation, more so than attacks by any other employees. This could be due to the increased level of access they have and their ability to hide their crimes. On the other hand, the financial losses resulting from other employees' attacks' will be less (Nykodym, Taylor, and Vilela 2005; Magklaras and Furnell 2005; Althebyan and Panda 2008; White and Panda 2009). The collaboration between a system administrator and an employee for the purpose of carrying out a crime might be extremely hard to detect and prevent since they are working at different levels of the hierarchy which may allow them to hide or cover their crime (Nykodym, Taylor, and Vilela 2005).

Furthermore, employees sometimes use their IT skills to harm an organisation'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 they are familiar with which may increase their opportunity to compromise these systems. Some researchers consider the level of employee sophistication as a potential factor which can influence their ability to commit insider crime. The levels of IT sophistication are set out below (Cohen 2001; Theoharidou et al. 2005):

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

Moreover, Magklaras and Furnell (2005) classified the end user's sophistication in terms of three essential characteristics.

- Breadth of knowledge: they indicate that advanced users are able to utilize a greater range of IT tools than intermediate or novice users.
- Depth of knowledge: The level of knowledge of some application or IT sub-domain which could be achieved either by training or individual experience is relative to the level of user sophistication.
- Finesse: the end user's ability to solve IT problems in effective and innovative ways is also considered as end user sophistication.

Similarly, IT industry publications emphasize the importance of technical skills as a factor contributing to insider threats. The most serious threat scenario to modern networks is the technically skilled outsider or insider who violates security for personal gain (Ortega 2006). Research shows that relatively sophisticated attack tools were used by insiders who compromise computer accounts or create unauthorized backdoor accounts to launch their attacks (Secret Service, Cert Analyze Insider Computer Sabotage 2005). According to Lynch (2006) and Bauch (2011), insiders

were likely to be technical employees and most often they have utilised several sophisticated attack tools.

Technically skilled employees pose a great risk to any organisation. Around 86% of insider threats were committed by technical employees most of whom were system administrators or were granted privileged system access (How to Weed out the New Insider Cybersecurity Threat 2007). Many organisations face such threats from trusted employees who have technical skills, are in a technical position and have been granted access to critical information (Lynch 2006; How to Weed out the New Insider Cybersecurity Threat 2007).

A thorough examination of incidents of insider threats reveals that most of the insiders who committed acts of sabotage held technical positions within the organisation. Unfortunately, such organisations endure financial losses that definitely negatively affect business operations. Eventually, such insider threat attacks cause greater damage to their business reputations (Lynch 2006). Organisations should acknowledge the threat of a technology-driven world, where computer operators could cause more damage than any harm that an ordinary employee could do by theft.

While theoretical academic literature and IT industry publications argue that employees in technical positions with technical skills are a factor in insider threats behaviour, 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. (2009), in all of the incidents they analysed the insider worked was 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 (Keeney et al. 2005a; Moore, Cappelli, and Trzeciak 2008; Kowalski et al. 2008; Hanley et al. 2009; CERT 2009). Moreover, Moore et al. (2009) and Hanley et al. (2011) assert that nearly 50% of the insiders involved in the incidents being studied

had held technical positions. On the other hand, the majority of the insiders in the cases analysed by King (2012) and Cummings et al. (2012) were employed in non-technical positions. Additionally, some researchers claim that less than 20% of the insiders were employed in a technical position (Randazzo et al. 2004; CERT 2006; Kowalski et al. 2008; Cappelli et al. 2008; Cummings et al. 2012).

Moreover, some of the insiders used sophisticated technical means to perform their attacks. Generally, they used several technical methods such as writing a script or program, including a logic bomb, or placing a virus on client computers, utilizing password crackers and downloading remote system administration tools. Randazzo et al. (2004) assert that approximately 10% of the incidents they analysed involved sophisticated tools or techniques. According to some insider incident reports, approximately 30% of the insiders used one or more sophisticated techniques to assist them in the attack, such as writing a script or program, establishing a backdoor account, or compromising another employee's account (Keeney et al. 2005a; CERT 2006, 2009; Hanley et al. 2009). Only two reports suggest that over half of the cases involved sophisticated technical methods (Cappelli et al. 2008; Kowalski et al. 2008).

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, such as downloading an exploit from the Internet.

2.4.4 Motivation

Academic literature asserts that motivation is one of the significant factors leading to insider threats (Wood 2000; Furnell 2006; Fyffe 2008; Walker 2008; White and Panda 2009; Sarkar 2010; Crossler et al. 2013). Insiders usually have a motive for

attacking their organisation. They often have direct physical access to the computer and they are familiar with the resource access controls. The motive for a malicious attack can be grouped into three main areas: IT sabotage, theft for financial gain, and theft for a business advantage. According to Furnell (2004, 7), motivations include *"greed, revenge, stress, and espionage, as well as being exacerbated by factors*". If employees want to attack their organisations, they are usually motivated by three things: greed, malice and/or fear. Greed is a factor when the attacker desires to achieve something from the attack, more often financial gain. Malice is a motivator when the attacker desires to cause harm to their organisation, usually as an act of revenge. Fear operates when the employee is being forced or blackmailed to perform the attack (Jones 2008b). Correspondingly, White and Panda (2009) categorised the motivation behind insiders' attacks into three main categories: IT sabotage, financial gain, and business advantage. Some of the recent attacks have been motivated by financial gain: attackers hope to gain by selling the organisation's data that resides in the database. Most often, insiders deliberately abuse the system to obtain sensitive data for financial or business gain. Moreover, Wood (2000) classified insider motivation into four groups. He believes that the insider is attempting to impose some kind of undesirable outcome within the organisation in order to achieve the following goals: profit, provoke change, subversion and personal motive. Whether the motivation is deliberate or accidental, it represents a significant risk of inappropriate user activity (Fyffe 2008). The malicious insider's motivation could involve the hope of direct personal gain, or the insider may have been recruited by competitive organisations that financially reward them for their betrayal (Walker 2008).

Once an employee is motivated to start the attack, s/he needs the opportunity to perform a harmful action. An opportunity is easily afforded by vulnerabilities such as weaknesses in access control, insufficient tasks separation, inherent technical vulnerabilities, or uncontrolled internet access (Jones 2008b). Some researchers have discussed opportunity as a motivational factor, and how the ease of access can motivate employees to abuse their organisation (Bloombecker 1984; Forester and Morrison 1994; Hitchings 1995). Bloombecker (1984) mentioned eight categories of

motivational factors. One of these is ‘the land of opportunity’, where malicious insiders abuse security gaps through their daily work. According to Forester and Morrison (1994), experts in computer crime have confirmed that opportunity more than anything else generates this kind of behaviour (Theoharidou et al. 2005; Robert and James 2006). If the insiders have a motive for harming their organisation as well as logical or physical access, and they familiar with the environment of the workplace, they can present a serious threat to the organisation (McNamara 1998; Shaw 2006).

Likewise, IT industry publications support the importance of the motivation factor in insider threats. Research has shown various motives behind threats of cybercrime. Some are created by foreign competition, while others are for personal gain (Ortega 2006). Some employees may want to violate the organisation for revenge, as a strategy for their professional advancement, or in some cases employees just may simply be looking for a quick way to skim off some finances. Unfortunately, the motives that drive each threat vary from one to another. Hence, it is very important to discuss the motives behind these threats for future protection screening (Blades 2010).

A study by Vista Research in 2002 revealed that insider threat represents 70% of the security violation, which is often committed by disgruntled employees (D'Arcy and Hovav 2007). Although there is a common statement that insider threats are made by a disgruntled employee or for a financial scam, some research which has examined threats and conducted surveys in this area show that this proposed motive may be just a myth. Nevertheless, a study of incidents from a behavioural and a technical perspective reveals that great deals of threats were motivated by the prospect of financial gain (Kirkpatrick 2008; Blades 2010). Hence, the advancement of an insider’s position through financial gain or career benefit is identified as a primary motivator. Some research has linked financial gain or benefit to an insider’s greed. Greed is often referred to as motivation for theft, in particular of proprietary information. Hence, reports cite greed as a motivational factor that drives insider threats. The PWC survey identified the need to sustain a luxurious lifestyle as a

specific motive. Moreover, they added that being in debt also may drive a threat to gain more money (Lynch 2006; Kirkpatrick 2008). Moreover, unsatisfied individuals may act in ways to attract negative attention. Disgruntled employees have the urge to avenge themselves by causing the organisation financial losses or simple loss of reputation. In the case of disgruntled employees, these unsatisfied employees want the organisation to report an insider threat to the police, stating that a disgruntled employee has done such and such, which will affect the company's reputation. Disgruntled employees want to harm or embarrass the organisation. However, in such cases it is easier to uncover the potential threats of an insider. In many cases, there were warning signs that disgruntled employees would launch an attack. Hence, organisations are responsible of monitoring such behaviours to look for signs of threat (D'Arcy and Hovav 2007; Kirkpatrick 2008; Willison and Siponen 2009). The USSS/CMU-SEI financial services study on insider threat incidents shows that in 85% of the cases, someone close (a co-worker, a friend, or a relative) knew of the insider's plans, motives and actions against the organisation. In the banking and finance sector, 19% of insiders were seen as disgruntled. About 27 % of the insiders had displayed obvious signs to the supervisor and co-workers that an attack was being planned. Such behavioural attitudes include increasing complaints that show dissatisfaction about the wages, an increase in time wasted on the cell phone in the office, refusal to work or communicate with new supervisors, increased outbreaks and conflicts, and isolation from co-workers (Kirkpatrick 2008).

In addition, some employees are motivated by patriotism. Espionage activities to obtain intelligence may in some cases be sanctioned and organized by foreign governments (Bauch 2011). There are several reasons for this: to keep local companies aware of their global competitors, and to retain the stability of their economic status. For many years France, China, Latin America and the former Soviet Union have used espionage as a common strategy to promote their country's economy. Such motives are very professionally planned and executed and are hard to prevent. Such employees usually have excellent performance charts and show no suspicious signs.. For example, two former distinguished employees from China were employed in an American organisation and were indicted for stealing trade

secrets to transfer to a joint venture with a Chinese telecommunications company (Kirkpatrick 2008). The rise of profit-driven cybercrime is the major motivator in many cases, while the involvement of foreign nationals and political motivations raises the spectre of network-based attacks against critical national infrastructure (Ortega 2006).

Furthermore, in some ongoing research it has been noted that some insider threats may be motivated by terrorism because the insider wants to threaten or harm those who have different ideologies or beliefs or goals from their own. For example, an insider could carry out a threat in the name of a terrorist group to harm the company or others because of their different ideological beliefs. In ongoing investigations, suspected plots of insider threats have been researched domestically and internationally (Kirkpatrick 2008).

Research has also indicated that insider threats can stem from the urge to advance one's career. The perpetrator in such cases commits to a threat by information theft of vulnerable data or codes that may be used to secure another job. In other circumstances, the insider may feel unsatisfied with the company's management policies or targets. Hence, the insider feels that he/she may do better by competing against his/her own company in the market place. Such insider threats may include exposing the company's secret information or assets. For example, a retired manager stole blueprints of his organisation and sold these to a Chinese organisation to set up his own company (Kirkpatrick 2008).

As mentioned earlier, there are various motives that drive insider threats, all of which should be addressed seriously by organisations. Organisations must be aware of the valuable information they hold and who has access to such information. Also, organisations must consider meeting their employees' needs in terms of career satisfaction and financial gains.

Evidence from reported incidents supports the theoretical positions found in the academic literature as well as the IT industry publications, 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 organisation's infrastructure. Insiders stole information to sell it, and modified data to achieve financial benefits for themselves.

Financial motivation accounts for less than half of the insider incidents; other motives include revenge, frustration with organisation management, culture or policy dissatisfaction, and sometimes that insiders were persuaded by outsiders (CERT 2006; Cappelli et al. 2008; Kowalski et al. 2008; Hanley et al. 2009). On the other hand, all of the insiders involved in organised crime cases attacked the organisation for financial gain (King 2012). Most of the insiders' cases analysed by King were motivated by financial gain and were employed by outsiders to commit their crimes. Organised crime is *"involving multiple insiders who often work in different areas of the organisation and who know how to bypass critical processes and remain undetected. Those insiders affiliated with organised crime are either selling information to these groups for further exploitation or are directly employed by them"(King 2012, 1).*

Researchers have suggested that as many as 84% of the incidents were motivated by revenge (Keeney et al. 2005a; Moore, Cappelli, and Trzeciak 2008), the second category of motivation. In Hanley et al. (2009), 80% of the incidents were motivated by a desire for revenge against their company. According to CERT (2006), CERT (2009) and Cummings et al. (2012) over half of the incidents they analysed were vengefully committed as retaliation for a negative event such as transfers or termination, salary or employer dissatisfaction, new managers, and demotions. Kowalski et al. (2008) 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. (2009) and CERT (2009) 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. (2009), 32% of the insiders analysed were acting to gain an immediate advantage at a new job and in 22% of the cases analysed by Cummings et al. (2012), the insider was motivated by competitive business advantage.

If the insiders have a motive for harming their organisation as well as logical or physical access either authorised or unauthorised, and they are familiar with the environment of the workplace, they can present a serious threat to the organisation (Shaw 2006).

2.4.5 Information Security Policy

Researchers in the academic literature claim that information security policy is one of the key factors that influence the insider threat behaviour (Cohen 2001; Magklaras and Furnell 2002; Pramanik, Sankaranarayanan, and Upadhyaya 2004; Furnell 2006; Walton and Limited 2006; Bishop et al. 2008; Hu et al. 2012; Crossler et al. 2013). Insider threats are affected by several aspects related to information security policy including the implementation of inappropriate policy for the information security and the technology, insufficient security training and awareness and out-dated security policy. Installing an appropriate information security policy, keeping it up to date and providing suitable training and awareness are vital tasks which require far more than just writing a security manual. Each organisation needs to know who has access to the data, what their own access policies are, and what actions they take to access data (Pramanik, Sankaranarayanan, and Upadhyaya 2004). According to Canavan (2007, 7) *"information security policy defines the organisation 's attitude to information, and announces internally and externally that information is an asset, the property of the organisation , and is to be protected from unauthorised access,*

modification, disclosure, and destruction". Information security policy provides guidelines that organisations can follow to protect their physical and information technology assets. All employees should follow the security policy to minimise the risk and to respond to any security incidents effectively. In general, a security policy determines that actions that are authorised for a specific user and purpose. For example, a security policy may state that employee X is authorised to read Y records in order to update the data. If employee X deletes the records, he is violating the security policy. The security policy will also be violated if he reads the records for the purpose of selling the information. Moreover, the security policy is violated if anyone else uses employee X's user account to read the records. This example reveals that security policies may state rules that are difficult to put into action. Users are able to misuse their privileges because the computer systems do not recognize people, only user accounts (Bishop et al. 2008). Therefore, organisations require a detailed security policy that focuses on human factors as well as physical and technical factors (Gaunt 1998).

Security policy, procedure, controls, guidelines and training are isolated from changes. Some executives responding to the EIU (2009) survey assert that their organisations have formulated IT policies to regulate the use of devices by employees, but not many 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"* (Furnell 2004, 4).

Some evidence suggests that the problems faced by organisations from internal threats are being reported along with matching evidence of insufficient security training and awareness (Furnell 2006). Security training and awareness are two areas on which an organisation must focus, and apply these in order to reduce the insider threats. Awareness among all kinds of employees is a vital element of the information security policy performance of any organisation (Albrechtsen and Hovden 2010).

An information security culture is defined as *"the attitudes, assumptions, beliefs, values and knowledge that employees/stakeholders use to interact with the organisation's systems and procedures at any point in time"*(Da Veiga and Eloff 2010, 198). If employees know that there is an effective security culture and that their colleagues apply it, this could make a difference. It would seem logical to expect that if organisations were to adopt a more responsible approach, the change will reduce the insider threat risks (Cohen 2001). Conversely, security culture could assist the insider to harm his/her organisation (Da Veiga and Eloff 2010). The bad news is that some existing security cultures are not keeping up to date and have no quick way to change (Walton and Limited 2006).

However, even if the security policy is appropriate and up to date, misuse of the policy is carried out by human factors either by violation or abuses (Magklaras and Furnell 2002). Therefore, human factors are the central issue. Security policy violation occurs when employees do not heed the organisational security policies. These include, for instance, copying or transferring confidential information to mobile devices, disabling security configurations, and leaking sensitive data to outsiders. Abuses of the information security policy include any employees' actions using computers against the organisation's established policies and procedures for personal gain. For instance, this may include accessing information and systems illegally, illegitimated copying of sensitive information, and selling sensitive information to a third party for personal gain (Guo 2013).

IT industry publications support the theoretical positions found in the academic literature, indicating that information security policy is one of the significant factors in insider threats. Establishing a suitable security policy is a fairly straightforward process, although it may be overlooked (Blades 2010). According to D'Arcy and Hovav (2007, 116) *"users' awareness of security-policy statements and guidelines decreases the likelihood that they will engage in IS misuse".* It is a challenge for organisations to find the balance between security policies and measures and productivity where there is no "one size fits all" policy; this depends on the industry and the sensitivity of data. For example, an organisation that conducts a military

study should have a policy that offers little or no flexibility. Even financial service organisations require strictly fixed policies that guarantee the safety of sensitive client information. Hence, security measures are often seen as a competitive advantage in such sensitive industries. Organisations must understand their industry requirements in order to determine the type of security policies they need to achieve productivity in a secure manner (Khanna 2005; Blades 2010; Ford 2012). Once the level of security needed is identified, which depends on the nature of the business, then the appropriate policies can be established and implemented (Hu et al. 2011).

Although most organisations have long-standing policies that govern email usage and network access, they fail to estimate or address the impact of new technologies that may pose further security risks. Technologies such as viruses, removable media storage devices such as USB thumb drives, iPods, and smart phones should be addressed in security policies. If the impact of new technologies and trends is not addressed, over time this may certainly lead to substantial security breaches (Steele and Wargo 2007). An information security officer at the University of Rochester in New York suggests that the best way to address insider threat is to establish an ongoing awareness program. Such a program should include IT staff, end users, corporate executives and external partners (Jaikumar 2005). Having a comprehensive security policy is one thing, but actually implementing such policy is something different altogether. Unfortunately, security measures are often considered to slow the process of productivity. Moreover, many organisations implement policies and forget them once they are there. However, without appropriate enforcement, and reminders of the policies put in place, employees, like their organisations, will forget that such policies are there for a reason and will find ways to circumvent the process of policies to speed up their productivity and be able to leave work early (Steele and Wargo 2007).

Organisations are reluctant to ask their employees to take time out to update their skills through training programs to ensure they are taking the right measures regarding security. Nevertheless, a security policy is useless if not taken seriously. Therefore, employees must be adequately trained through various channels of

communication to understand that they are expected to follow policies and procedures. As mentioned earlier, organisations find it a challenge to keep their employees interested in training facilities; thus organisations must create inspired ways to increase employee participation in training and education (Steele and Wargo 2007; Blades 2010). Such training programs must explain or give examples of security breaches that may have occurred. Employees must understand the consequences that may rest on their shoulders if a breach occurs. It is also very useful to emphasise the organisation's custodial role in protecting data related to their customers and employees. One of the few things that scare individuals is identity theft; therefore, an explanation of how such activities could occur in an organisation and how this could potentially breach security, is also very effective. Hence, the need to protect one's own identity is seen a useful method to keep employees always engaged in such training programs. More importantly, the changing landscape of technology should be emphasised. Awareness must be raised of such technologies and the risks they create. Therefore, employees must know how new devices, gadgets and software programs fit into the policy, and how the risks that such technologies bring to the table can be minimized (How to Weed out the New Insider Cybersecurity Threat 2007). It is an ongoing challenge to keep such mandatory training alive and repetitive without making it boring. Keeping training programs interesting can be difficult; therefore, organisations may want to consider using a third party to provide such training services. Moreover, for ongoing reminders of policies and security measures, administration should always send out reminders and emails as methods of keeping their employees up to date and reminded (Steele and Wargo 2007; Addressing the Insider Threat 2007).

Despite the fact that theoretical academic literature and IT industry publications argue that security policy and policy culture are factors in insider threat behaviour, empirical evidence from reported incidents varies. 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.

In 70% of the cases studied by Randazzo et al. (2004), insiders had broken through or tried to break through systemic vulnerabilities in processes, procedures or policies to launch their attacks. In 61% of these cases, the insiders exploited weaknesses inherent in the design of the hardware, software, or network. While, in 39% of cases, the insiders were unaware of the technical security measures in their organisation. Kowalski, Cappelli and Moore (2008) assert that in 62% of the cases they studied, the insiders violated systemic vulnerabilities in policies, processes, procedures or applications. Most of these violations occurred because of a lack of physical and technical access controls, thereby facilitating the insider theft. Moreover, Kowalski et al. (2008) claim that in half of the incidents they analysed, 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 addition, 33% of incidents occurred because of security policy violation (Cappelli et al. 2008). On the other hand, Spooner et al. (2009) declare that none of the insiders exploited any technical vulnerability or security policies when carrying out their thefts.

2.4.6 Psychological Factors

The greatest security threat arises from the authorised employee. *"People design, develop, and use as well as misuse information systems. It is, therefore, necessary to understand the psychology of people involved in both malicious and non-malicious insider activity"*(Sarkar 2010, 114). Some resarchers have attempted to study the psychological profiles of insiders who were likely to offend, before the incident. Many researchers want 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 reliably discovering potential criminals in advance. Criminals differ in their motivations and psychological make-up.

Thus, while it should be possible to identify some types of very antisocial behaviour, it remains very difficult to identify other offenders because they can conceal themselves from prior 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 behaviour. In addition, insiders' threat activity can gradually evolve from non-malicious intent to more malicious intent (Pfleeger 2008).

A psychological screening could be performed before an employee is hired (Sarkar 2010). A rigorous psychological evaluation might be sufficient to identify possible inside attackers although 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 whether or not the employee would be beneficial to the organisation (Pfleeger 2008).

As a result of this dilemma, even if such a psychological test existed, its use might be counterproductive. Predictions do not seem reliable in the budding field of psychological profiling. The relative lack of cases to work with, the poor understanding of the best definition of average acceptable behaviour, and the ambiguity in the identification of the boundary between acceptable and unacceptable behaviour, all combine to make the development of useful psychological profiles difficult (Pfleeger 2008).

However, Shaw, Ruby, and Post (2005) assert that there are numerous features that, when found together, could indicate and increase the possibility of identifying potential harmful behaviour on the part of the insider. These features are: computer dependency, a history of personal and social frustrations, ethical lapses, a sense of entitlement, reduced loyalty and lack of empathy (Sarkar 2010).

Another major use for psychology is a positive one: the development of ways to support good behaviour. 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 hiring a good employee or refusing somebody who has not yet demonstrated harmful behaviour; the risk of a false negative is the failure to detect or prevent an attack (Pfleeger 2008).

While the theoretical academic literature is diverse in regard to the psychological factors, IT industry publications support the significance of such risk factors in insider threat. There are some psychological characteristics which, when exhibited by an employee, could indicate an increase in the likelihood of inappropriate behaviour; these include: a sense of entitlement, computer addiction, personal and social frustrations, rationalize their violations, lack of empathy and reduced loyalty. Some studies show that a key characteristic of many of the insider attackers was a sense of personal entitlement. This is a personal feeling that one is special and better than others, and therefore should be better recognized or privileged. This feeling, accompanied by pre-existing anger toward authority figures, creates a desire for revenge. In these cases, psychological factors and emotions may spur employees to plan an attack. According to Professor R. Caldwell, a computer scientist who led separate studies in 1990 and 1993 recognized that some individuals suffer from "revenge syndrome." Some unfortunate individuals experience a series of negative incidents in their lives and frequently have a history of personal and social frustration. In most cases, abused and neglected children display this syndrome which is characterised by feelings of anger, hostility towards authority, lack of social skills, and a tendency to attack and walk out on the system (Steele and Wargo 2007).

According to psychologists, computer-addicted characters are more likely than non-addicted users to become aggressive, lonely people who are incapable of making friends or being team players. Psychologists report that such people are mainly interested in exploring networks, and breaking through security codes and measures in order to compete and challenge the professionals. Moreover, many insiders do not believe that their violations and actions are criminal or unethical. Instead, some justify their actions because of their circumstances. These individuals lack moral

self-consciousness that may prevent others from committing such violations. Similarly, a research on ethical limitations within the "information culture" conducted by S. Harrington and published in 1995 reported that almost 7% of computer experts do not object to hacking or doing harm to a network. Unfortunately, according to their rationale, if a network is not sufficiently secured, it is only fair game to crack it. In addition, some studies reported that IT employees had the tendency to identify more with their expertise and skills rather than with their employer. Similarly, a study of computer fraud conducted by the U.S. Department of Health and Human Services in 1986, found that computer programmers and experts who engaged in scams felt more loyal to their skills than to their employer (Steele and Wargo 2007).

According to Hu et al. (2011), employees with low self-control are more likely to commit the violations. In contrast, individuals who have strong moral beliefs are less likely to abuse their organisation even if the opportunities exist.

In light of the implication that insiders are irritated first and attack later, the MERIT learning tool emphasises the relationship between them. This suggests that an insider threat may be detected before it actually occurs if the managers or supervisors are able to detect suspicious or concerning behaviour. Concerning behaviour includes decrease in performance, and behavioural antics that cause frustration and unpleasantness to others. Managers are urged to keep a close eye on employees who are disgruntled after a negative work-related episode. It is also recommended that they monitor the employee's online activity after the incident. In cases of such obvious and unexpected changes of attitude, companies may have a window of opportunity to detect a hidden security threat and perhaps prevent an incident from taking place. Although the organisation cannot monitor all employees' online actions, it is easier to target suspicious employees and monitor them. Targeted monitoring of online activity by employees of concern can assist in the detection and prevention of insider threats (How to Weed out the New Insider Cybersecurity Threat 2007).

Organisations should ensure that their recruitment screening policies enable thorough background checks of their employees. Managers should be made aware of red flags that can be observed in the employee's attitudes and communication skills (Kirkpatrick 2008)

Although the theoretical academic literature is diverse in regard to the psychological factors, empirical evidence from reported incidents support the IT industry publications that personal predispositions and behaviours are a common factor in internal incident cases. According to the United States Secret Service and CERT, about 80% of insiders who performed attacks on their organisations had demonstrated negative behaviours before the incident, and 92% had experienced a negative occupational event such as a demotion, transfer, warning, or termination (Cole 2008). According to Moore, Cappelli, and Trzeciak (2008) the majority of the insiders in the MERIT cases who committed IT sabotage demonstrated the impact of personal predisposition. Personal predisposition is *"a characteristic historically linked to a propensity to exhibit malicious insider behaviour"* (Moore, Cappelli, and Trzeciak 2008, 12). 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 (Band et al. 2006). 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 because of troublesome behaviour before the incident (Moore, Cappelli, and Trzeciak 2008). 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 (Keeney et al. 2005a). According to Cappelli et al. (2008), 60% of the insiders had exhibited several incidents of concerning behaviour or activity before the incident occurred, such as delays, absences and poor job performance. Their figures indicate that 55% of the criminal insiders displayed a noticeable worrisom behaviour prior to the attack and 38% of the insiders had been arrested previously. Kowalski et al. (2008) report that

in 43% of cases the insiders demonstrated inappropriate behaviour before the attack and about 31% of the insiders had been previously arrested. These individuals were arrested for: financial or fraud offences (14%), nonfinancial offences (6%), drugs or alcohol offences (3%) and violent and other offences (6%).

2.4.7 Cultural Factors

Organisational culture shapes the employees' behaviour and this may dominate the security policies and processes (Sarkar 2010). Organisational culture is defined as *"the shared values, norms and expectations that direct the way people approach their work and interact with each other"* (Colwill 2009, 5). According to Royds (2009), 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 behaviour. The culture of an organisation can influence the behaviour of employees and eventually contributes to the effectiveness of an organisation. In almost all organisations, information is considered to be a critical asset; consequently, an ideal organisational culture should incorporate information security controls in the daily tasks and implicit behaviour of employees (Thomson and von Solms 2006). Most organisations experience some kind of transformation at some stage in their development. Original organisation cultures are often dismantled and rebuilt, including the concepts and behaviours used to achieve security. However, if cultural changes are not addressed explicitly, they can cause fear, ambiguity and doubt in employees, which can impact on their attitudes to security (Ashenden 2008; Crinson 2008).

Additionally, culture differences can affect the insider threat behaviour since the acceptable traditions for doing business differ according to region and area. For example, some practices considered illegal in the Western world may be acceptable in other parts of the world, such as the giving of substantial gifts (Colwill 2009). According to Luo and Shenkar (2011), the friction between employees is not only a

result of the culture differences, but also can be a product of the nature of the interface between them. Cultural differences to some extent produce a clash, which is exacerbated the more the conflicting cultures interact with each other.

Although much of the academic literature reviewed suggests that cultural factors are important in insider threats behaviour, not many IT industry publications support this claim. Only one paper discussed culture as a factor. Kirkpatrick (2008) claims that employees with different cultural backgrounds may have different levels of awareness of law and ethics regarding theft. This can increase the problem of insider threat. Moreover, some countries expect their citizens to help their home country when working abroad.

Moreover, empirical evidence from reported incidents reviewed in this study varies in its support of the highlighted factor. No single country or region was frequently represented. According to Kowalski et al. (2008), insiders did not share a common national or regional culture and 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. (2009) confirm that insiders come from different lands: 50% were American, and 40% were foreign nationals including Chinese and Taiwanese. Another study by Keeney et al. (2005a) emphasised that insiders were demographically diverse with regard to culture and ethnic background, age, gender and marital status. On the other hand, Cummings et al. (2012) maintain that only eight cases out of 46 (17%) involved citizens of a foreign country, while 83% of the cases were American.

2.4.8 Outsourcing

The academic literature maintains that there are rapidly increasing numbers of third-party workers being given long-term access to organisations' 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 an organisation’s employees and members of the third party (Shaw, Ruby, and Post 1998). Many organisations outsource IT tasks to third parties who have the expertise for such tasks. There is a high risk of data abuse when outsourcing jobs with confidential data to a third party (Sarkar 2010). Contractors’ employees may be given a level of logical and physical access equal to that of an organisation’s full-time employees (Shaw, Ruby, and Post 1998). The dynamics of the labour force in the market and the increased rate of worker turnover could lead to an increase in the vulnerability of organisations, to loss of intellectual property and the probability of high value or high impact knowledge being transferred to a competitor or other external sources. This provides the opportunity for malicious insiders, who now have access to collections of information that have not previously been collected, to harm the organisation (Whitworth 2005; Colwill 2009). According to Cole and Ring (2005), outsourcing is becoming a norm for almost all organisations regardless of size. They point out that outsourcing presents new challenges and concerns that all organisations should to be aware of. Through outsourcing, the organisation will increase the scope of insiders to include the outsourcing company.

Similarly, IT industry publications emphasize that outsourcing could contribute to insider threats. According to (Bucki 2011, 1), outsourcing is *“any task, operation, job or process that could be performed by employees within an organisation, but is instead contracted to a third party for a significant period of time. In addition, the functions that are performed by the third party can be performed on-site or off-site*”. An organisation signs an agreement with another outside company to perform the tasks or functions of an entire department. In both cases, the management control is in the hands of an outsider. In such cases, organisations must understand that each company is driven by different standards, missions and managerial styles; most importantly, organisations must understand that all outsourced employees or outsourced companies will be driven to make a profit from the services they provide (Khanna 2005).

Outsourcing organisations should consider the associated risks. Outsourcing employees could put vulnerable and confidential information at risk and increase the possibilities of security breaches. Each and every business runs on the valuable knowledge it has gained through its business experience. Confidentiality could be compromised if such valuable knowledge is easily handed over to outsourced employees, since confidential information is at risk of being transferred elsewhere. Organisations should take into account the level of information that outsourced employees have access to, their knowledge, and sharing proprietary. Therefore, organisations should first investigate the outsourcing company to ensure their data will remain protected. Then, companies should state clear warnings in the contract and include a penalty clause in case an incident occurs (Blades 2010; Financial Institution Security Risks and Concerns: The Top Eight 2007).

While academic literature and IT industry publications suggest that outsourcing is an important factor affecting behaviour 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 only 8.7% of all CERT insider threat cases involved contractors (Lewellen et al. 2012). Many reports did not indicate this as a significant factor; and those reports which mentioned this factor did not give it much attention. Most of the reports studied state that contractors were involved in less than 20% of insider incidents. According to Kowalski et al. (2008), 16% of the insiders at the time of the incident were contractors, sub-contractors, or temporary employees. In all insider incidents analysed by Kowalski, Cappelli and Moore (2008), 18% only were contractors. Cappelli et al.(2008) declare that in only two out of fifteen cases they analysed were there contractors or outsourcing employees involved, and all were current employees.

2.4.9 Remote Access

Some of the academic literature discusses the importance of remote access in insider threat. According toBlackwell (2012); Cole and Ring (2005), remote access can

establish a great opportunity for the insiders to attack their organisation. As stated by Sarkar (2010, 123)*"Working from home, working strange hours or remotely could mean that the employee do not wish his activities be noticed by his co-workers or his supervisors".* Shaw (2006) examined several law enforcement files and noticed that in most of the cases, the employees attacked remotely. Moreover, mobile devices were able to access the organisation's network remotely and load sensitive data, exposing the data to possible loss or theft as the data on mobile devices are usually not encrypted or backed up. According to Sarkar (2010, 120), *"any device like a laptop, a PDA or a mobile that accesses a corporate network or stores data is a potential risk to intellectual property or sensitive customer data. These portable devices are a great source of data leakage".* Disgruntled employees who have authorised access to confidential information could copy this information to their mobile devices and sell it to third parties for personal gain (Aldhizer and Bowles 2011).

IT industry publications support the theoretical positions found in the academic literature, indicating that remote access is a factor in insider threats. According to IT industry publications, remote access is one of the factors contributing to insider threat. Remote access technologies similar to Virtual Private Networks (VPN) give individuals the privilege to access a private company's system from a computer anywhere in the world. Although there are numerous advantages to remote access such as business convenience, especially for those who need to work from home or who are travelling (Data Insecurity—Is Not Knowing the Cause Part of Your Problem? 2008), the risks are also considerable. Viruses may be lodged onto the network or system through remote access. Hence, information theft may be easily committed through remote access (Griffin 2009; Bauch 2011). Researches have shown that mobility has indirectly caused insider threats of information theft or breaches. The granting of remote access increases the risks although employees may be unaware of such breaches (Secret Service, Cert Analyze Insider Computer Sabotage 2005; Data Insecurity—Is Not Knowing the Cause Part of Your Problem? 2008; Castle 2009; Assessing the Seriousness of Security Threats from Employee

Misuse of It Resources 2009). Moreover, establishing and maintaining unauthorized remote access can lead to serious malicious actions (Bauch 2011).

Despite the fact that theoretical academic literature and IT industry publications argue that remote access is a factor in insider threat behaviour, empirical evidence from reported incidents varies. Some of the reports show that a high percentage of the crimes are committed through remote access, while others report only a small percentage. Employees can access the organisation's networks from outside the workplace, from their homes or elsewhere. Several researchers claim that the number of crimes which were carried out through remote access is significant. In 87% of the cases studied by Keeney et al. (2005a), the victim organisations gave their employees remote access, and in 56% of the incidents, the attacks were carried out through remote access. Most of the insiders in IT sabotage cases used remote access to launch their attack, and in 30% of the fraud cases, the insiders used remote access (CERT 2006). According to Moore, Cappelli, and Trzeciak (2008) in 64% of the cases they studied, the insiders used remote access to attack. Half of the cases reported in (Hanley et al. 2009) used remote access to attack. In about 43% of the cases, the insider attacks were conducted via remote access from outside the workplace (Kowalski et al. 2008). Randazzo et al. (2004) report that 30% of the attacks were carried out from the insiders' homes via remote access and 57% of those were attacks carried out both from the workplace and from home. On the other hand, some reports maintain that less than 20% of the incidents were conducted via remote access (Cappelli et al. 2008; Moore et al. 2009; Spooner et al. 2009; Hanley et al. 2011).

2.4.10 Gender

There is almost no academic or IT industry literature investigating gender as a factor in insider threat behaviour. 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 threat behaviour.

According to Moore et al. (2009), in 82% of overall CERT cases, the insider was male and 91% of the insiders who stole intellectual property were male. Another study indicates that 94% of the insiders were male (Hanley et al. 2011). Males committed 90% of the crimes studied by Spooner (2009). In another study, 96% of the insiders were male (Keeney et al. 2005a). Insiders who carried out IT sabotage were mainly male and males constituted 80% of the insiders who stole secret proprietary information (CERT 2006). The majority of the insiders were also male in the research by CERT (2009) and Hanley et al. (2009). However, some reports indicate that the numbers of males and females were equal; in a study presented by Kowalski et al. (2008), 50% of the insiders in cases were male and 50% were female. Cappelli et al. (2006; 2009) support the contention that half of the insiders were male and the other half female in cases of fraud and theft for financial gain. On the other hand, 31% of the insider fraud cases analysed by Cummings et al. (2012) were committed by males and 69% were committed by females. Likewise, King (2012) found that the majority of the insiders in the analysed cases were female.

2.5 Insider Threat Models

One of the major obstacles to the detection and prevention of insider attack is that very few studies on this subject have been designed to solve the problem in a broad, comprehensive manner. Most of the models which have been studied for this research focus on the insider threat for specific problems within specific organisations. Several models have recently been presented to detect and prevent insider threat and most of these have focused on technical issues; however, very few have discussed the social, cultural and demographic factors. Insider threat models that are representative of the research space are set out below:

- Parker (1998), developed a model based on a list of factors which includes skills, knowledge, resources, authority, and motives and used it to insider and outsider attacks almost for all cybercrime. This model omitted several other

factors which relate to insider behaviour such as culture and background. Wood (2000) proposes a model based on the insider's motivation. The insider should have a motive for the attack, a target, and the ability to launch the attack. This model focuses only on one factor and does not consider other factors such as technical and social factors.

- Gonzalez and Sawicka (2002) developed a systems dynamic simulation model to discover complex security problems; the purpose of their research project was to gain an understanding of the role of human factors in information security systems. They used a simple case to demonstrate how system dynamics may provide insight into the people security problem and help in designing robust security policies. The model focuses on human factors and does not address other insider threat issues such as the technological and organisational environments.
- Magklaras and Furnell (2005) presented a model for insider threat prediction based on one factor which is end user sophistication. This model considers the sophistication of an end user as a potential factor that influences their ability to comment insider misuse. The Magklaras and Furnell model ignores many other factors that relate to insider misuse such as insider motivation, access, culture and psychological factors.
- Hu, Bradford and Liu (2006) developed a model for detection of insider attacks by intrusion detection systems based on the assumption that an insider is described by job function. However, the influence of social insider factors is not considered in this model.
- Althebyan and Panda (2007) developed a model of insider threat prediction, focusing on two: the insider's knowledge and existing dependencies among objects in the system. Their model limits the possibilities for the insider to gain access to documents and obtain sensitive information from the organisation. This model however, focuses on cyber insiders and does not consider social insiders.
- Another model presented by Jones (2008a) focused on organisational factors such as changing environment, social and business cultures to catch the

malicious insider and to mitigate their threat to the organisation. Nevertheless, the influence of human and technical factors is not considered in this model.

- Moore, Cappelli, and Trzeciak (2008) presented a system dynamics model of the insider IT sabotage problem, where the insider's main aim is to harm some parts of the organisation such as business operations, information and the system or network. Their model mostly focuses on one primary problem; they did not consider any other types of insider threat such as fraud or the theft of sensitive information.
- Pfleeger et al. (2010) presented an insider threat model which described insiders and their actions based on the organisation, the environment, the system, and the individual. They gave several examples of inappropriate insider action such as theft of intellectual property, tax fraud and proliferation of e-mail responses, and demonstrated how each situation arose and how it could be addressed. This model could be considered as a good step in understanding insider threat because previous research focused on malicious insiders, while their study suggests that unintentional insider action can be just as debilitating to any organisation. However, their model does not address several factors such as remote access, whether the insider is outsourced, the descriptions of insider motivation for instance, whether an insider's action was motivated by financial gain or by revenge.
- Sasaki (2011) proposed an insider threat detection model generating a trigger that made malicious insiders carry out suspicious actions such as deleting files and e-mails. This model focused mainly on technical issues without considering other factors such as personal and organizational issues.
- The last model considered here is that of Brdiczka et al. (2012) who presented an approach for insider threat detection by combining inconsistency detection from social and information networks with psychological profiling of individuals. Their approach could be implemented in any organisations' communication data such as email or IM, file accesses, and login data.

However, this model omits many factors such as organisational, environmental and cultural factors.

2.6 Research Gap

Most of the studies that were examined include insider threat models but these models were not empirically validated or tested and most of the papers present non-validated defence methods against insider threat. In addition, nearly all of the previous models focus mainly on one primary problem, and only one model addressed four factors. None of the reviewed models addresses all the ten factors identified in the literature and very few models consider both technical and human factors (see Table 2.4). Little can be found in the previous sources regarding social, cultural and demographic factors and their effects on the insider threat. Moreover, the scopes of prior studies have been limited to specialised areas, resulting in isolated findings, where many factors related to insider behaviour, such as culture, background and education, have been omitted. Hence, there is a research gap, because although a number of academic research models explain the insider threat behaviour factors, none of these captures all factors. These missing aspects constitute knowledge gaps. Providing specific models of the insider threat without making a holistic contribution only adds to the obstacles preventing insider threat, as stated by Huth et al. (2013, 2) *"an approach is necessary to provide holistic solutions to the problem of insider threats".* Thus, there is a need for a holistic model that combines all these different factors, thereby more accurately reflecting the real world situation.

Furthermore, as well as the need for a holistic model, there is a need to verify each of the factors in the holistic model, because of the disagreement of the academic literature and the previous cases some areas. The factors contributing to insider threat were not equally supported by all three sources (academic, IT industry publications and reported incidents) studied for this research. Research has produced conflicting results. For example, academic sources support the importance of a security policy as they suggest that a good one could prevent insider threat; however, reported incidents

found that security policies have limited effect. As can be seen from Table 2.5, the practitioner view does not match the academic view, as some sources strongly support some factors while other sources have highlighted others. There are areas where the academic research does not sharply reflect the actual insider threat incidents. Therefore, further investigation is necessary in order to identify the main contributing factors to insider threat behaviour.

Therefore, the overall aim of this research is to develop a holist insider threat model of the factors that influence insider threat behaviour. To the best of the researcher's knowledge, there is no published study that provides a holistic view of the insider threat contributing factors that address the three sources studied for this research (academic, IT industry publications and reported incidents). Therefore, this study intends to fill this empirical research gap.

Table 2.3: Insider threat models

Models	Access and level of trust	Insider Knowledge	Insider IT skills	Motivation	Information security	Psychological factors	Cultural factors	Outsourcing	Remote access	Gender
Parker (1998)	✓	✓	✓	✓						
Wood (2000)				✓						
Gonzalez and Sawicka (2002)					✓					
Magklaras and Furnell (2005)			✓							
Althebyan and Panda (2007)		✓								
Jones (2008a)							✓			
Pfleeger et al (2010)							✓			
Sasaki (2011)	✓									
Brdiczka et al. (2012)	✓					✓				

Table 2.4: Insider threat contributing factors and the three sources

Factors	Academic sources	IT industry publications	Reported Incidents
Access and level of trust	**The following references support access and level of trust as a factor:** (McNamara 1998; Wood 2000; Cohen 2001; Furnell 2004; Kemp 2005; Nykodym, Taylor, and Vilela 2005; Walton and Limited 2006; Okolica, Peterson, and Mills 2006; Contos 2007; Swartz 2007; Althebyan and Panda 2008; Bellovin 2008; Dallaway 2008; Fyffe 2008; Liu, Wang, and Camp 2008; Walker 2008; Liu, Wang, and Camp 2009; Sarkar 2010; Willison and Warkentin 2013)	**The following references support access and level of trust as a factor:** (Thompson and Ford 2004; Ansanelli 2005; Secret Service, Cert Analyze Insider Computer Sabotage 2005; Khanna 2005; Lynch 2006; Ortega 2006; Addressing the Insider Threat 2007; Financial Institution Security Risks and Concerns: The Top Eight 2007; How to Weed out the New Insider Cybersecurity Threat 2007; Roberts 2007; Kirkpatrick 2008; Castle 2009; Chickowski 2009; Wehrum 2009; Blades 2010; Messmer 2010; Bauch 2011)	**The following references support access and level of trust as a factor:** (Randazzo et al. 2004; Keeney, Cappelli, et al. 2005; CERT 2006; Moore, Cappelli, and Trzeciak 2008; Kowalski et al. 2008; CERT 2009; Moore et al. 2009; Hanley et al. 2009; Spooner et al. 2009; Cummings et al. 2012; King 2012).
Insider knowledge	**The following references support insider knowledge as a factor:** (Wood 2000; Magklaras and Furnell 2005; Steele and Wargo 2007; Althebyan and Panda 2008; Dallaway 2008; White and Panda 2009; Neumann 2010).	**The following references support insider knowledge as a factor:** (Neumann 1999; Khanna 2005; Ortega 2006; Kirkpatrick 2008; Castle 2009; Willison and Siponen 2009; Buckley 2010; Blades 2010; Hu et al. 2011).	**There were no references addressing insider knowledge as a factor.**

Factors	Academic sources	IT industry publications	Reported Incidents
Gender	**There were no references addressed gender as a factor**	**There were no references addressed gender as a factor**	**The following references support gender as a factor:** (Keeney, Cappelli, et al. 2005; Cappelli et al 2006; CERT 2006; Kowalski et al 2008; Moore et al 2009; Spooner 2009; Cappelli et al 2009; Hanley et al. 2009; CERT 2009; Hanley et al. 2011, Cummings et al. 2012; King 2012)
Insider Technical Skills	**The following references support insider skills as a factor:** (Cohen 2001; Nykodym, Taylor, and Vilela 2005; Magklaras and Furnell 2005; Theoharidou et al. 2005; Althebyan and Panda 2008; White and Panda 2009).	**The following references support insider skills as a factor:** (Secret Service, Cert Analyze Insider Computer Sabotage 2005; Ortega 2006; Lynch 2006; How to Weed out the New Insider Cybersecurity Threat 2007; Bauch 2011).	**The following references support insider technical skills as a factor:** (Keeney, Cappelli, et al. 2005; Moore, Cappelli, and Trzeciak 2008; Cappelli et al. 2008; Kowalski et al. 2008; Hanley et al. 2009; Spooner et al. 2009; CERT 2009; Moore et al. 2009; Hanley et al 2011). **The following references provide only weak support** Randazzo et al. 2004; CERT 2006; Hanley et al. 2009; King 2012; Cummings et al. 2012).

Factors	Academic sources	IT industry publications	Reported Incidents
Motivation	**The following references support motivation as a factor:** (Bloombecker 1984; Forester and Morrison 1994; Hitchings 1995; McNamara 1998; Wood 2000; Furnell 2004; Theoharidou et al. 2005; Robert and James 2006; Furnell 2006; Shaw 2006; Fyffe 2008; Jones 2008b; Walker 2008; White and Panda 2009; Sarkar 2010; Crossler et al. 2013).	**The following references support motivation as a factor:** (Ortega 2006; Lynch 2006; D'Arcy and Hovav 2007; Kirkpatrick 2008; Willison and Siponen 2009; Blades 2010; Bauch 2011)	**The following references support motivation as a factor:** (CERT 2006 ; Cappelli et al. 2008; Kowalski et al. 2008; Hanley et al. 2009) King 2012(Keeney, Cappelli, et al. 2005; Moore, Cappelli, and Trzeciak 2008) CERT (2006), CERT (2009) and Cummings et al. (2012) Hanley et al. (2009) Kowalski et al. (2008)
Outsourcing	**The following references support outsourcing as a factor:** (Shaw, Ruby, and Post 1998; (Whitworth 2005; Cole and Ring 2005; Colwill 2009; Sarkar 2010)	**The following references support outsourcing as a factor:** (Khanna 2005; Financial Institution Security Risks and Concerns: The Top Eight 2007; Blades 2010; Bucki 2011)	**The following reference provides only weak support:** (Kowalski, Cappelli and Moore 2008; Cappelli et al. 2008; Kowalski et al. 2008; Lewellen et al. 2012)

Factors	Academic sources	IT industry publications	Reported Incidents
Information security policy	**The following references support information security policy as a factor:** (Gaunt 1998; Cohen 2001; Magklaras and Furnell 2002; Pramanik, Sankaranarayanan, and Upadhyaya 2004; Furnell 2004; Furnell 2006; Walton and Limited 2006; Canavan 2007; Bishop et al. 2008; Albrechtsen and Hovden 2010; Da Veiga and Eloff 2010; Hu et al. 2012; Crossler et al. 2013; Guo 2013).	**The following references support information security policy as a factor:** (Khanna 2005; Jaikumar 2005; Addressing the Insider Threat 2007; Steele and Wargo 2007; D'Arcy and Hovav 2007; How to Weed out the New Insider Cybersecurity Threat 2007; Blades 2010; Hu et al. 2011; Ford 2012)	**The following references support information security policy as a factor:** (Randazzo et al. 2004; Kowalski, Cappelli and Moore 2008; Kowalski et al. 2008) **The following reference provides only weak support:** (Cappelli et al. 2008) **The following reference provides no support:** (Spooner et al. 2009)
Psychological factors	**The following references support the psychological factor:** (Shaw, Ruby, and Post 2005; Sarkar 2010) **The following reference provides only weak support:** (Pfleeger 2008)	**The following references support the psychological factor:** (Steele and Wargo 2007; How to Weed out the New Insider Cybersecurity Threat 2007; Kirkpatrick 2008; Hu et al. 2011)	**The following references support the psychological factor:** Keeney, Cappelli, et al. 2005; Band et al. 2006; Cole 2008; According to Moore, Cappelli, and Trzeciak 2008; Cappelli et al. 2008; Kowalski et al. 2008)

Factors	Academic sources	IT industry publications	Reported Incidents
Cultural factors	**The following references support cultural factors:** Thomson and von Solms 2006; Ashenden 2008; Crinson 2008; Royds 2009; Colwill 2009; Sarkar 2010; Luo and Shenkar 2011)	**The following references support cultural factors:** (Kirkpatrick 2008)	**The following references support cultural factors:** (Keeney et al. 2005; Kowalski et al. 2008; Spooner et al. 2009) **The following reference provides only weak support:** (Cummings et al. 2012).
Remote access	**The following references support remote access as a factor:** (Cole and Ring 2005; Shaw 2006; Sarkar 2010; Aldhizer and Bowles 2011; Blackwell 2012)	**The following references support remote access as a factor:** (Secret Service, Cert Analyze Insider Computer Sabotage 2005; Data Insecurity—Is Not Knowing the Cause Part of Your Problem? 2008; Castle 2009; Assessing the Seriousness of Security Threats from Employee Misuse of It Resources 2009; Griffin 2009; Bauch 2011).	**The following references support remote access as a factor:** (Randazzo et al. 2004; Keeney, Cappelli, et al. 2005; CERT 2006; Moore, Cappelli, and Trzeciak 2008; (Kowalski et al. 2008; Hanley et al. 2009) **The following references provide only weak support:** (Cappelli et al. 2008; Moore et al. 2009; Spooner et al. 2009; Hanley et al. 2011)

2.7 Summary

Chapter Two provides a critical review of the relevant literature related to this research from three different sources: academic research, IT industry publications and published reported incidents. It describes in detail the risk of insider threat as well as the previous insider threat models, the gaps in the previous research were also discussed in detail. This review highlights the crucial need for a holistic insider threat model and reemphasizes the significance of this research, because the academic research provided diverse models that reflect differences and disagreements. Moreover, none of the previous models captures all the factors that emerged from this review.

In addition, a detailed analysis of the factors contributing to insider threat, gathered from the three different sources, provided sound evidence in support of the need for more investigation in order to verify each factor. The factors that emerged from the three different sources (academic sources, IT industry publications and published reported incidents) were not equally supported by all the sources since some sources have highlighted some factors while other sources have supported others. Thus, this chapter highlights the need for a holistic insider threat model, investigating the important contributing insider threat factors from all three sources in order to minimise the insider threat.

CHAPTER THREE: RESEARCH OBJECTIVE, QUESTIONS AND CANDIDATE RESEARCH MODEL

3.1 Introduction

Chapter Two reviewed the insider threat literature from three different sources: academic research, IT industry publications and published reported incidents. The scope of the literature search and the selection criteria were detailed. It also described in detail the risk of insider threat as well as the insider threat contributing factors. Finally, Chapter Two highlighted the research gaps.

This chapter addresses the main elements that drive this research, the research objectives and corresponding research questions. It starts with the research objectives followed by the research questions and significance of the research. The research objectives and research questions sections will address the 'what' of the research while significance will justify the 'why' of this study. Finally, the candidate research model will be presented at the end of this chapter.

3.2 Research Objective

The crucial need for a holistic model of insider threat was evidenced in Chapter Two, as most of the previous models focus on some factors while ignoring others. The overall aim of this research is to develop a conceptual insider threat model that can frame a holistic view of insider threat behaviour and inform the development of best practices to manage the insider threat. This research studied the insider threat in an effective way by providing a comprehensive perspective for insider behaviour by

developing a holistic insider threat model. To do so, the researcher conducted a thorough examination of social, technical and organisational factors. As discussed in section 2.6, previous research in this area focused on quite narrow and specific areas and most of the models and frameworks developed so far specialise in either people to people relationships, segmentation of tasks, access to information or network architectures (Huth et al. 2013). The very rigorous and structured search approach in Chapter Two revealed that, to date, no published prior research has taken a holistic view of the insider threat. Huth et al. (2013) support this, stating that researchers still struggle to develop a holistic approach that addresses and defines the insider threat problem.

Therefore, the main objective of this research is to gain a holistic view of the insider threat by understanding the factors that influence insider threat behaviour, both by individuals and organisations, and then develop security measures (best practices) to manage insider threat behaviour.

3.3 Research Questions

The literature from three sources reviewed in Chapter Two revealed the lack of agreement concerning the factors that contribute to insider threat. Some sources strongly support some factors while other sources have highlighted others. To examine this issue, the factors contributing to insider threat should be accurately determined and it is essential to conduct further investigation in order to identify these factors. Hence, the main purpose of this research is to develop a holistic insider threat model by understanding the factors that influence insider threat behaviour. Accordingly, the first research question is:

> *RQ_1: What are the factors that influence the insider to behave inappropriately regarding security?*

In addition, section 2.3 clearly demonstrated that the incidence of insider threats has steadily increased year by year, and there are indications that this trend will continue (Brdiczka et al. 2012). A comprehensive security guideline is necessary in order to minimise the insider threat risk. This leads to the second research objective which is the development of the best practices to manage insider threat behaviour to mitigate the risk. Correspondingly, the second research question is:

> *RQ_2: How can organisations manage insiders' potential abuse of security?*

3.4 Research Significance

The insider threat is a complex problem involving both human factors and computational elements; this threat is managed by a combination of technical and behavioural strategies. This research makes two important contributions: theoretical and practical.

3.4.1 Theoretical Contribution

Theoretical significance refers to the coverage of the literature, the contribution to knowledge in the field of study and future research opportunities within the field of study. This research proposes a new conceptual insider threat model for a holistic view of insider threat behaviour to present an insight into the insider threat - including people, tools, technology and environment. The significance of this model lies in its understanding of the insider threat from a wider perspective instead of a single view. The proposed model adds to the knowledge base for further research and practice since it can be used by other researchers to test and improve the model in further studies.

3.4.2 Practical Contribution

As stated by Brdiczka et al. (2012), the incidence of insider threats has experienced a continuous increase each year, and there are indications that this trend will continue. Previous studies illustrated in section 2.3 revealed that insider threat leads to great financial losses in organisations. A Cyber Security Watch Survey conducted in January 2011 showed that around 43% of participants had experienced an insider incident between 2004 and 2010 and 46% of the participants stated that insider attacks were more costly than other attacks (Holmlund et al. 2011; CERT 2012). According to a CERT study, the average costs of insider threat exceed $50M in losses (King 2012). These losses demonstrate that the insider threat is a serious problem which costs organisations a great deal.

This research will minimise the problem of the insider threat by providing best practices to manage insider behaviour. The contributions of this research are applicable to business and user needs especially in security and IT departments. The proposed best practises will contribute to avoiding and preventing insider threats in organisations. These best practises will be useful in different organisations and for audiences who are aware of organisational security issues such as the Chief Information Security Officer (CISO).

3.5 Candidate Holistic Insider Threat (HIT) Model and the Factors

The candidate HIT model is an amalgamation of the factors derived from academic sources, IT industry publications and incident reports. The literature review revealed nine factors that contribute to insider threat behaviour namely: access and level of trust, insider knowledge, insider technical skills, motivation, information security policy, psychological factors, cultural factors, outsourcing, remote access and gender. Table 2.4 in section 2.6 illustrates that some insider threat factors were supported by all three sources while others were supported by only one or two

sources. Therefore, the combinations of academic sources, IT industry publications and reported incidents factors result in the development of the candidate HIT model.

Factors in the candidate HIT model and their explanation are given below:

3.5.1 Individual Characteristics

Two factors are combined together (psychological factors and gender) as both relate to personal characteristics. In 82% of overall CERT cases, the insider was male (Moore et al 2009; Hanley et al. 2011). According to Cummings et al. (2012), the high incidence of males does not indicate that they are more likely to commit insider threat as much, as it might reflect the distribution of men in these roles within the organisations.

However, there are a number of personal features that could predict harmful behaviour. These features include: psychological factors, personal factor (such as personal predispositions) and inappropriate or concerning behaviour prior to the incident (Shaw, Ruby, and Post 2005; Steele and Wargo 2007; Cappelli et al 2008; Sarkar 2010; Hu et al. 2011).

As explained in section 2.4.6, examples of psychological factors include social frustrations and computer dependency. Personal predispositions can be recognized by some noticeable features such as alcohol and drug addiction, physical partner abuse, violations arrests, hacking, and security violations (Band et al. 2006). Personal predisposition is a common feature in many insider threat cases (Band et al. 2006; Moore, Cappelli, and Trzeciak 2008; Cole 2008). Furthermore, inappropriate or concerning behaviour (such as delays, absences and poor job performance) prior to the incident could indicate an increased threat of potential malicious activities (Cappelli et al 2008). Many criminal insiders behaved in inappropriate ways prior to the incident (Keeney, Cappelli, et al. 2005; Cappelli et al 2008; Kowalski et al. 2008). As discussed previously in Chapter Two, in some cases the insiders had

revealed a noticeable concerning behaviour or activity before the incident which indicates that individual characteristics could contributing to insider threat.

3.5.2 Outsourcing

Outsourcing is any task, operation or job performed by a third party. This task cannot be completed by employees within an organisation for reasons such as a shortage of time, employees or skills (Shaw, Ruby, and Post 1998). Although most organisations find outsourcing is beneficial, the risk of security violation or compromised intellectual property rights is increased (Sarkar 2010; Blades 2010).

As explained in section 2.4.8, outsourced employees increase the risk of insider threat behaviour as sometimes they are given the same logical and/or physical access as the organisation's full time employees (Shaw, Ruby, and Post 1998). In addition, engaging a relatively high number of outsourcing agreements could expose the confidential data to serious threat (Whitworth 2005; Colwill 2009). Therefore, all organisations must take into consideration the threat posed by the outsourced employees and carefully consider their level of access and their knowledge.

3.5.3 Information Security Policy

An information security policy is a guideline that the organisation can follow to protect its physical and information technology assets (Canavan 2007). All employees should strictly follow the security policies guideline to minimise the risk of any potential threats and to be able to respond to any security incidents efficiently (Hu et al. 2012; Crossler et al. 2013). Overall, security policy identifies the activities that are authorised for a specific user and purpose.

As discussed in section 2.4.5, an appropriate security policy should depend on the business and the sensitivity of data. All organisations should be aware that when implementing the appropriate security policy, they should provide sufficient

information security policy training and awareness, and keep their information security policy up to date (Cohen 2001; Magklaras and Furnell 2002; Pramanik, Sankaranarayanan, and Upadhyaya 2004; Furnell 2006; Walton and Limited 2006; Bishop et al. 2008; Hu et al. 2012; Crossler et al. 2013). Training and awareness programs are very essential in order to minimise the risks of the insider threat (Jaikumar 2005). Likewise, the appropriate enforcement and reminders of the established policies will help to mitigate the risk (Steele and Wargo 2007). An inappropriate information security policy will increase the risk of the insider threat; therefore, all organisations must consider how best to implement an appropriate information security policy, and keep it up to date.

3.5.4 Remote Access

Remote access allows employees to access the organisation's networks from outside the organisation's physical boundaries. In this study, remote access is introduced as access by an employee who can gain entrance into the organisation's networks from outside the workplace, either from their home or other place, through mobile devices or any other device. As discussed previously in section 2.4.9, giving employees remote access to organisational information will increase the security risks (Keeney, Cappelli, et al. 2005; CERT 2006; Sarkar 2010). Such risks include viruses as these could be transferred to the organisation's network through untrusted devices, and information theft can easily be committed via this access (Griffin 2009; Bauch 2011). Furthermore, allowing mobile devices to access organisational information remotely from outside the organisation's physical boundary poses a great threat to the information since these devices are a source of data leakage (Sarkar 2010). Remote access increases the risk of insider threat since it could lead to information theft or data leakage.

3.5.5 Cultural Factors

This study divides the cultural factors into organisational culture and national/regional culture (see section 2.4.7). Organisational culture is the shared values and norms that provide ways for employees to achieve their tasks and to interact with each other (Thomson and von Solms 2006; Colwill 2009; Sarkar 2010). Organisational culture shapes employees' behaviour and it may direct the security policies. Thus, if the organisational culture tolerates unethical behaviour, the employee definitely will behave inappropriately.

Furthermore, culture differences increase the risk of insider threat behaviour since the employees come from different cultural backgrounds with different levels of awareness of law, and ethics regarding theft. In addition, cultural differences sometimes lead to clashes between employees and the organisation which in turn may increase the insider threat. (Bond 2004; Crinson 2008; Royds 2009; Casali and Day 2010; Colwill 2009; Sarkar 2010). Therefore, cultural differences sometimes play a role in explaining the abuse of the organisation's system or information.

3.5.6 Motivation

The motivation for a malicious attack is grouped into three main areas: revenge, theft for financial gain, and theft for a business advantage (Furnell 2004) as mentioned in section 2.4.4. Most often, insiders intentionally misuse their organisation to obtain data for financial or business gain (White and Panda 2009). Malicious insider's motivation could include the desire for direct personal gain or sometimes the insider may have been recruited by competitive organisations that financially reward them for their disloyalty. Moreover, the insider could be persuaded by the outsider when the employee is being forced or blackmailed to perform the attack (Wood 2000; Furnell 2006; Fyffe 2008; Walker 2008; White and Panda 2009; Sarkar 2010; Crossler et al. 2013). Studies show that unsatisfied employees have the desire to revenge themselves by causing the organisation financial losses. In such a case, the

insider incidents take place after the insider has been involved in a negative work-related event (Lynch 2006; Kirkpatrick 2008). Insider motivation is considered as an important factor contributing to insider threat; if the insiders have a motive for harming their organisation, and moreover have access, they can easily misuse their organisation.

3.5.7 Access and Level of Trust

Section 2.4.1 illustrated that the misuse of access is one of the most common types of attack and is considered one of the most difficult types of attack to detect and prevent (Fyffe 2008; Willison and Warkentin 2013). Many organisations give their employees more access and trust than what they essentially need to do their job (Cohen 2001; Furnell 2004; Nykodym, Taylor, and Vilela 2005; Bellovin 2008; Willison and Warkentin 2013). High level of trust offers the crucial privileges that malicious insiders need to allow them to carry out a successful insider attack (Magklaras and Furnell 2005; Contos 2007). A privileged employee, more than others, can cause serious harm to organisations (Sarkar 2010; Willison and Warkentin 2013). For example, employees in technical positions who have a system administrator or privileged system access can present a serious threat to the organisation.

Furthermore, it is essential to immediately disable employees' access when they are terminated. Access to an organisation's physical and technical systems by individuals who previously had legitimate access can create a significant threat to the organisation. (McNamara 1998; Cohen 2001; Furnell 2004; Nykodym, Taylor, and Vilela 2005; Bellovin 2008; Fyffe 2008; CERT 2009; Willison and Warkentin 2013). Physical and logical access is one of the most important factors contributing to insider threat. Therefore, organisations should be aware of all access paths to the information available to all employees.

3.5.8 Insiders' Knowledge

Insiders' knowledge refers to any employees using the knowledge gained from their legitimate jobs for illegal gain (Willison and Siponen 2009). Insiders can be anyone within the organisation including full-time employees, contractors or administrators. As explained in section 2.4.2, whoever they are, the more knowledge they have the more harm they can do (Khanna 2005; Castle 2009). Insiders often have a great deal of knowledge about their organisation; they are usually aware of the potential value of the organisation's information and the methods required to grant access to this information. Moreover, insiders have a great knowledge about policies, procedures, security countermeasures and their weaknesses (Magklaras and Furnell 2005; Dallaway 2008; Althebyan and Panda 2008; White and Panda 2009; Bishop et al. 2010). Thus, insiders are well-informed about the areas that can be targeted and how to obtain the information required.

3.5.9 Technical Skills

Technically skilled employees are considered as the most serious threat to any organisation networks (Ortega 2006). As earlier described in section 2.4.3, insiders can use their technical skills to harm an organisation's system via a number of means including hacker tools, writing a script or program that includes a logic bomb, placing a virus on client computers, utilizing password crackers, downloading remote system administration tools, gaining access to the system after termination and the setup, and using backdoor accounts (Cohen 2001; Magklaras and Furnell 2005; Theoharidou et al. 2005; Sarkar 2010). Insiders often have the technical skills that are usually related to the system they are familiar with, which gives them a better opportunity to misuse this system.

According to Cohen (2001) and Theoharidou et al. (2005), the level of employee sophistication can influence their ability to execute insider threat. They divided the levels of IT sophistication to three categories include advanced (end users with a

high level sophistication), ordinary (end users with a medium level sophistication) and novice (end users with a low level of IT sophistication). Organisations should acknowledge the threat of a technology-driven world, where a technically skilled employee could cause greater harm than can any ordinary employee.

As discussed in section 2.6 of the previous chapter, there is a crucial need for a holistic model of insider threat to address all the contributing factors, as most of the previous models focus on one factor while ignoring the others. This study has taken into consideration all the factors that have been addressed by the previous literature. The candidate HIT model is presented in Figure 3.1 to illustrate these factors.

The candidate HIT model will be utilized in the preparation of a survey method in Chapter Five. In the quantitative phase of the study, the factors in the candidate HIT model are validated. The outcome from the survey is the enhanced HIT model with the factors that influence the insider threat behaviour. Thus, the candidate HIT model is the foundation for the quantitative phase of this study.

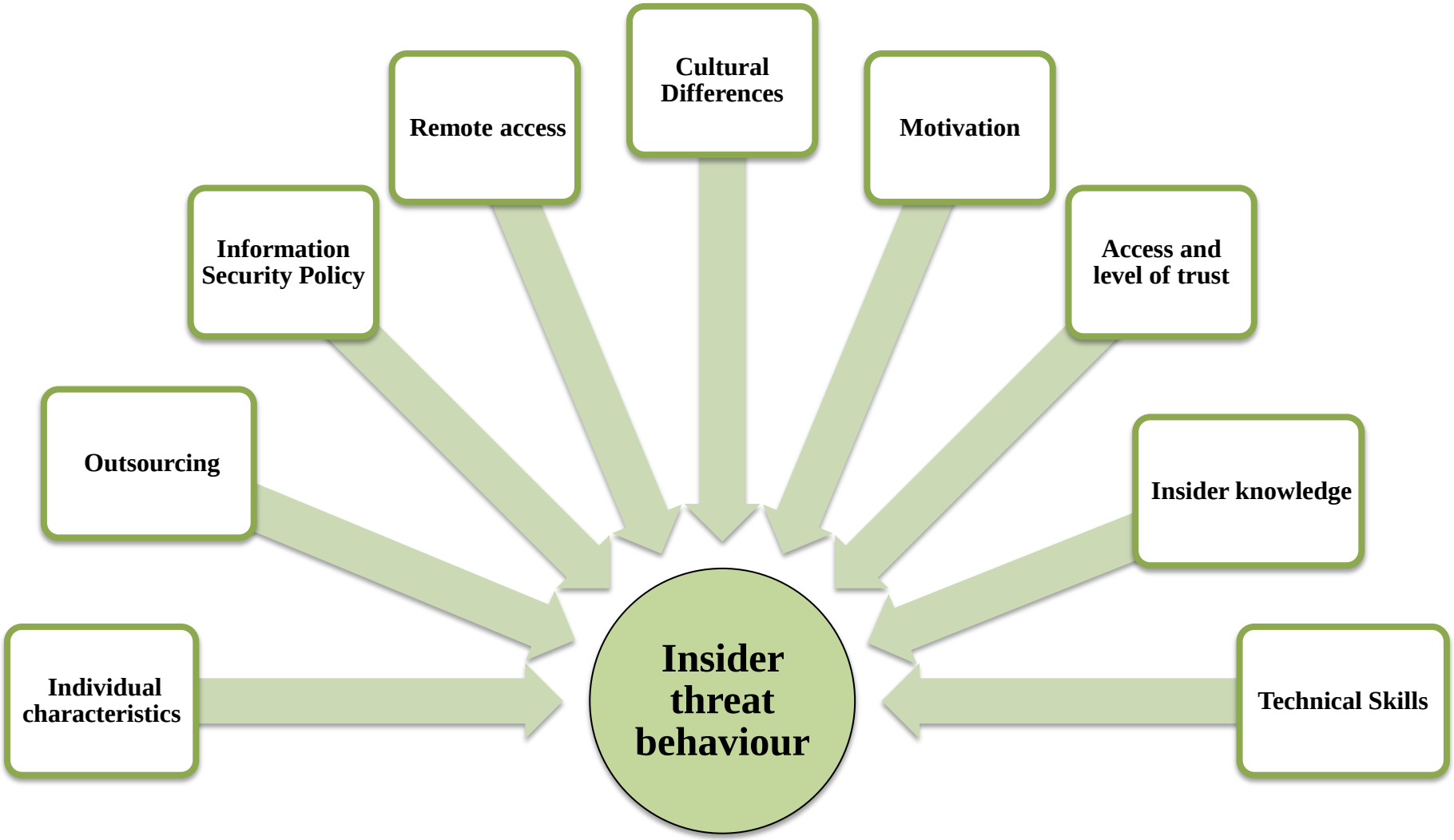


Figure 3.1: Candidate HIT model

3.6 Summary

This chapter discussed in detail the research objectives, research questions and research significance. This study has two main objectives: (1) to develop a holistic conceptual insider threat model by understanding the factors that influence insider threat behaviour and (2) to develop best practices to manage insider threat behaviour. In addition, this chapter presented the research questions, followed by the discussion of the two main contributions of this study: theoretical and practical contributions. Finally, Chapter three presented the candidate HIT model and an explanation of each factor in the model was also provided.

The next chapter will explain in detail the research methodology and the research phases.

CHAPTER FOUR: RESEARCH METHODOLOGY

4.1 Introduction

In Chapter Three, the research objectives and the research questions provided the foundation for this chapter as they help to determine the selection of the research methodology. Given the research gap whereby there is no holistic insider threat model, the research objective aims to develop and evaluate the holistic insider threat model. These processes ideally need a mixed method approach in order to develop and assess the HIT model.

In this chapter, the mixed method research design is described and the reasons for adopting this method will be justified. This is followed by explanations of the research phases. There are two major phases in this study: developing a conceptual holistic insider threat model and developing best practices to manage the abusive behaviour. The sample selection, data collection, and data analysis for each of the sequential stages are explained. This chapter addresses the 'how' of the study.

4.2 Research Method

This study poses real challenges with regard to methodology because of the difficulty of collecting data relating to the insider threat. In order to examine insider threat, it is essential to collect data from insiders themselves and real life cases. However, insiders are very difficult populations to survey and also cases of insider threat are often unreported; even when they are reported, they are confidential and information about them is protected. Therefore, accessing these data to study the insider threat is a challenge and in this study the response to this challenge is that the data has been

collected from experienced security professionals who dealt directly with the insider threat cases, which is a good way of assessing the model. Furthermore, finding an appropriate sample of experienced security professionals is one of the challenges for this study because of the specialised nature of the knowledge. In order to solve this problem, the researcher employed an outside agency to help recruit the required participants without any difficulties.

This study adopts a mixed method approach in order to assist in the research phases and to understand the research problem. Both quantitative and qualitative data collection methods were utilized at different points in the research.

The use of both quantitative and qualitative data collection in a single study is known as a mixed method research (Tashakkori and Teddlie 2003). Mixed method research is defined as *"the class of research where the researcher mixes or combines quantitative and qualitative research techniques, methods, approaches, concepts, or language into a single study"*(Johnson and Onwuegbuzie 2004, 17).

The mixed method approach could be difficult for a single researcher, because the researcher must be familiar with both qualitative and quantitative research. The researcher needs to study both qualitative and quantitative methods and understand how to combine them appropriately (Johnson and Onwuegbuzie 2004; Yin 2006; Mengshoel 2012; Creswell and Clark 2007).

Researchers recommend the combined use of both qualitative and quantitative research methods as this strengthens the study and produces a more comprehensive knowledge base essential to the development of theory and practice (Mingers 2001; Johnson and Onwuegbuzie 2004; Creswell 2008; Ford 2012). According to Creswell (2003, 24) *"A mixed methods design is useful to capture the best of both quantitative and qualitative approaches"*. Mingers (2001) state that mixed methods offer a wider range of data that delivers richer and more reliable results than a single research method, especially in the field of information systems.. Furthermore, the merging of both quantitative and qualitative methods offers a more in-depth understanding of the

research problem and questions than the use of a single method (Creswell and Clark 2007; Creswell 2008). Miles and Huberman (1994, 42) state that combining quantitative and qualitative data provides *"a very powerful mix"*. For example, the researcher might survey a large number of people using closed-ended questions and then following this up with an open-ended interview question for a few people to collect their voices and opinions about the topic. *"In these situations the advantages of collecting both quantitative data qualitative data prove advantageous to best understand a research problem"* (Creswell 2003, 24). Therefore, quantitative and qualitative data were collected and analysed in order to address and answer the research questions. This study adopts the mixed methods approach since the combination of quantitative and qualitative methods provides a more in-depth understanding of the research gaps than the use of a single method. It also allows a wide range of information to be collected to answer the research questions; moreover, it is considered to be the best way to develop theory and practice.

The Explanatory Mixed Methods Design number III in Figure 4.1 is selected to help define the research process. Rather than gathering data simultaneously, the quantitative and qualitative data was collected sequentially in two phases (Ivankova, Creswell, and Stick 2006). The rationale for this is that the quantitative data collection and analysis provide a wide view of the research problem; then an in-depth analysis of the collected qualitative data is required to refine and enhance the result and to explain the wide view (Creswell and Clark 2007). The Explanatory Mixed Methods Design allows the researcher to *"Collect quantitative data first in the sequence. This is followed by the qualitative data collection. Researchers often present these studies in two phases, with each phase clearly identified in headings in the report. This type of mixed method the researcher uses the qualitative data to refine the result from the quantitative data"*(Creswell 2008, 560). In this type of mixed method design, the priority is the quantitative data collection and analysis. This is achieved by presenting the quantitative method first with a substantial sample of data collections. Then, in the second phase, it is essential that a small amount of qualitative data be collected.

According to Creswell (2008) and Ivankova, Creswell, and Stick (2006), this type of mixed methods design combines the best of both quantitative and qualitative data collection methods. In the first phase, the quantitative results will be obtained from a large number of individuals, and then in the second phase, the finding will be evaluated and refined via an in-depth qualitative method.

The objective of the Explanatory Mixed Methods Designs number III aligns with this study in the sense that the quantitative method will assist the researcher to identify the factors which will adjust the candidate HIT model. While, qualitative method aims to validate the enhanced HIT model and to ensure that it represents a holistic view of the insider threat contributing factors.

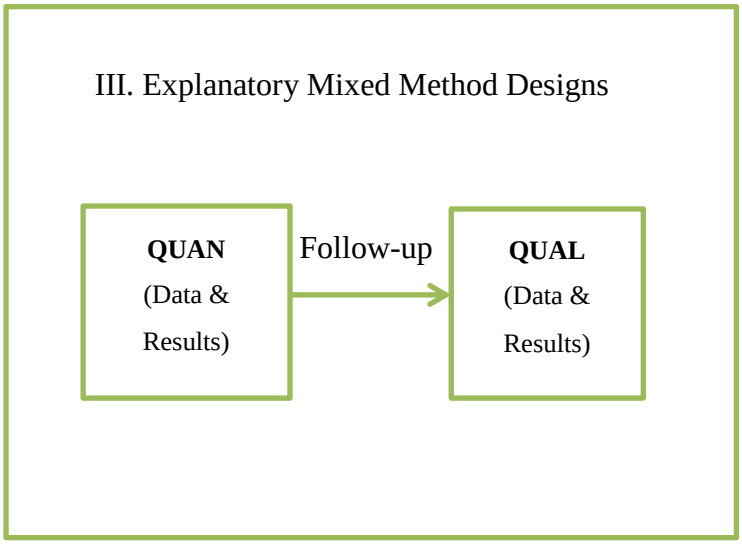


Figure 4.1: Explanatory Mixed Methods Design number III
(Creswell 2008, 557)

4.3 Research Phases

The adoption of mixed methods inevitably requires a phased research approach. In this study, a quantitative stage is conducted first, followed by a qualitative stage as explained in section 4.2. Hence, this study is conducted in phases. In phase one, a holistic model is developed from the literature and then tested quantitatively, followed by a qualitative stage to verify the results from the previous stage. This phase addresses the first research question. In addition, phase two is conducted to develop the best practices in order to manage the factors in phase one; this addresses the second research question. The sequential phases of the mixed methods research design are illustrated in Figure 4.2.

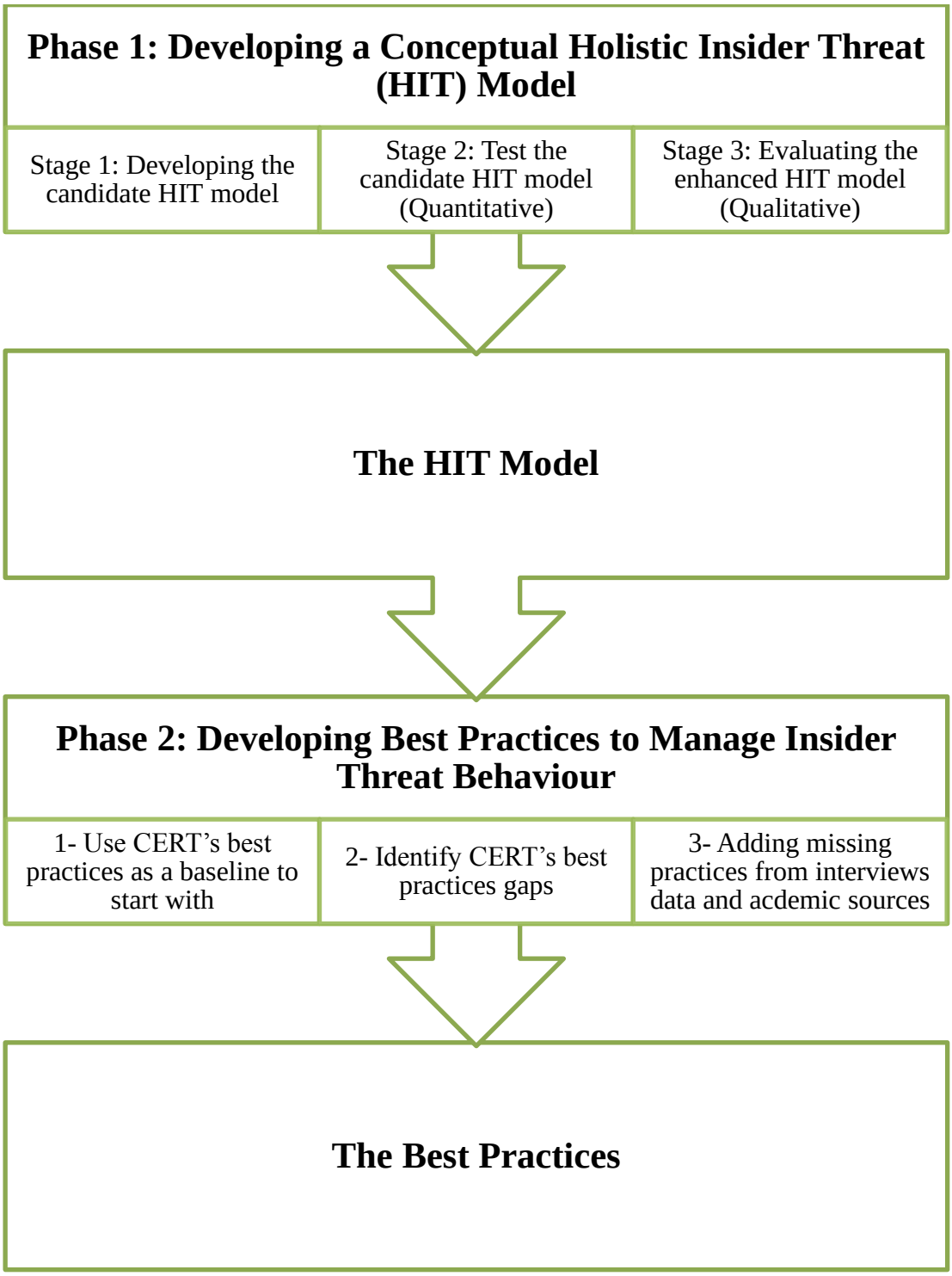


Figure 4.2: Sequential phases of the mixed methods research design

4.4 Phase 1: Developing a Conceptual Holistic Insider Threat (HIT) Model

Phase one is carried out in three stages: developing the candidate HIT model, testing the candidate HIT model through quantitative data collection and evaluating the enhanced HIT model via qualitative data collection.

4.4.1 Stage 1: Developing the candidate HIT Model

The first stage in phase one commenced with an extensive review of the literature related to insider threat. In this stage, the researcher reviewed and studied three sources: academic research (such as conference proceedings, journal articles and books), IT industry publications (such magazines and Web white papers) and published reported incidents (such as CERT reports), to cover different aspects of the insider threat (details in section 2.2). The critical review concluded that although there are a number of academic research models explaining the insider threat behaviour factors, none of them addresses all factors.

The factors contributing to insider threat that emerged from the literature review as discussed in section 2.6 were not equally supported by all three sources studied for this research. Therefore, there is a need for a holistic model to address all these factors together with a verification of each factor due to the conflicting results from the three sources. This review leads to a gradual building of the candidate HIT model. Combining all factors from three sources will inform the development of the candidate HIT model to include all factors suggested by academic research, IT industry publications and published reported incidents as detailed in section 3.5.

The collected data were analysed using content analysis to identify factors that are suggested or confirmed by previous sources include academic sources, published reported incidents and IT industry publications. Qualitative content analysis *"involves a process designed to condense raw data into categories or themes based*

on valid inference and interpretation" (Zhang and Wildemuth 2009, 2). Content analysis includes two approaches: inductive and deductive. The inductive process is often used to derive themes and categories from the data through careful examination and continuous comparison. While the deductive process uses the concepts or variables generated from theory or previous studies (Patton 2002; Berg and Lune 2011).

The inductive content analysis (Mayring 2000a) process guided the data analysis. According to Mayring (2000b, 4), the main idea of the inductive content analysis is to formulate

> *"a criterion of definition, derived from theoretical background and research question, which determines the aspects of the textual material taken into account. Following this criterion the material is worked through and categories are tentative and step by step deduced. Within a feedback loop those categories are revised, eventually reduced to main categories".*

The researcher followed systematic steps recommended by Creswell (2008). Firstly, the researcher closely read the academic research, CERT reports of insider incident cases and IT industry articles. During this step, the key words were highlighted. Secondly, the identified key words were labelled and categorised into themes constituting the main factors which include: access and level of trust, insider knowledge, insider technical skills, motivation, information security policy, psychological factors, cultural factors, outsourcing, remote access and gender (coding done through NVivo version 10). Once the main factors had been identified, a third step was taken to reduce any overlapping should one segment of text be coded according to more than one theme. Finally, the researcher constantly reviewed the data and the developed themes. In this step, two themes (factors) were combined as explained in section 3.4.1. Hence, the factors in the candidate HIT model are: individual characteristics, outsourcing, information security policy, remote access, cultural factors, motivation, access and level of trust, insiders' knowledge and technical skills as presented in Figure 3.1.

4.4.2 Stage 2: Testing the candidate HIT Model (Quantitative Stage)

In this stage, the candidate insider threat model is evaluated using the quantitative approach which focuses on *"deduction, confirmation, theory/hypothesis testing, explanation, prediction, standardized data collection, and statistical analysis"*(Johnson and Onwuegbuzie 2004, 18). The quantitative stage in this study involved the administration of an online survey in Jun 2012. The survey method is one of the most common data collection approaches in quantitative research (Myers 1997; Creswell 2003). The survey method has many benefits including the economy of the design, being less expensive than the other method, and usually providing greater anonymity than the other method (Creswell 2003; Cavana, Delahaye, and Sekaran 2001).

A survey is a *"system for collecting valid information from or about people to describe, compare, or explain their knowledge, attitudes, and behaviour"* (Fink 2010, 152). The data from the survey method can be collected either directly or indirectly: directly by asking individuals to answer questions, indirectly by recording people's written or oral thoughts and opinions (Fink 2010). Thus, the survey method is suitable for investigating the answers for RQ_1 outlined in Chapter Three, since this research question is concerned with the factors that affect insider behaviour and the data is collected directly from the participants through an online survey.

In order to select the appropriate research methods to evaluate the candidate HIT model, numerous processes were involved. Firstly, the literature was reviewed and studied in-depth to identify the existing methods. Secondly, the target population was identified and the best way to communicate with them was determined. Thirdly, the practical constraints were considered. Subsequently, it was established that the most appropriate method for evaluating the model is the electronic survey approach. Online surveys are flexible in their application, keep the costs associated with data

collection to a minimum, and enable large amounts of data to be collected within a short time frame (Gordon and McNew 2008).

The use of an online survey has many advantages such as fast data retrieval, high quality data without typographical errors because the data is automatically stored, and the ability to integrate that data into statistical and graphical solutions. In addition, the response can be anonymous, especially among researches who collect sensitive information (Gordon and McNew 2008). This survey assessed a respondent's experience and knowledge of insider threat behaviour factors and required information about demographics, employment, and whether they had previously faced an insider threat problem in their workplace; all these questions could be considered to elicit personal and sensitive information. Therefore, the use of an online survey was considered the most appropriate evaluation method for the candidate HIT model.

There are three types of online survey: e-mail, Web-based and personal digital assistants (PDAs) or hand-held devices (Gordon and McNew 2008). There are several advantages to collecting the data through a Web-based survey (Creswell 2008; Gordon and McNew 2008). Although a Web-based survey has some drawbacks (e.g. if the server is down, participants cannot access the survey, and it requires programming skills), there are several benefits of using this type of online data collection. The following are the several advantages of the Web-based survey(Gordon and McNew 2008, 606, 607):

Web

- *The response can be relatively anonymous*.
- *The data can be automatically stored inside a database for later data mining and analysis.*
- *Transcription costs are non-existent*
- *Multimedia elements can now be easily added to any survey in a Web environment*
- *Web surveys allow for ''skip'' and ''context'' logic.*

- *In some online Web survey services, data can be saved directly to an SPSS*

The Web-based survey was chosen to collect the data for this study. According to Boas and Hidalgo (2013), the online survey tools that are usually used by scholars include Qualtrics, SurveyGizmo or SurveyMonkey to construct, manage and handle the survey. The survey was distributed to the participants through the Qualtrics website (www.qualtrics.com). Qualtrics is an online survey tool that has a credible reputation to develop and capturing survey results, it allows users to perform online data collection and analysis (Boas and Hidalgo 2013).

Having selected the survey as the preferred data collection tool, an appropriate population sample had to be decided. The focus of this research is to study the insider threat behaviour and to identify its contributing factors. The data collected in this stage is used to verify the candidate HIT model. Because the insider threat is a security issue (Chinchani et al. 2005),valuable information about insider threat can be collected from the top security management level since they directly handle and deal with the insiders. The decision was made to evaluate the model based upon data gathered within the USA, because most of the collected data which assisted in the development of the insider threat model were from the USA (academic literature, IT industry publications and publish reported incidents). This ensures that the model is evaluated in the same context that it was developed.

The collected data was analysed using SPSS (Statistical Package for the Social Sciences) version 20.0. The focus in this stage is to validate the factors identified in the literature. The researcher tested the candidate HIT model through a preliminary analysis of the survey. The factor analysis technique was utilized to identify an improved list of factors. There are two types of factor analysis: Exploratory Factor Analysis, and Confirmatory Factor Analysis (Alhija 2010). In Exploratory Factor Analysis (EFA), the researcher investigates the number of variables as the title suggests (Williams, Brown, and Onsman 2010). EFA *"explore the underlying dimensions of a construct. The primary considerations inherent in the use of factor analysis include conceptual/theoretical considerations, design considerations,*

statistical considerations, and reporting considerations, is exploratory in nature" (Alhija 2010, 162). The Exploratory Factor analysis technique was utilized to identify groups of inter-related factors to produce an improved set of robust factors. The factor analysis offered an improved list of factors, which is considered to be a more consistent interpretation of the data than the original grouping. The survey design and analysis are presented in Chapter Five.

4.4.3 Stage 3: Evaluating the Enhanced HIT Model (Qualitative stage)

This stage aims to evaluate whether the enhanced HIT model produced from the factor analysis comprised all the important insider threat contributing factors. In this stage, the enhanced HIT model from the previous stage was evaluated through the qualitative method. Qualitative research often relies on a small sample due to the in-depth nature of studies and analysis (Cormack 1991). The strength of qualitative research is *"its ability to provide complex textual descriptions of how people experience a given research issue. It provides information about the "human" side of an issue – that is, the often contradictory behaviors, beliefs, opinions, emotions, and relationships of individuals"* (Mack et al. 2005, 1). Interviews are one of the most common types of qualitative method approaches (Creswell 2003; Westerman 2006; Mack et al. 2005). According to Mack et al. (2005, 2), interviews are *"optimal for collecting data on individuals' personal histories, perspectives, and experiences, particularly when sensitive topics are being explored"*. This phase aims to collect data from experienced industry professionals that reflect their experiences regarding the insider threat factors and security measures to control these factors. Thus, the interview method is suitable for validating the answers for RQ_1 and investigating the answers for RQ_2 outlined in Chapter Three.

Although a face-to-face interview is the traditional way of conducting a interview, during the last few decades, data have been collected by different means such as focus groups, telephone, e-mail, and internet (Bolderston 2012).

Telephone interviews *"can be as productive as more traditional face to face methods"* (Bolderston 2012, 68). Hanna (2012) suggests that although interviewing people by telephone may lead to the loss of some subtleties associated with face-to-face interviews, this helps the researcher to 'stay at the level of text' and avoid adding context material to the data. One of the important advantages of the telephone interview is the practical benefit associated with arranging and scheduling the interview, and the flexibility to change the time which is very useful, especially if participants are busy people. Furthermore, telephone interviews are very suitable and convenient as a means of collecting data from participants in different and distant locations from the researcher (Egan, Chenoweth, and McAuliffe 2006; Bolderston 2012). Phone interviews were very useful for this research as they provided the researcher with more flexibility when arranging the interviews and the researcher was not required to travel to other countries in order to collect the data.

In addition, Skype is considered as an alternative to traditional face-to-face interviews (Bertrand and Bourdeau 2010; Hanna 2012). Collecting data through Skype offers synchronous face-to-face communications with the participants. Moreover, Skype allows the researcher to overcome the "*criticisms associated with losing visual and interpersonal aspects of the interaction"* (Hanna 2012, 242) since the researcher can record both video and audio communications of the interview. Collecting data through Skype in this study provided the researcher with the benefits of the face-to-face interview without having to travel to the participants' locations.

Interviews by email for the purpose of qualitative research were first conducted in the late 1990s (Egan, Chenoweth, and McAuliffe 2006). Email interviews offer greater flexibility to participants who are not able to be interviewed by telephone or Skype due to their busy schedule. According to Reid, Petocz, and Gordon (2008), McCoyd and Kerson (2006) and Creswell (2008), email interviews are acknowledged as an acceptable alternative mode for interviewing participants in research studies. Email interviews, unlike other interviews that are conducted on one day, may sometimes extend to months, with long gaps between questions and replies

(Gibson 2010). The advantage of using email interviews is that *"participants can choose when to respond to questions. Many people clearly spend time and effort writing, reviewing and editing their response before they send it"* (Gibson 2010, 3). Although, email interviews tend to be slower than the other types of interviews used in this study, they can provide rich information. In most of the email interviews conducted for this study, the participants provided detailed answers to each question and some of them supported their answers with examples. Although email interviews took longer to conclude, there was no need for transcription, thereby making it easier for the researcher to begin analysing the data.

The three interview types are a convenient means of collecting data from geographically remote participants (Egan, Chenoweth, and McAuliffe 2006; Bolderston 2012). Therefore, in this study the researcher provided three options: interview by telephone, Skype or email. In this way, participants were able to choose the method that was most convenient for them without impacting on the quality of the collected data.

The data for this stage was collected through semi-structured interviews. The interviews were carried out between October 2012 and December 2012. In-depth, semi-structured interviews with open-ended questions were used to collect qualitative data for this study. Fontana, Andre, and Frey. (1994) described interviewing as *"the art of science"*. Semi-structured interviews are defined by Longhurst (2009, 580) as *"the verbal interchanges where one person, the interviewer, attempts to obtain information from another person by asking questions"*. In-depth, semi-structured interviews are one of the most commonly used qualitative methods since they give the opportunity for more in-depth investigation since the interviewer is able to probe further and elicit more detailed responses from the interviewees. In addition, in-depth, semi-structured interviews are more useful than other methods since they investigate and attempt to understand complex behaviours, experiences, and opinions. Moreover, they offer to the interviewers and interviewees the time and space to explore issues thoroughly. According to Longhurst (2009, 582) *"Semi structured, in-depth interviewing can prove*

particularly useful for investigating personal, sensitive, or confidential issues which informants might find difficult to disclose and discuss in a group interview or focus group". A semi-structured interview is not just a random conversation or an integrative session. The researcher is guided by a willingness to understand and learn from the respondent, and creates an informal yet fruitful interaction that is guided by a series of interesting questions. Semi-structured interviews are intended to construct knowledge and reveal meanings through words, gestures, implications, jokes, facial movement and social fabricated talk and personal stories (Warren 2001; Dearnley 2005).

The enhanced HIT model was evaluated by the Chief Information Security Officer; the rationale for interviewing these people is the same as the rationale for the survey in stage two. The recorded data were transcribed and then analysed using the two-step content analysis approach recommended by Miles and Huberman (1994). Firstly, the interview responses were examined individually, and then secondly, they were cross-examine and the findings from each individual interview were integrated. The outcome of this phase was the final HIT model that contains a comprehensive set of insider threat factors. This holistic model provides the foundation for the next phase of the study. The interview design and analysis are detailed in Chapter Six.

4.5 Phase 2: Developing Best Practices to Manage Insider Threat Behaviour

While the previous phase provides data and analyses that enable the researcher to answer the research question one, it does not provide an answer for research question two. The qualitative data collected for this study supports two goals. The first goal is to evaluate the HIT model to provide an answer for RQ_1. The second goal is to collect information about the best practices to control and manage the factors in the HIT model to provide an answer for RQ_2. In this phase, the interview data that were collected in the previous phase were used in the development of the best practices.

During the interviews, the researcher ensured that the data collected not only answered research question, one but also provided answers to research question two.

This phase seeks to manage and control the factors produced in phase one by developing a set of security measures (best practices) to manage insider threat behaviour based on the factors in the HIT model. These best practices are the outcome of collecting CERT best practices for each factor, identifying any gaps in CERT's best practices, adding missing practices (from interviews data and academic sources) and finally synthesizing these into an integrated, coherent list of best practices (details in Chapter Seven).

4.6 Summary

This chapter described the research methodology and design. The mixed methods selection was explained and justified. The advantages and disadvantages of the mixed methods approach were presented. This was followed by detailed descriptions of the quantitative and qualitative data collection methods used in this study. This study has two main phases: (1) developing a conceptual HIT model and (2) developing best practices to manage the abusive behaviour. Phase one includes three stages: (1) developing the candidate HIT model, (2) test the candidate HIT model through quantitative data collection and (3) evaluating the enhanced HIT model via qualitative data collection.

In the previous chapter (Chapter Three) stage one of the first phase was described and in section 3.5 the candidate HIT model was presented. The next chapter (Chapter Five) will discuss stage two of the first phase: testing the candidate HIT model through quantitative data collection.

CHAPTER FIVE: QUANTITATIVE PHASE AND ENHANCED RESEARCH MODEL

5.1 Introduction

Chapter four explained in detail the methodology adopted for this research and Chapter Three presented the candidate HIT model. This integrative model was derived from three sources (academic, IT industry publications and published reports of incidents) and provides the groundwork for this phase of the study.

This chapter discusses the following in greater detail: survey design, target population and analyses of the survey. It also covers the main changes in the candidate HIT model and how the factor analysis results produced an improved list of factors. At the end of Chapter Five, an enhanced HIT model is presented.

5.2 Survey Development

5.2.1 Target Population

The target population for this survey are all from the United States of America (USA) and from the top security management level as discussed previously in section 4.4.2. The participants have one of the following job titles: IT Security Manager, Principal Cyber Security Manager, Security Systems Administrator and Senior IT Security Consultant. The individuals who accepted the invitation to participate in this survey came from a wide cross-section of industries including mining, utilities, construction, manufacturing, wholesale trade, retail trade, transportation and warehousing, information, finance and insurance, real-estate and rental and leasing, professional, scientific, and technical services, management of

companies and enterprises, administrative and support and waste management and remediation services, educational services, health care and social assistance and arts, entertainment, and recreation.

As discussed in section 4.2, one of the challenges for this study was to obtain access to the required population with the aforementioned specific job titles that are located in different regions from that of the researcher. The target population were recruited through an outside agency (Qualtrics). The survey contained a couple of questions to verify and to ensure that the participants were appropriate as a sample. Qualtrics distributed the survey to 568 individuals, with 100 completed, 247 unacceptable, with an overall 31% response rate which is considered acceptable (Cavana, Delahaye, and Sekaran 2001).

5.2.2 Survey Design

The development of the survey required a thorough understanding and accurate interpretation of the previous models of insider threat behaviour which were derived from three sources (academic research sources, published reports on reported incidents, and IT industry publications). This also took into consideration the research questions for this study.

The survey design process consisted of the following steps.

- Design the hard copy of the survey.
- Review the survey questions with the supervisors.
- Receive approval from the university's Ethics Committee.
- Design a preliminary version of the online survey.
- Conduct a pilot test.
- Design the online survey.
- Distribute the survey.
- Receive the responses.
- Analyse the survey responses.

- Enhance the model.

The survey used in this research was structured in a simple manner and was a maximum of three pages in length. It was estimated that the average time needed to complete the online survey would be 15 minutes. The survey for this study comprised six questions in two sections, as shown in Appendix 1.

The types of question used in this survey were:

- Multiple choice – single answer
- Matrix of choice – multiple answers
- Six-point Likert scale
- Free text boxes.

The first section of the survey asked the participants demographic questions such as their gender, job title, experience. These questions were a combination of multiple choices (single answer) and matrix of choice (multiple answers).

In the second section of the survey, the participants were asked two questions. The first question presented the nine insider threat behaviours factors; for each factor there were three variables presented in three statements in addition to three controlling statements (to control the common method bias in the survey (Conway and Lance 2010)) totalling thirty statements in all. This question used a six-point Likert scale to measure each item. The scale ranged from 1 to 6 and consisted of the following values: strongly agree, agree, neutral, disagree, strongly disagree and unable to judge.

According to Chomeya (2010), the reliability of Cronbach's alpha coefficient value of the six-point Likert scale is higher than the five-point Likert scale. Moreover, the validity from alpha coefficient of the six-point Likert scale yielded a higher reliability than the five-point Likert scale. This scale was chosen because of its appropriateness for the type of perceptual questions being used in this survey.

The second question in this section asked the participants to add their comments on the insider threat factors.

A cover letter was attached to explain the objectives of the survey and the purpose of the study. The potential participant was also informed of the anticipated time required to complete the survey. Special instructions regarding each question and how to complete the survey were provided.

A preliminary version of the survey was developed and presented to a panel of experienced academics in research design and structure. These academics were members of the researcher's thesis committee who systematically review and evaluate survey designs and questions. Several well-conceived changes were made according to their recommendations and review.

5.2.3 Reliability and Validity of the Survey

5.2.3.1 Pilot Test

According to Oppenheim (1992) and Fink (2010), a pilot test can determine the validity, reliability and practicality of the survey instrument. The extent to which respondents understand the survey's questions will determine the quality of the survey data. A pilot test of the survey helps the researcher to ascertain whether respondents understand the survey's questions and respond as intended. Fink (2010) suggests that a group of five to ten individuals who are similar to the potential respondents in demographic and experience can evaluate each survey questions individually or in a group.

In order to improve the reliability and quality of the survey, this survey was piloted using ten respondents in May 2012 who manually read through and answered the survey. The pilot study did not indicate any major issues with the survey.

Furthermore, a second pilot test was conducted using a Web-based method. The pilot test also used Qualtrics to ensure that the entire survey design was suitable and valuable for the potential data collected and free of defects. A total of ten respondents were selected by Qualtrics to test the survey. This was intended to determine whether there were any existing questions or data items that could present problems to the respondents before the official study was conducted.

5.2.3.2 Common Method Bias

Common method bias usually arises from having a common rate, a common measurement context, a common item context or from the characteristics of the items themselves (Podsakoff et al. 2003; Siemsen, Roth, and Oliveira 2010; Malhotra, Kim, and Patil 2006). According to Cote and Buckley (1987), method bias is the error in a measure as a result of how the data is collected. If a model has multiple constructs and these measures are utilised, these constructs may share a common method bias because the condition that the data was collected through one source and their similarity in construction (Donaldson and Grant-Vallone 2002). To avoid the significant impact of the method, the researchers need to prove the construct validity of the measures used. Researchers should be able to justify that the measures they chose have construct validity and provide evidence that they have taken into account common method bias in the design of their study (Conway and Lance 2010).

Two techniques were used to avoid common method bias and to prevent bias in the participants' responses to the survey.
Firstly, three controlling statements are added:

- The risk of insider threat behaviour is increased by the lack of customer and/or client participation in product development.
- The risk of insider threat behaviour is increased by a poor level of health and fitness among employees.
- The risk of insider threat behaviour is increased by organisation ownership being limited by shares.

Respondents should not agree with these three statements included in the survey because they are not related to the study at all. These statements were also chosen because they make no sense whatsoever. They have been added to the survey to test and control respondents' awareness and bias. Respondents who agreed with the three statements were excluded from the study. However, none of the respondents agreed with these control statements, indicating that the survey responses were not affected by common method bias, thereby demonstrating the rigour of this study.

Secondly, all questions were ordered in a random manner to ensure that respondents understood the questions and did not relate each question to the previous ones. The researcher decided not to present the questions relevant to each factor in a particular order to prevent respondents from answering the questions similarly. Thus, the questions were presented in a manner to test the respondents' awareness of control.

5.2.3.3 Internal Consistency

According to (Fink 2010, 158), a survey's internal consistency *"refers to the extent to which all the items or questions assess the same skill, characteristic, or quality"*. Cooper and Schindler (1998) state that reliability in a scales-based survey relates to the consistency of scale performance to ensure that the result will be free of random and systematic errors. Cronbach's alpha coefficient was calculated to provide an indication of whether the items in a scale were assessing the same construct. Alpha coefficient is a widely-used method for assessing internal consistency and reliability of a survey. This method was developed by Cronbach (1951) to measure the reliability of a scale for a specific sample group, since it is essential that items within a scale assess the same construct. The range of alpha coefficients is between 0 (inconsistent) to 1 (perfectly consistent). The higher the constant, the more reliable it is. An alpha coefficient of 0.70 is widely considered to be an acceptable value (Hair et al. 2010; Cooper and Schindler 1998). Internal consistency was obtained for this survey with a Cronbach alpha of .908 which is almost perfectly consistent.

5.3 Preliminary Analysis

In this section, the researcher discusses the analysis of the survey data. As previously mentioned, this survey is divided into two sections. The first part consists of the demographic questions and the second section consists of the insider threat behaviour factors questions. SPSS version 20.0 was used to analysis the collected data. This information is presented both in tabular and graphical form for the convenience of the reader the tables contains the numeric values where the graphs communicate the proportion.

5.3.1 Section One: Demographic Analysis

As mentioned earlier, of the 568 distributed surveys, the researcher received a total of 100 completed surveys. The majority (86%) of the participant responses were from males, while the number of responses from female participants was relatively small (14 or 14%). Moreover, the participants in this survey were divided into four categories according to their job title: IT Security Manager, Principal Cyber Security Manager, Security Systems Administrator and Senior IT Security Consultant. Most of the participants were IT security managers; 60% and 88.33% of this category were males (53 male and 7 female). Security Systems Administrators accounted for 15% of the participants (11 male and 4 female), Senior IT Security Consultant represented 14% (12 male and 2 female) of the total participants and finally, eleven participants 11% (10 male and 1 female) were Principal Cyber Security Managers (See Figure 5.1). Tables 5.1 and 5.2 summarise the demographics of the sample.

Table 5.1: Sample Demographics (N=100)

Gender	Response	Percentage
Male	86	86%
Female	14	14%
Total	100	100%
Job Title	**Response**	**Percentage**
IT Security Manager	60	60%
Principal Cyber Security Manager	11	11%
Security Systems Administrator	15	15%
Senior IT Security Consultant	14	14%
Total	100	100%

Table 5.2: Participants' gender and job titles

Job Title	Gender		
	Male	Female	Total
IT Security Manager	53	7	60
Principal Cyber Security Manager	10	1	11
Security Systems Administrator	11	4	15
Senior IT Security Consultant	12	2	14
Total	86	14	100

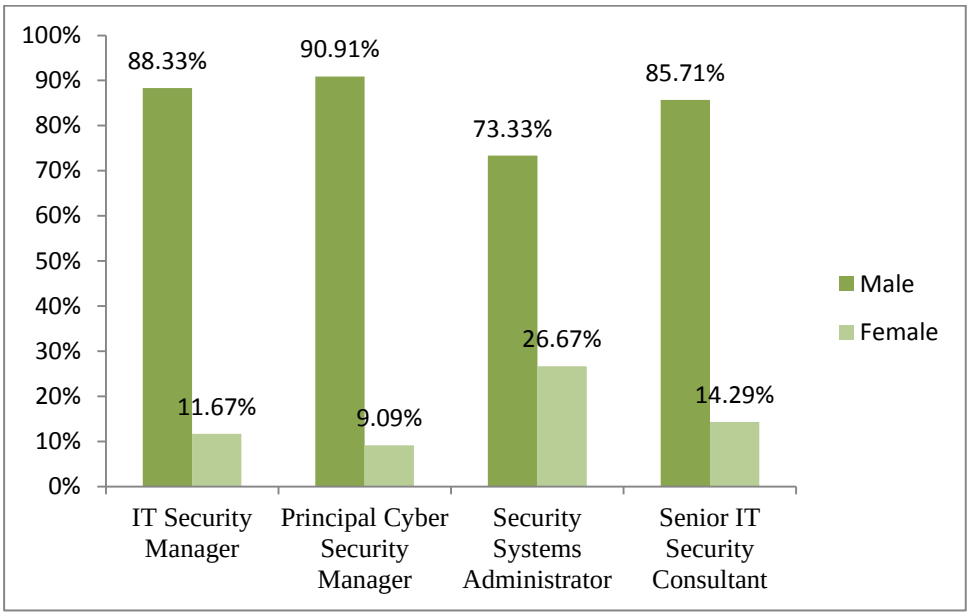


Figure 5.1: Participants' gender and job titles

Furthermore, the majority of the participants 87% (76 Male and 11 Female) were experienced in dealing with insider threat, while only 13% (10 Male and 3 Female) had never experienced insider threat previously as shown in Figure 5.2. Therefore, the sample was highly qualified to comment on insider threat behaviour, further contributing to the rigour of this research. Most IT security managers 88.33% had previously experienced insider threat, while only 11.67% had not. Similarly, 81.82% of the principal cyber security managers had experienced insider threat, and only 18.18% had never. Eighty per cent of the security systems administrators had previously experienced insider threat, and just 20% had not. Likewise, most senior IT security consultants (92.86%) had experienced insider threat, while 7.14% had not. Table 5.3 and Figure 5.3 present participants' job titles and their experience in dealing with insider threat behaviour.

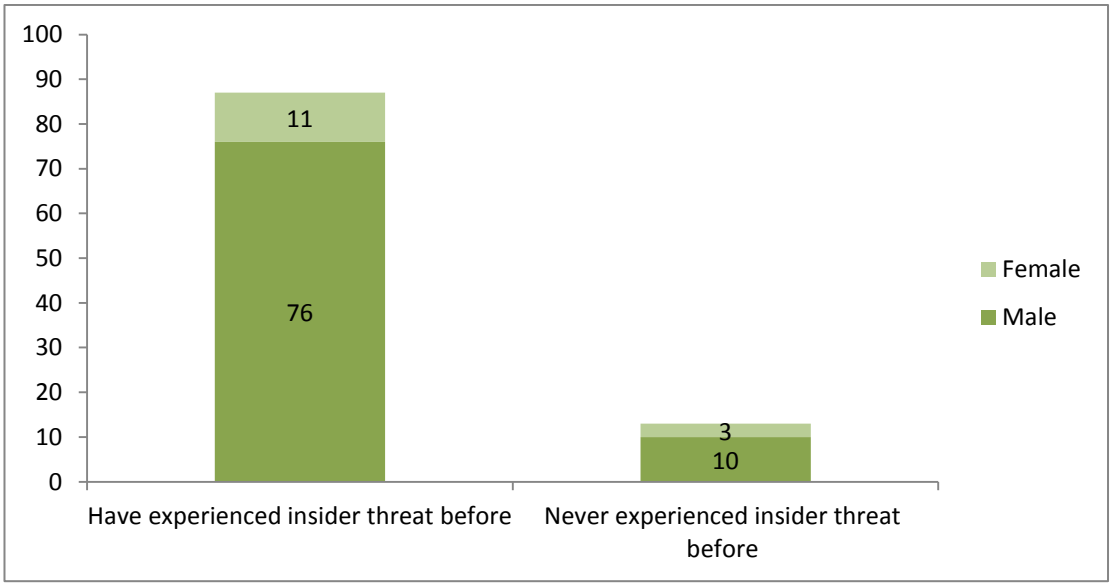


Figure 5.2: Participants' gender and their experience in dealing with insider threat

Table 5.3: Participants' job titles and their experience in dealing with insider threat behaviour

Do you have experience in dealing with insider threat behaviour?			
Job Title	**Yes**	**No**	**Total**
IT Security Manager	53	7	60
Principal Cyber Security Manager	9	2	11
Security Systems Administrator	12	3	15
Senior IT Security Consultant	13	1	14
Total	87	13	100

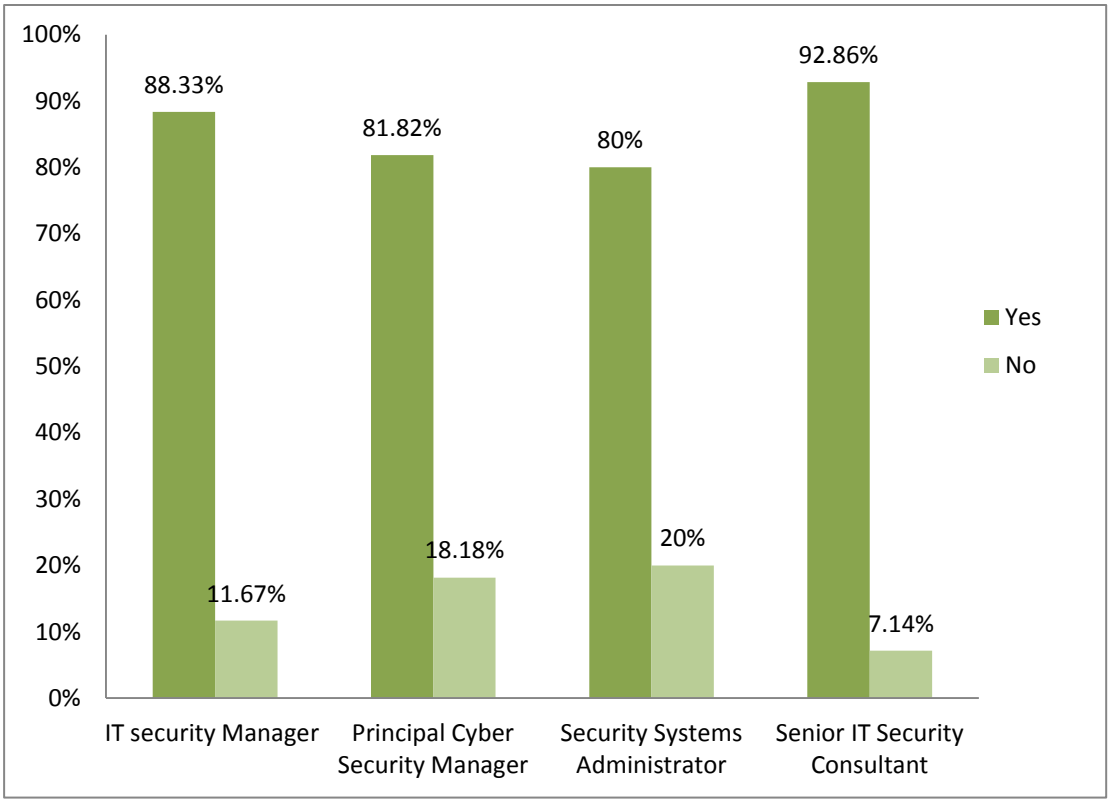


Figure 5.3: Participants' job titles and their experience in dealing with insider threat behaviour

As mentioned previously, the participants for this study came from various industry sectors including mining, utilities, construction, manufacturing, wholesale trade, retail trade, transportation and warehousing, information, finance and insurance, real-estate and rental and leasing, professional, scientific, and technical services,

management of companies and enterprises, administrative and support and waste management and remediation services, educational services, health care and social assistance and arts, entertainment, and recreation. The industries in this study were classified according to NAICS, the North American Industry Classification System which is used by Federal statistical agencies to classify the business establishments in the USA for the purpose of collecting and analysing statistical data. Table 5.4 indicates the numbers of participants from each industry.

Table 5.4: Numbers of participants from each industry and their gender

Industry	Response			Percentage
	Male	Female	Total	
Mining	1	0	1	1%
Utilities	3	1	4	4%
Construction	5	0	5	5%
Manufacturing	17	3	20	20%
Wholesale Trade	1	0	1	1%
Retail Trade	4	0	4	4%
Transportation and Warehousing	3	1	4	4%
Information	5	0	5	5%
Finance and Insurance	15	4	19	19%
Real Estate and Rental and Leasing	1	0	1	1%
Professional, Scientific, and Technical Services	16	2	18	18%
Management of Companies and Enterprises	2	0	2	2%
Administrative and Support and Waste Management and Remediation Services	2	0	2	2%
Educational Services	6	0	6	6%
Health Care and Social Assistance	8	2	10	10%
Arts, Entertainment, and Recreation	5	1	6	6%

5.3.2 Section Two: Insider Threat Factors

This section examines the nine major factors contributing to inappropriate insider threat behaviours that emerged from the investigation of past research literature,

published reports of incidents and from IT industry publications. These factors include: psychological factors, outsourcing providing the opportunity, information security policy, remote access facilities, cultural differences, motivation to carry out the abuse, access and level of trust, insider knowledge and technical skills.

This section discusses separately the three statements for each of the nine factors. The participants were asked to indicate their level of agreement (strongly agree (1), agree (2), neutral (3), disagree (4), strongly disagree (5) and unable to judge (6)) with each statement. The mean and percentage were calculated for each factor.

Descriptive statistics were computed to indicate how respondents answered the range of items in the survey and to understand the key variables. The researcher divided the analysis of the second section of the survey into nine parts, each of which discusses one of the proposed factors in order to demonstrate the analysis process.

5.3.2.2 Participants' Overall Responses to Section Two

The participants' average responses to the 27 statements pertaining to the increased risk of insider threat behaviour is based on their experience, was between 1.96 and 2.77 – corresponding to a value of "strongly agree" or "agree" (1 = strongly agree, 2 = agree, 3 = neutral, 4 = disagree, 5 = strongly disagree, 6= unable to judge). Three statements had an average response between 3.0 and 3.24; all three statements were closer to neutral. Table 5.5 lists the statements in ascending order of the mean value of all participants' responses.

Descriptive statistics were computed to indicate how the participants responded to each statement in this section of the survey and to understand the profiles of all variables.

Table 5.5: Descriptive statistics

The risk of insider threat behaviour is increased by ...	Min Value	Max Value	Mean	Variance	Standard Deviation	Total Responses
...the implementation of inappropriate information security policy.	1	6	1.96	0.83	0.91	100
...organisational culture that tolerates unethical behaviour.	1	5	1.96	0.99	0.99	100
...not promptly canceling access of ex-employees.	1	5	2.1	1.08	1.04	100
...outdated information security procedures or policies.	1	5	2.1	0.88	0.94	100
...a technically skilled insider who violates the security for personal gain.	1	5	2.13	1.12	1.06	100
...insiders being motivated to harm their organisation.	1	6	2.15	1.24	1.11	100
...psychological factors such as social frustrations or computer dependency.	1	5	2.18	0.8	0.89	100
...insiders' knowledge of the potential value of the organisation's information.	1	5	2.22	1	1	100
...outsourced employees being given the same logical and/or physical access as the organisation’s regular employees.	1	6	2.26	1.08	1.04	100
...insufficient information security policy training and awareness.	1	6	2.34	1.14	1.07	100
...insiders being unduly motivated by financial gain.	1	5	2.38	1.23	1.11	100
...insiders' knowledge of the methods used to detect insider threat behaviour.	1	6	2.41	1.11	1.06	100
...granting access to third- parties contracted to conduct work within the organisation.	1	5	2.44	0.83	0.91	100
...insiders' knowledge of methods to grant access to the organisation's information.	1	5	2.45	0.98	0.99	100
...inappropriate or concerning behaviour prior to the incident such as delays, absences and poor job performance.	1	5	2.47	1.14	1.07	100
...insiders being vulnerable to coercion by outsider.	1	5	2.48	1.28	1.13	100
...allowing authorised mobile device to access organisational information from outside the organisation physical boundary.	1	6	2.48	1.08	1.04	100
...high levels of access to IT systems given to employees.	1	5	2.51	1.26	1.12	100
...the organisation engaging a relatively high number of outsourcing agreements.	1	6	2.54	1.04	1.02	100

The risk of insider threat behaviour is increased by ...	Min Value	Max Value	Mean	Variance	Standard Deviation	Total Responses
...cultural clash between employees and the organisation.	1	5	2.54	1.06	1.03	100
...personal factors such as alcohol and drug addiction or violent behaviour.	1	6	2.54	1.36	1.17	100
...giving employees remote access to organisational information.	1	6	2.75	1.22	1.1	100
...employees' level of technical sophistication.	1	5	2.76	0.97	0.99	100
...employees from backgrounds where acceptable practices differ.	1	6	2.77	1.29	1.14	100
...high levels of trust given to employees.	1	6	3	1.47	1.21	100
...employees working from home.	1	6	3.22	1.32	1.15	100
...employees having formal training in computer science, IT or similar.	1	6	3.24	1.38	1.17	100

5.3.2.3 Participants' Responses to Each Factor

Individual characteristics

There are numerous personal characteristics that could indicate an increased possibility of harmful behaviour on the part of the insider as detailed in section 3.5.1. Table 5.6 summarises the statements and the responses to the individual characteristics factor.

Table 5.6: Individual characteristics

Please indicate your level of agreement to each statement: **The risk of insider threat behaviour is increased by ...**	**[1] Strongly Agree (SA)**	**[2] Agree (A)**	**[3] Neutral (N)**	**[4] Disagree (D)**	**[5] Strongly Disagree (SD)**	**[6] Unable to judge (UJ)**	**Mean**
...psychological factors such as social frustrations or computer dependency.	22	47	23	7	1	0	2.18
...personal factors such as alcohol and drug addiction or violent behaviour.	19	35	27	12	6	1	2.54
...inappropriate or concerning behaviour prior to the incident such as delays, absences and poor job performance.	15	46	22	11	6	0	2.47

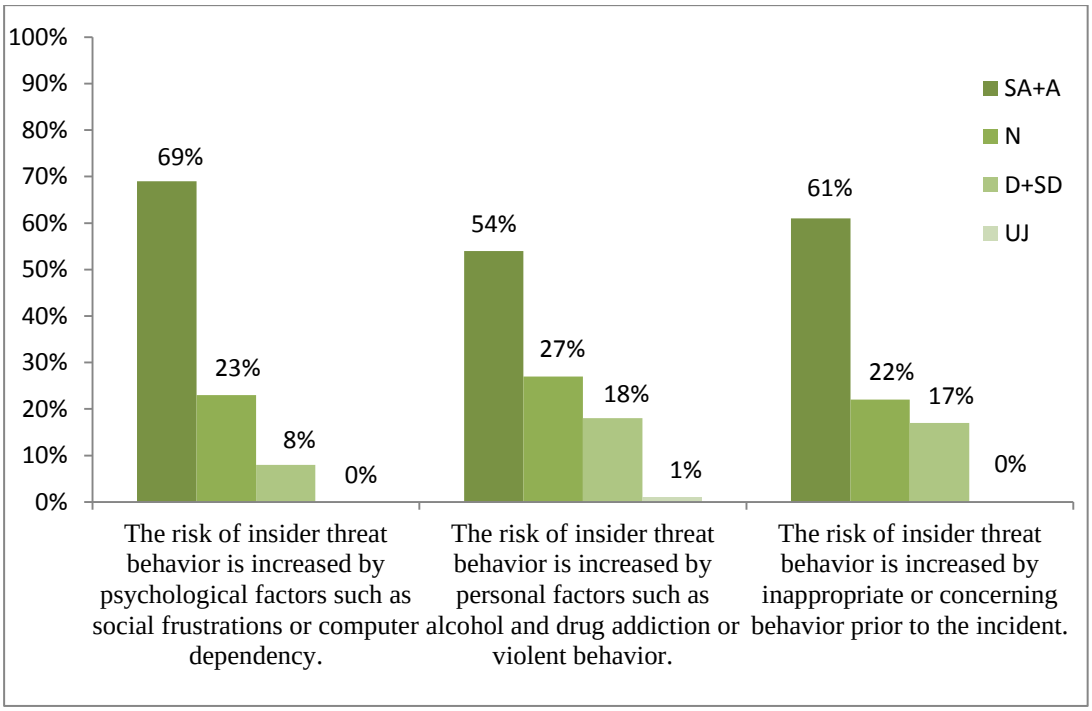


Figure 5.4: Individual characteristics

The researcher included three statements to evaluate the personal characteristics factor. As can be seen in Figure 5.4, most participants agreed 69% (22% (SA) + 47% (A)) that psychological factors such as social frustrations or computer dependency may increase the risk of insider threat behaviour, while only 8% (7% (D) + 1% (SD)) of the participants disagreed. On the other hand, 23% were neutral (N) and neither agreed nor disagreed that social frustrations or computer dependency may increase the risk of an insider threat behaviour.

54% of participants agreed (19% (SA) + 35% (A)) that personal factors such as alcohol and drug addiction or violent behaviour may increase the risk of an insider threat behaviour, and just 18% (12% (D) + 6% (SD)) of the participants disagreed, while 27% of the respondents were neutral (N).

Additionally, 61% of participants agreed (15% (SA) + 46% (A)) that inappropriate or concerning behaviour prior to the incident such as delays, absences and poor job performance, may indicate an increased risk of an insider threat behaviour; in contrast, no more than 17% (11% (D) + 6% (SD)) of the participants disagreed.

However, 22% of the participants were neutral (N) about the statement that inappropriate or concerning behaviour prior to the incident could indicate and increased risk of insider threat behaviour.

The outcome supports the proposition that the personal characteristics can be considered as one of the factors that increase the risk of insider threat behaviour. The percentage in Figure 5.4 and the mean from Table 5.6 indicates that more than the half of the participants agreed about all three statements. Moreover, this was confirmed by participants' comments. An IT security manager claimed *"in my experience the likely hood of a problem depends on the personalities involved. Organisations need to be sure they are not making it easy to get to sensitive data, but there is a balance between security and utility. It comes down to people"*. Another IT security manager said "A threat inside or outside will be acted out by unscrupulous peoples". Finally, a Principal Cyber Security Manager stated *"Insider threat behaviour is affected by the psychology of human beings living in this world"*.

Outsourcing

The researcher provides three statements to evaluate whether outsourcing is an important factor contributing to inappropriate insider threat behaviour (outsourcing described in detail in section 3.5.2). Table 5.7 presents the statements and the responses to the outsourcing factor.

Table 5.7: Outsourcing

Please indicate your level of agreement to each statement: The risk of insider threat behaviour is increased by ...	[1] Strongly Agree (SA)	[2] Agree (A)	[3] Neutral (N)	[4] Disagree (D)	[5] Strongly Disagree (SD)	[6] Unable to judge (UJ)	Mean
...outsourced employees being given the same logical and/or physical access as the organisation's regular employees.	22	46	21	7	3	1	2.26
...the organisation engaging a relatively high number of outsourcing agreements.	15	36	32	15	1	1	2.54
...granting access to third- parties contracted to conduct work within the organisation.	15	38	37	8	2	0	2.47

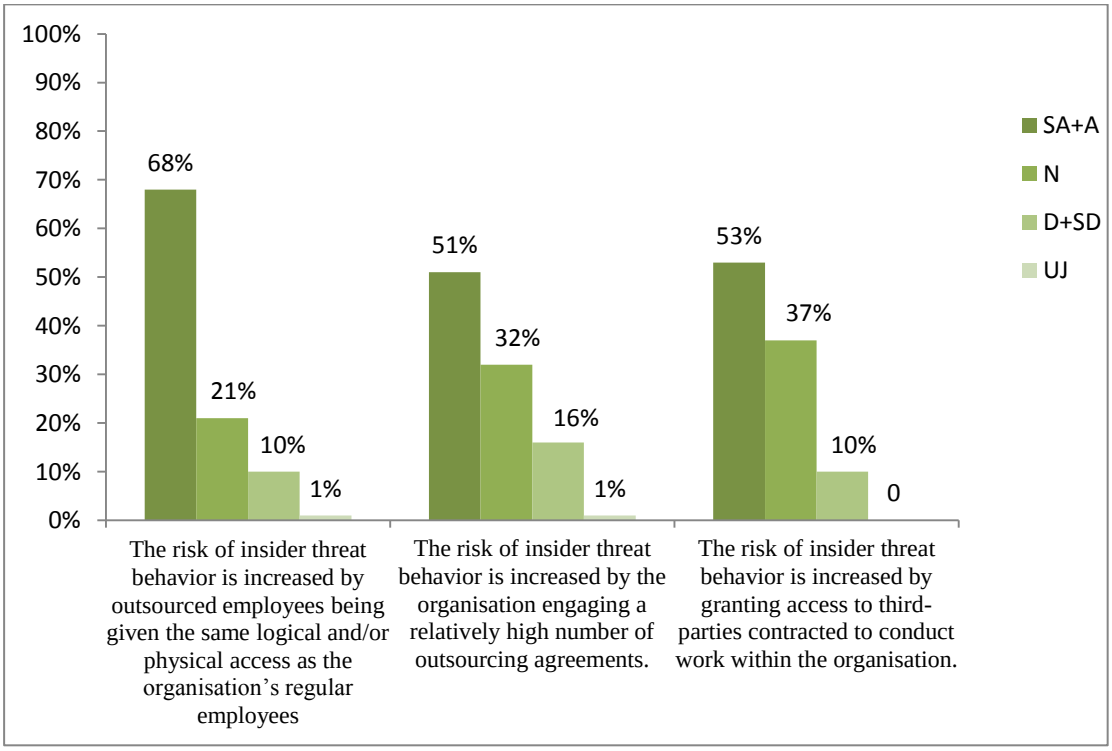


Figure 5.5: Outsourcing

As can be seen in Figure 5.5, most participants agreed 68% (22% SA + 46% (A)) that the risk of insider threat behaviour is increased by outsourced employees being given the same logical and/or physical access as the organisation's regular employees, while only 10% (7% (D) + 3% (SD)) of the participants disagreed. On the other hand, 21% were neutral (N) and neither agreed nor disagreed with the statement; only one participant was unable to judge.

About half of the participants 51% agreed (15% (SA) + 36% (A)) that if organisations engage a relatively high number of outsourcing agreements, this is most likely to increase the risk of insider threat behaviour; however, 16% (15% (D) + 1% (SD)) of the participants disagreed. A total of 32% of the participants were neutral (N); only one participant was unable to judge.

Moreover, 53% of participants agreed (15% (SA) + 38% (A)) that granting access to third parties contracted to conduct work within the organisation increases the risk of insider threat behaviour; however, no more than 10% (8% (D) + 2% (SD)) of the participants disagreed. Thirty-seven per cent of the participants were neutral (N); none of the participants was unable to judge.

The responses regarding the outsourcing factor were mixed. The participants' responses for this factor were varied since the percentage in Figure 5.5 indicates that most of the participants agreed that the risk of insider threat behaviour is increased by outsourced employees being given the same logical and/or physical access as the organisation's regular employees. On the other hand, responses to other statements were not that clear. Half of the participants agreed that the risk of insider threat behaviour is increased by the organisation engaging a relatively high number of outsourcing agreements and granting access to third parties contracted to conduct work within the organisation, while almost 30% of them disagree. Table 5.7 shows that the mean of the participants' responses to each statement were [2] agree; thus the researcher concludes that another analysis method needs to be utilised in order to identify whether or not the outsourcing factor should be considered as a factor contributing to an insider threat.

Information Security Policy

An organisation can become a victim as a result of its security policy in several ways including the implementation of inappropriate security policy, insufficient information security policy training and awareness, and out-dated information security procedures or policies as described in section 3.5.3. Table 5.8 summarises the statements and the responses to the information security policy factor.

Table 5.8: Information security policy

Please indicate your level of agreement to each statement: **The risk of insider threat behaviour is increased by ...**	**[1] Strongly Agree (SA)**	**[2] Agree (A)**	**[3] Neutral (N)**	**[4] Disagree (D)**	**[5] Strongly Disagree (SD)**	**[6] Unable to judge (UJ)**	**Mean**
...the implementation of inappropriate information security policy.	31	51	11	6	0	1	1.96
...insufficient information security policy training and awareness.	20	45	21	10	3	1	2.34
...outdated information security procedures or policies.	26	49	16	7	2	0	2.10

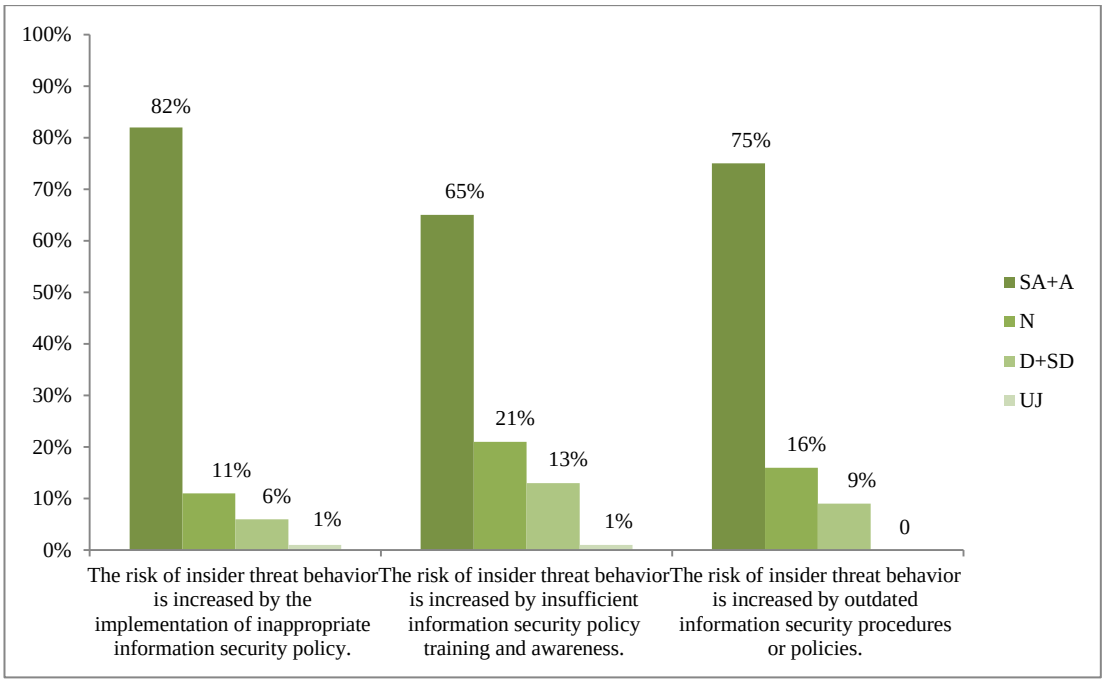


Figure 5.6: Information security policy

As can be seen in Figure 5.6, the majority of participants agreed 82% (31% SA + 51% (A)) that the risk of insider threat behaviour is increased by the implementation of inappropriate information security policy, while only 6% (6% (D) + 0% (SD)) of the participants disagreed. On the other hand, 11% were neutral (N) and neither agreed nor disagreed; only one participant was unable to judge.

Moreover, 65% (20% (SA) + 45% (A)) of the participants agreed that insufficient information security policy training and awareness will increase the risk of insider threat behaviour, while 13% (10% (D) + 3% (SD)) of the participants disagreed. A total of 21% of the participants were neutral (N), while just one participant was unable to judge.

Seventy-five per cent of participants agreed (26% (SA) + 49% (A)) that out-dated information security procedures or policies will increase the risk of insider threat behaviour, whereas only 9% (7% (D) + 2% (SD)) of the participants disagreed. Sixteen per cent of the participants were neutral (N) and none of the participants was unable to judge.

Information security policy is an essential factor contributing to inappropriate insider threat behaviour. The majority of the participants' responses indicated the importance of information security policy as can be seen in Figure 5.6. Most participants agreed that the risk of insider threat behaviour is increased by implementation of inappropriate information security policy, insufficient information security policy training and awareness and out-dated information security policy. Furthermore, the means presented in Table 5.8 suggest that the participants agree that information security policy is a very important aspect of insider threat behaviour.

Participants' comments also supported the significance of information security policy; an IT security manager stated *"Having strong policies here is critical. Also, having an internal system to detect the possibility of insider threat behaviour is equally important"*. Another IT security manager claimed *"The idea is to have a strict security policy, enforce it and test it. Educate all the employee, personnel and contractors accessing you facilities and networks"*. Moreover, A Senior IT Security Consultant maintained that *"Security policy is everything and sticking to that policy"*. Finally, one of the principal Cyber Security Managers claimed *"insider threat is always a danger. Making sure the right policies are in place to help in reducing risks"*.

Remote Access

Remote access allows employees to access the organisation's network from anywhere in the world. The researcher provided three statements to evaluate whether remote access is an important factor contributing to inappropriate insider threat behaviour (remote access described in detail in section 3.5.4). Table 5.9 presents the statements and the responses to the remote access factor.

Table 5.9: Remote access

Please indicate your level of agreement to each statement: The risk of insider threat behaviour is increased by ...	[1] Strongly Agree (SA)	[2] Agree (A)	[3] Neutral (N)	[4] Disagree (D)	[5] Strongly Disagree (SD)	[6] Unable to judge (UJ)	Mean
...employees working from home.	6	24	26	31	12	1	3.22
...giving employees remote access to organisational information.	13	31	29	23	3	1	2.75
...allowing authorised mobile device to access organisational information from outside the organisation physical boundary.	15	42	28	11	3	1	2.48

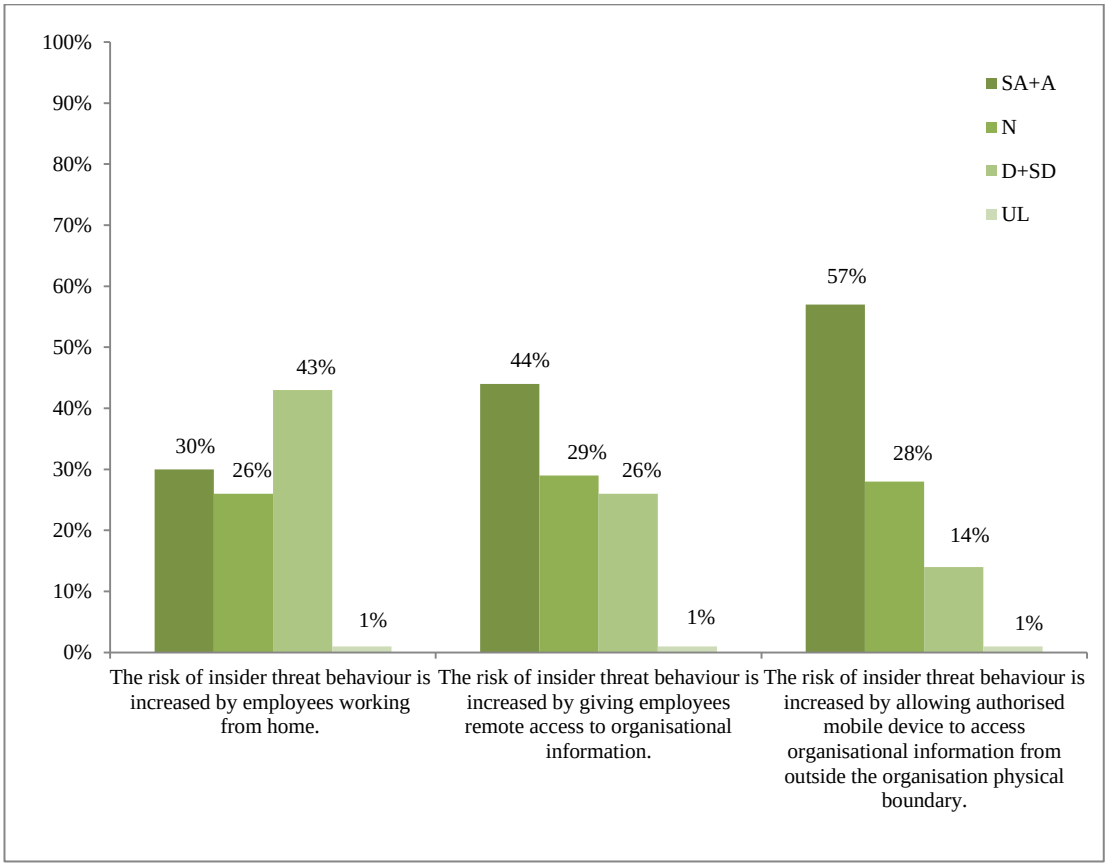


Figure 5.7: Remote access

The researcher included three statements to evaluate the remote access factor. As can be seen in Figure 5.7, although 30% (6% (SA) + 24% (A)) of participants agreed that working from home increases the insider threat behaviour, 43% (31% (D) + 12% (SD)) of them disagreed. Twenty-six per cent were neutral (N) and neither agreed nor disagreed that the risk of insider threat behaviour could be increased by an employee working from home. Only one participant was unable to judge.

On the other hand, 44% of participants agreed (13% (SA) + 31% (A)) that giving employees remote access to organisational information increases the possibility of insider threat, while 26% (23% (D) + 3% (SD)) of the participants disagreed. A total of 29% of the participants were neutral (N) and one participant was unable to judge.

Similarly, more than half of the 57% of participants agreed (15% (SA) + 42% (A)) that allowing authorised mobile devices to access organisational information from outside the organisation's physical boundaries could increase the risk of insider threat behaviour; however, no more than 14% (11% (D) + 3% (SD)) of the participants disagreed. However, 28% of the participants were neutral (N) and one participant was unable to judge.

The participants' responses regarding remote access factor were varied. Despite the fact that the percentage in Figure 5.7 shows that the participants disagreed that working from home could increase the insider threat behaviour, Table 5.9 indicates that the mean for this statement is neutral. Alternatively, Table 5.9 indicates that the mean for the other two statements were [2] agree. Therefore, the researcher concludes that another analysis method is essential in order to identify whether or not remote access is a factor contributing to insider threat.

Cultural factors

Cultural factors in this study cover the organisational culture and national/regional culture as described in section 3.5.5. Table 5.10 summarise the statements and the responses to the cultural factors.

Table 5.10: Cultural factors

Please indicate your level of agreement to each statement: The risk of insider threat behaviour is increased by ...	[1] Strongly Agree (SA)	[2] Agree (A)	[3] Neutral (N)	[4] Disagree (D)	[5] Strongly Disagree (SD)	[6] Unable to judge (UJ)	Mean
...organisational culture that tolerates unethical behaviour.	37	41	14	5	3	0	1.96
...employees from backgrounds where acceptable practices differ.	11	34	31	17	5	2	2.77
...cultural clash between employees and the organisation.	17	31	37	11	4	0	2.54

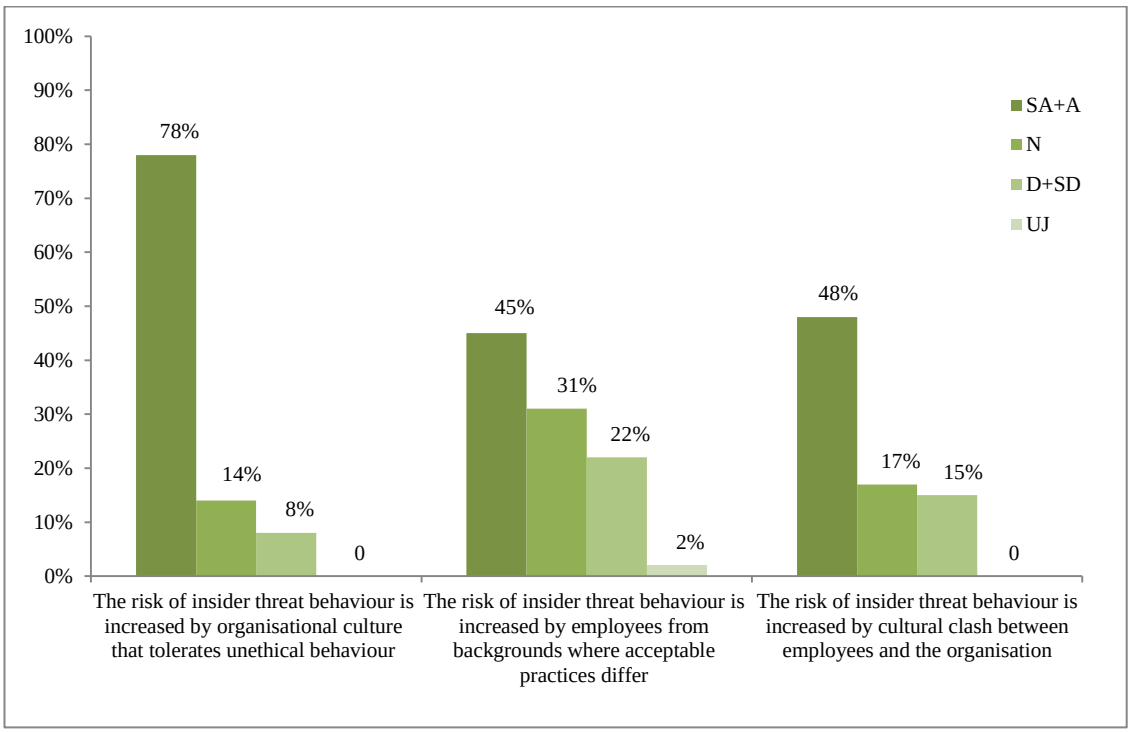


Figure 5.8: Cultural factors

Figure 5.8 illustrates that the majority of participants agreed 78% (37% SA + 41% (A)) that the risk of insider threat behaviour is increased by organisational culture

that tolerates unethical behaviour, while only 8% (5% (D) + 3% (SD)) of the participants disagreed. On the other hand, 14% were neutral (N) and neither agreed nor disagreed.

About 45% (11% (SA) + 34% (A)) of participants agreed that employees from various backgrounds where acceptable practices differ will increase the risk of insider threat behaviour; however 22% (17% (D) + 5% (SD)) of the participants disagreed and a total of 31% of the participants were neutral (N) concerning that statement and only two participants were unable to judge.

Likewise, 48% (17% (SA) + 31% (A)) of participants agreed that cultural clash between employees and the organisation increases the risk of insider threat behaviour, and 15% (11% (D) + 4% (SD)) of the participants disagreed. 37% of the participants were neutral (N).None of the participants was unable to judge.

To sum up, the results indicate that the responses concerning the importance of the cultural factor in increasing the risk of insider threat were mixed. The participants' responses for this part were divided, since the percentage in Figure 5.8 indicates that most of the participants agreed with the first statement (the risk of insider threat behaviour is increased by organisational culture that tolerates unethical behaviour), while fewer than half agreed with the other two statements (that employees from different backgrounds where acceptable practices differ and cultural clash between employees and the organisation increased the risk of insider threat behaviour). On the other hand, Table 5.10 demonstrates that the mean of the participants' responses for all three statements were [2] agree. Consequently, the need for a further analysis method is necessary.

Motivation

The motivation for deliberate insider threats could be considered as the fuel for the malicious actions as detailed in section 3.5.6. The researcher provided three statements to evaluate whether or not motivation is an important factor contributing

to inappropriate insider threat behaviour. Table 5.11 summarises the statements and the responses to the motivation factor.

Table 5.11: Motivation

Please indicate your level of agreement to each statement: The risk of insider threat behaviour is increased by ...	[1] Strongly Agree (SA)	[2] Agree (A)	[3] Neutral (N)	[4] Disagree (D)	[5] Strongly Disagree (SD)	[6] Unable to judge (UJ)	Mean
...insiders being unduly motivated by financial gain.	24	34	27	10	5	0	2.38
...insiders being motivated to harm their organisation.	29	45	15	5	5	1	2.15
...insiders being vulnerable to coercion by outsider.	20	38	21	16	5	0	2.48

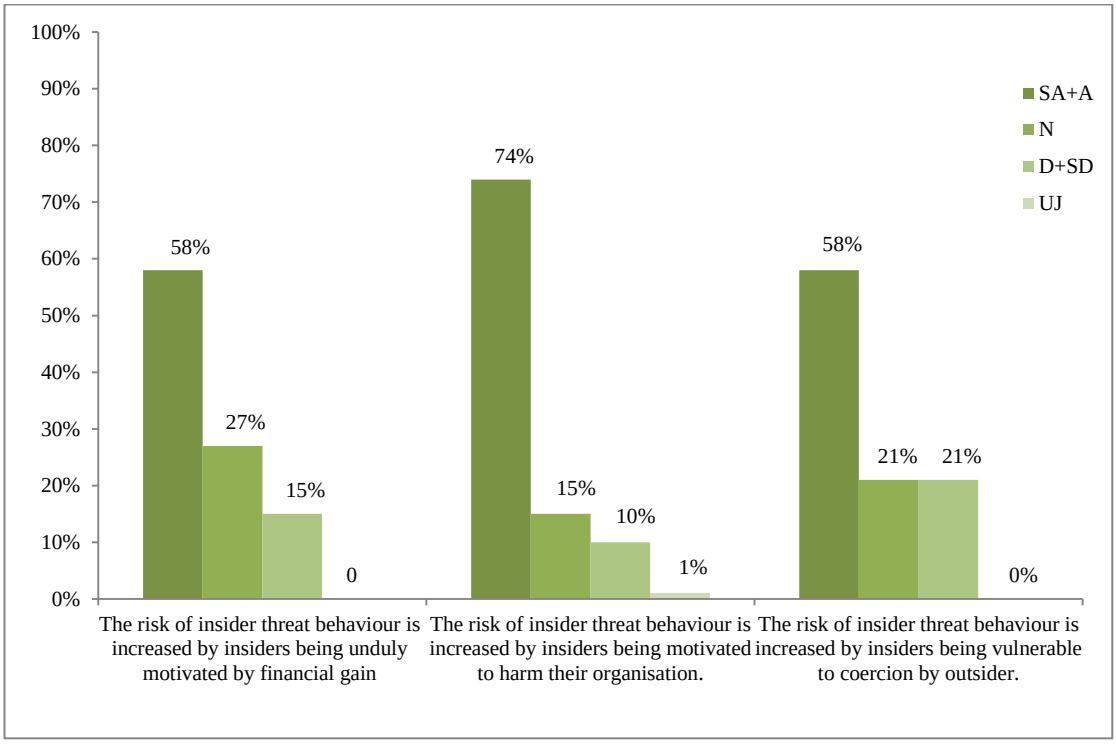


Figure 5.9: Motivation

Figure 5.9 shows that more than half of participants agreed 58% (24% SA + 34% (A)) that the risk of insider threat behaviour is increased by insiders being unduly motivated by financial gain, while 15% (10% (D) + 5% (SD)) of the participants disagreed. On the other hand, 27% were neutral (N) and neither agreed nor disagreed that insider threat behaviour is increased by insiders being motivated by financial gain.

Almost three quarters of the participants 74% (29% (SA) + 45% (A)) agreed that insiders being motivated to harm their organisation increased the risk of insider threat behaviour, while only 10% (5% (D) + 5% (SD)) of the participants disagreed. Fifteen per cent of the participants were neutral (N), and only one participant was unable to judge.

Moreover, 58% of participants agreed (20% (SA) + 38% (A)) that insiders being vulnerable to coercion by outsider increased the risk of insider threat behaviour. In contrast, 21% (16% (D) + 5% (SD)) of the participants disagreed and 21% of the participants were neutral (N). None of the participants was unable to judge.

After reviewing the outcome of this part, the researcher concluded that motivation is a factor contributing to insider threat behaviour. Most of the participants' responses supported the importance of motivation, as can be seen in Figure 5.9. The majority of the participants agreed with the second statement (the risk of insider threat behaviour is increased by insiders being motivated to harm their organisation), and more than the half of the participants agreed about the other statements. Moreover, the mean presentation in Table 5.11 indicates that the participants agreed that motivation can produce insider threat behaviour.

Additionally, participants' comments support the proposition that the insider motivation is an essential factor in insider threat behaviour, an IT security manager claimed that "*Many good points here. Motivation for some will always very important"*. Another IT security manager maintained *"Threat materialize based on the same factors at work in any theft situation - opportunity, motive and the*

risk/reward calculation on the part of the individual". Moreover, A Senior IT Security Consultant stated *"I think the main factor regarding insider threat behaviour is a disgruntled employee's desire to sabotage or give confidential information to another employer"*. Another Senior IT Security Consultant said *"An insider's personal motivation, training experience, emotional state, cultural norms, all are pivotal factors toward insider threats"*. Finally, one of the principal Cyber Security Managers claimed that insider threat behaviour is *"usually due to revenge or money"*.

Access and Level of Trust

Misuse of access is one of the most difficult types of attack to detect and prevent, since the insider uses his or her authorised access rights to perform illegal tasks (access and level of trust described in detail in section 3.5.7). The researcher provided three statements regarding access and level of trust to evaluate whether it could be considered as an important factor contributing to inappropriate insider threat behaviour or not. Table 5.12 summarises the statements and the responses to the motivation factor.

Table 5.12: Access and Level of Trust

Please indicate your level of agreement to each statement: **The risk of insider threat behaviour is increased by ...**	**[1] Strongly Agree (SA)**	**[2] Agree (A)**	**[3] Neutral (N)**	**[4] Disagree (D)**	**[5] Strongly Disagree (SD)**	**[6] Unable to judge (UJ)**	**Mean**
...not promptly cancelling access of ex-employees.	31	42	17	6	4	0	2.10
...high levels of trust given to employees.	10	29	25	24	11	1	3.00
...high levels of access to IT systems given to employees.	18	39	23	14	6	0	2.51

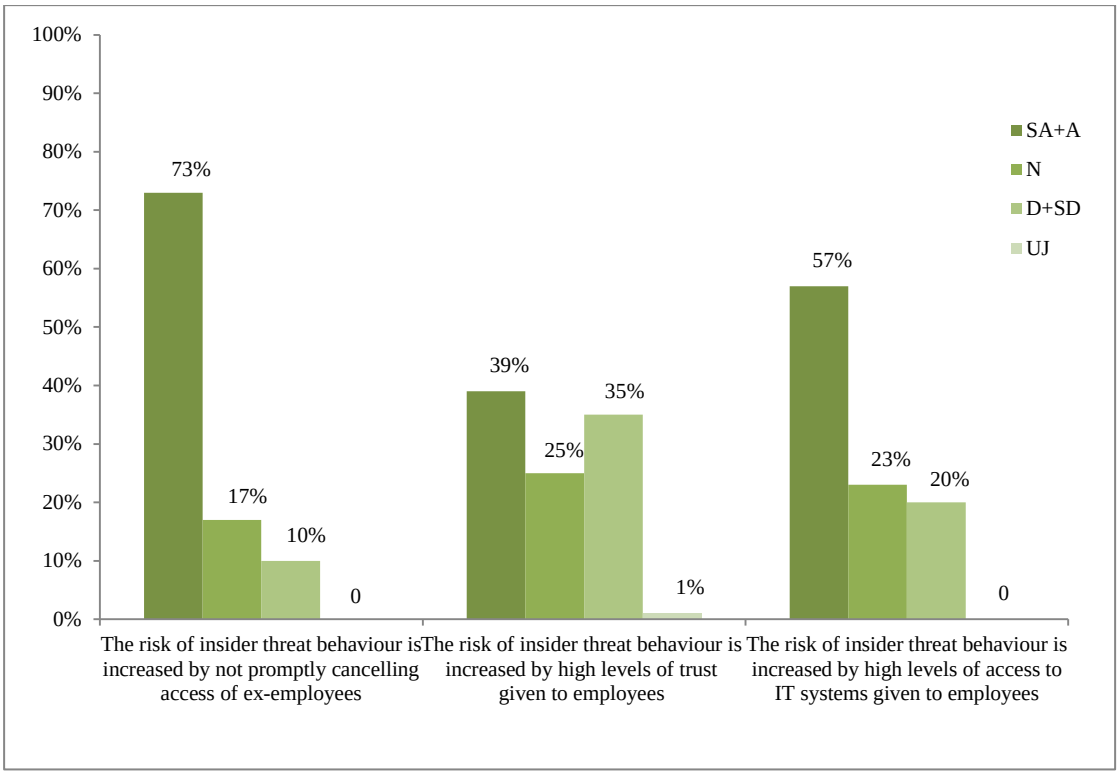


Figure 5.10: Access and Level of Trust

Figure 5.10 demonstrates that, most of the participants agreed 73% (31% SA + 41% (A)) that the risk of insider threat behaviour is increased by not promptly cancelling access of ex-employees, and only 10% (6% (D) + 4% (SD)) of the participants disagreed. On the other hand, 17% were neutral (N) and none of the participants was unable to judge.

Thirty-nine per cent (10% (SA) + 29% (A)) of the participants agreed that high levels of trust given to employees will increase the risk of an insider threat behaviour, but 35% (24% (D) + 11% (SD)) of the participants disagreed and 25% of the participants were neutral (N) regarding to this statement with only one participant being unable to judge.

Approximately half of the participants 57% (18% (SA) + 39% (A)) agreed that high levels of access to IT systems given to employees will increase the risk of insider threat behaviour. However, only 20% (14% (D) + 6% (SD)) of the participants

disagreed, 23% of the participants were neutral (N), and none of the participants was unable to judge.

To sum up, the responses regarding access and level of trust factor were mixed. While most of the participant agreed with the first statement, less than half agreed with the second statement. The percentages in Figure 5.10 and the mean in Table 5.12 indicate that most participants agreed that the risk of insider threat behaviour is increased when not promptly cancelling access of ex-employees. Moreover, Senior IT Security Consultant claimed *"cancel ex-employee access immediately"*. However, the mean was neutral regarding the third statement (the risk of insider threat behaviour is increased by the high levels of trust given to employees). Thus, the researcher concludes that an additional analysis method is needed in order to find out whether access and level is a contributing factor to insider threat behaviour.

Insiders' knowledge

Employees have a great knowledge about their organisation and are usually familiar with some or all the internal processes of their target systems as described in section 3.5.8. Table 5.13 summarises the statements and the responses to the insiders' knowledge factor.

Table 5.13: Insiders' knowledge

Please indicate your level of agreement with each statement: The risk of insider threat behaviour is increased by ...	[1] Strongly Agree (SA)	[2] Agree (A)	[3] Neutral (N)	[4] Disagree (D)	[5] Strongly Disagree	[6] Unable to judge (UJ)	Mean
...insiders' knowledge of the potential value of the organisation's information.	28	33	30	7	2	0	2.22
...insiders' knowledge of the methods used to detect insider threat behaviour.	18	40	31	7	2	2	2.41
...insiders' knowledge of methods of granting access to the organisation's information.	17	38	30	13	2	0	2.45

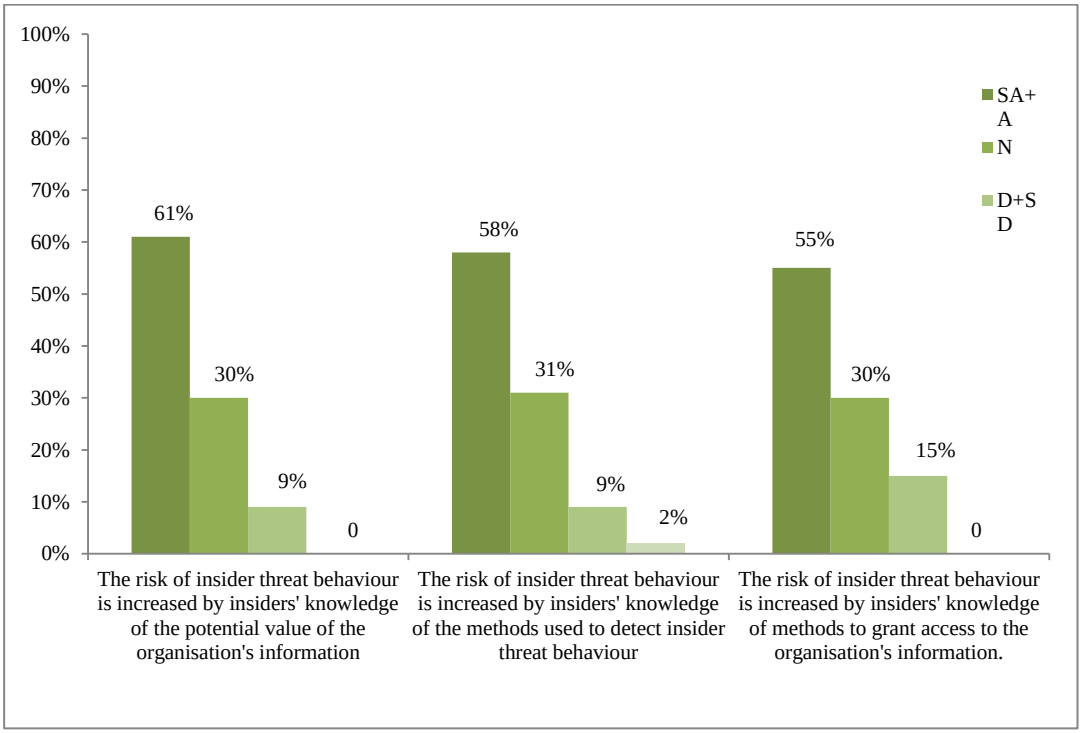


Figure 5.11: Insiders' knowledge

Figure 5.11 shows that 61%of the participants agreed (28% SA + 33% (A)) that the risk of insider threat behaviour is increased by insiders' knowledge of the potential

value of the organisation's information to outsiders. Only 9% (7% (D) + 2% (SD)) of the participants disagreed. On the other hand, 33% were neutral (N) and none of the participants was unable to judge.

Additionally, 58% (18% (SA) + 40% (A)) agreed that insiders' knowledge of the methods used to detect insider threat behaviour will increase the risk of such behaviour. However, only 9% (7% (D) + 2% (SD)) of the participants disagreed. A total of 31% of the participants were neutral (N),and two participants were unable to judge.

Similarly, 55% (17% (SA) + 38% (A)) of participants agreed that insiders' knowledge of methods to grant access to the organisation's information will increase the risk of insider threat behaviour. Only 15% (13% (D) + 2% (SD)) of the participants disagreed, about 30% of the participants were neutral (N), and none of the participants was unable to judge.

The outcome of this part of the survey has partially supported the proposition that insiders' knowledge is one of the factors that contributing to insider threat since only approximately half of the participants agreed with the three statements as can be seen in Figure 5.11. In addition, the mean presented in Table 5.13 indicates that the participants agreed that insiders' knowledge is a very important aspect of insider threat behaviour. Consequently, a further investigation and analysis is required to identify whether or not insiders' knowledge should be considered as a factor contributing to insider threat.

Technical skills

Insiders often have the technical skills which are usually limited to the system they are familiar with which may increase their opportunities to compromise this system (details in section 3.5.9). The researcher provides three statements to evaluate whether IT skills are an important factor contributing to inappropriate insider threat behaviour or not. Table 5.14 summarised the statements and the responses to the IT skill factor.

Table 5.14: IT skills

Please indicate your level of agreement with each statement: **The risk of insider threat behaviour is increased by ...**	**[1] Strongly Agree (SA)**	**[2] Agree (A)**	**[3] Neutral (N)**	**[4] Disagree (D)**	**[5] Strongly Disagree (SD)**	**[6] Unable to judge (UJ)**	**Mean**
...employees having formal training in computer science, IT or similar.	6	24	25	32	11	2	3.24
...technically skilled insider who violates the security for personal gain.	29	46	12	9	4	0	2.13
...employees' level of technical sophistication.	7	39	28	23	3	0	2.76

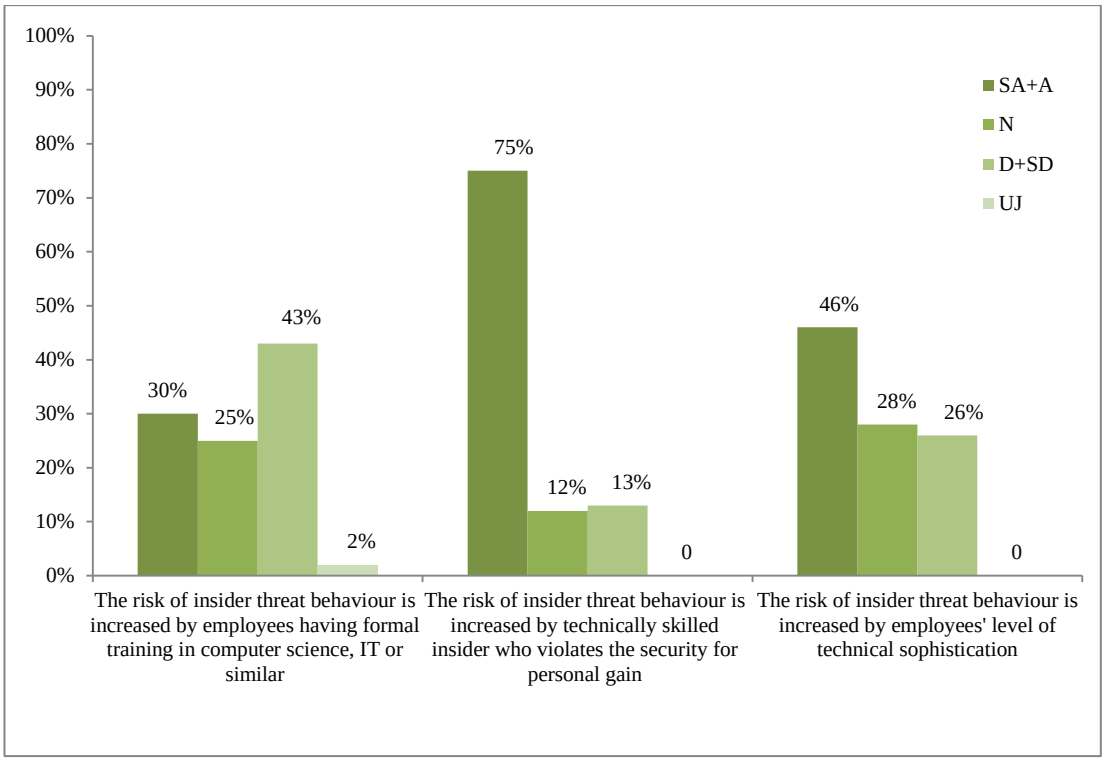


Figure 5.12: IT skills

In the last part, the researcher included three questions to evaluate the technical skill factor. As can be seen in Figure 5.12, although 30% (6% (SA) + 24% (A)) of participants agreed that employees having formal training in computer science, IT or similar skills increased the insider threat behaviour, 43% (32% (D) + 11% (SD)) of them disagreed. Twenty-five per cent were neutral (N) and neither agreed nor disagreed with the statement. Two participants were unable to judge.

On the other hand, the majority of participants (75% - 29% (SA) + 46% (A)) agreed that a technically skilled insider who violates the security for personal gain is increasing the insider threat, while only13% (9% (D) + 4% (SD)) of the participants disagreed. A total of 12% of the participants were neutral (N).

Similarly, 46% (7% (SA) + 39% (A)) of the participants agreed that employees' level of technical sophistication increased the risk of insider threat behaviour. Twenty-six per cent (23% (D) + 3% (SD)) of the participants disagreed, and 28% of the participants were neutral (N).

The results above indicate that employees' technical skill cannot be considered a significant factor contributing to insider threat behaviour, since the responses regarding this factor were varied. Despite the fact that the percentage in Figure 5.12 shows that most of the participants agreed with the second statement (technically skilled insider who violates the security for personal gain is increasing the insider threat), about half of them disagreed with the first statement (employees having formal training in computer science, IT or similar skills could increase the insider threat behaviour). On the other hand, Table 5.14 indicates that the mean for the first statement is neutral. Alternatively, participants' comments confirmed the opinion of a Senior IT Security Consultant who stated *"Most insiders planned for the attack well in advance, by using some of their technical skills and techniques like meaningful errors and preparatory behaviour".* Therefore, the researcher concludes that another analysis method is essential in order to identify whether or not employees' technical skills contribute to insider threat.

5.4 The Need for Factor Analysis

As discussed previously in Chapter Two, the factors that emerged from a review of three different sources (academic sources, IT industry publications and published reported incidents) were not equally supported by all the sources. That is, some sources have highlighted some factors while other sources have supported others. This shows a significant contribution of this study, since the three sources provided competing models that reflect differences and disagreements. This study has taken into consideration all the factors that have been addressed by all three sources in order to yield the candidate list of factors that present a holistic approach. The researcher tested the candidate HIT model through the preliminary analysis of the survey.

The preliminary analysis has revealed that there is a further debate regarding the factors because the analysis did not present an unequivocal list of factors that contribute to the threat. While there is a strong support for some factors such as

information security policies, support for other factors varies (such as outsourcing, remote access and cultural factors). Moreover, the correlation matrix (see Appendix 2) indicates that there is a strong correlation not only between each group of verbals for each factor but also between different groups. Although, the preliminary analysis shows that there are correlations between verbals for some factors, there are many correlations for the verbals across other factors. The preliminary analysis result did not definitely identify the underlying factors; therefore the presented factors required further analysis.

All the above illustrated that the candidate factors are inconsistent, which may be because many of the suggested factors may be circumstantial rather than actually contributing to insider threats. For example, remote access does not contribute insider threat because all organisations grant remote access. However, remote access may be a tool that makes it easier for an insider to carry out a threat, the fact that he is influenced by other factors together with the remote access may constitute a stronger threat. Moreover, motivation alone as a factor will not be enough to commence a threat. An insider must have other facilitating factors along with his motivation in order to pose threat. Similarly, outsourcing does not necessarily indicate insider threat.

Due to the competing models provided by the three different sources, and the results of the primary analysis, the need for another analysis is indicated. The factor analysis will show the relevance between factors and will present a distinct set of factors. The factor analysis will present a different, improved list of factors which will reflect a consistent interpretation of the data, unlike the original grouping.

5.5 Factor Analysis

Factor analysis provides another perspective of the survey results. Factor analyses is a data reduction technique, the general purpose of which is to reduce the variables to a smaller set of new factors (Hair et al. 2010). According to Hair et al. (2010), factor

analysis can perform data reduction by either identifying representative variables from a larger set of variables or generating a totally new set of factors smaller in number that partially or completely replace the original set of factors.

5.5.1 Steps involved in Factor Analysis

According to Pallant (2011, 182 & 183), there are three main steps in conducting factor analysis:

5.5.1.1 Step 1: Assessment of the Suitability of the Data for Factor Analysis

Two main issues should be considered when deciding whether or not factor analysis is suitable for this study: sample size and sample sufficiency.

- **Sample size**

Although many researchers recommend large sample sizes, some researchers consider that a smaller sample size such as 150 or less should be sufficient if the factor loading is high (Pallant 2011). Hair et al. (2010) suggest that a sample of 100 participants requires a factor loading of .55 and above to be significant. Therefore, in this study, only a .55 and above factor loading was used. Table 5.15 presents the guideline for identifying significant factor loading according to Hair et al. (2010, 128).

Table 5.15: Guideline for identifying significant factor loadings based on sample size.

Factor Loading	The sample size needed for significance
.30	350
.35	250
.40	200
.45	150
.50	120
.55	100
.60	85
.65	70
.70	60
.75	50

- **Sample sufficiency test and sphericity test**

The second issue to be addressed is the sufficiency of the sample. SPSS provides two tests to determine whether factor analysis is suitable for the data: Bartlett's test of sphericity (Bartlett 1954), and the Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy (Kaiser 1974). Bartlett's test of sphericity should be significant (p = .05 or smaller) (Pallant 2011, 183). An acceptable result for Bartlett's Test of Sphericity is when *"the correlation matrix has significant correlations among at least some of the variables"* (Hair et al. 2010, p. 104). For the KMO test, a score of .70 is considered acceptable, while .80 or greater is excellent (Hair et al. 2010).

The following Table 5.16 gives information about the two sample sufficiency tests for factor analysis. Table 5.16 indicates that the minimum standards have been met or exceeded; the KMO value is .874 which is above .7, and Bartlett's test is significant p = .000. Therefore, factor analysis is appropriate for this study.

Table 5.16: KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.808
Bartlett's Test of Sphericity	Approx. Chi-Square	1195.412
	df	351
	Sig.	.000

5.5.1.2 Step 2: Factor Extraction

Factor extraction *"involves determining the smallest number of factors that can be used to best represent the interrelationships among the set of variables"*(Pallant 2011, 184).

There are a number of techniques for determining the number of factors to retain (Hair et al. 2010; Pallant 2011):

- Kaiser's criterion is a widely-used technique, also known as the eigenvalue rule. Using this rule, only factors with an eigenvalue greater than 1.0 are retained.
- A number of factors are determined by the researcher according to research objectives or prior research.
- The scree test technique involves retaining all factors above the inflection point at which the direction of the curve changes dramatically and becomes horizontal (elbow), as these factors explain most of the variance in the data set.
- Sufficient factors to meet a specified percentage of variance explained, more often 60% or greater.

In order to determine how many factors to extract in this study, the researcher tried all previous techniques. However, Kaiser's criterion was the most appropriate method. The researcher began by determining the number of factors according to the earlier number of factors. Furthermore, the scree test technique has been utilised to

help the researcher to find an accurate and meaningful list of factors. However, neither these techniques was of great assistance to the researcher in identifying the appropriate number of factors.

The graph in Figure 5.13 shows a change (or elbow) in the shape after the second factor; there is an obvious break between the second and third components which means that components 1 and 2 describe the variance much more than the other components. However, these two components do not meet a specified percentage of variance which is often 60% or greater. Therefore, the researcher decided to extract eight factors according to Kaiser's criterion technique.

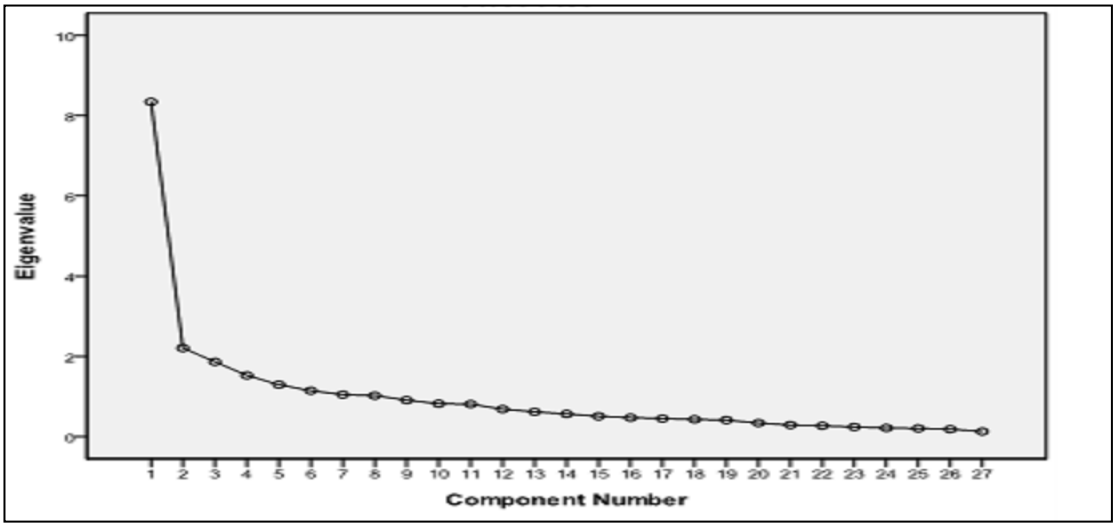


Figure 5.13: Scree Plot

Finally, Kaiser's criterion was utilised, and only the components with eigenvalue of 1 or above were extracted. The Total Variance Explained table below was used to determine how many components meet this principle. The first set of columns, labelled Initial Eigenvalues, was checked to find out the components with an eigenvalue of 1 or greater. Eight components recorded eigenvalues above 1 (8.346, 2.209, 1.863, 1.527, 1.296, 1.144, 1.047, and 1.021). These eight components explain a total of 68.345% variance (Table 5.17).

Table 5.17: Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	8.346	30.910	30.910	8.346	30.910	30.910	3.274	12.125	12.125
2	2.209	8.180	39.090	2.209	8.180	39.090	2.701	10.003	22.128
3	1.863	6.902	45.992	1.863	6.902	45.992	2.314	8.571	30.699
4	1.527	5.656	51.647	1.527	5.656	51.647	2.196	8.134	38.833
5	1.296	4.801	56.448	1.296	4.801	56.448	2.165	8.019	46.851
6	1.144	4.236	60.684	1.144	4.236	60.684	2.031	7.521	54.373
7	1.047	3.879	64.563	1.047	3.879	64.563	1.961	7.262	61.635
8	1.021	3.781	68.345	1.021	3.781	68.345	1.812	6.710	68.345
9	.909	3.366	71.711						
10	.821	3.041	74.752						
11	.810	3.001	77.753						
12	.685	2.537	80.290						
13	.617	2.286	82.576						
14	.566	2.095	84.671						
15	.505	1.871	86.542						
16	.473	1.753	88.295						
17	.449	1.664	89.958						
18	.430	1.594	91.553						
19	.411	1.524	93.077						
20	.339	1.254	94.331						
21	.288	1.066	95.397						
22	.270	1.001	96.398						
23	.240	.890	97.287						
24	.215	.795	98.083						
25	.205	.759	98.842						
26	.185	.685	99.526						
27	.128	.474	100.000						

5.5.1.3 Step 3: Factor Rotation and Interpretation

Once the number of factors has been determined, rotation is the next step in order to assist with the researcher's interpretation. The general purpose of the rotation method is to obtain simpler and theoretically more meaningful factor solutions. In many cases, the rotation of the factors improves the interpretation by reducing some of the

ambiguities that often accompany initial un-rotated factor solutions (Hair et al. 2010). The Varimax method was used to rotate the data in this study. The Varimax technique is a widely-used orthogonal approach which attempts to minimise the number of variables by keeping the high loading variables for each factor (Pallant 2011; Alhija 2010). After using the Varimax method, the researcher examined the rotated component matrix and started the interpretation with the first variable on the first component and moved horizontally from left to right looking for the highest loading value (positive or negative) for that variable on any component. Similarly, this was done with the second variable, again looking for the highest loading for that variable on any component, moving from left to right. This process was repeated for all other variables until all variables had been reviewed for their highest loading on a component. In this study, the minimum highest value was .55 according to Hair et al. (2010)'s suggestion. For easier interpretation, in options the researcher typed .55 in the Absolute value below section and in Coefficient Display Format section, the researcher clicked on Sort by size and Suppress small coefficients. See Table 5.18. It should be noted that in the following table, loadings below .55 have been excluded for ease of interpretation.

Table 5.18: Rotated Component Matrix

	Component							
	1	2	3	4	5	6	7	8
Cultural clash between employees and the organisation	.719							
Organisational culture that tolerates unethical behaviour	.618							
Insiders being unduly motivated by financial gain	.614							
Insiders' knowledge of the potential value of the organisation's information	.612							
Technically skilled insiders who violate the security for personal gain.	.551							
The implementation of inappropriate information security policy.		.787						
Out-dated information security procedures or policies.		.643						
Insufficient information security policy training and awareness.		.556						
Inappropriate or concerning behaviour prior to the incident such as delays, absences and poor job performance			.813					
High levels of trust given to employees.			.688					
Employees from backgrounds where acceptable practices differ.				.841				
Insiders being vulnerable to coercion by outsider.				.574				
Allowing authorised mobile device to access organisational information from outside the organisation physical boundary.					.776			
High levels of access to IT systems given to employees.					.609			
Giving employees remote access to organisational information.						.739		
Granting access to third- parties contracted to conduct work within the organisation.						.617		
Insiders' knowledge of the methods used to detect insider threat behaviour.							.751	
Employees' level of technical sophistication.							.55	
Employees working from home.								.749
Psychological factors such as social frustrations or computer dependency.								.589

Once the variables of each component had a significant loading, the researcher assigned a suitable name to each component. According to Hair et al. (2010), the names selected to represent a factor will be significantly influenced by variables with a higher loading. Therefore, the researcher carefully examined and studied all significant variables for each factor, emphasising variables with a higher loading in order to name a factor accurately reflecting the variables loading on that factor. Table 15.19 summarizes the improved extracted factors including the name, eigenvalues, description and variables for each factor.

Table 5.19: Interpretation of the improved insider threat contributing factors

Factor Name	Eigenvalues	Description	Variables	Loading	Original factors from the candidate HIT model
Conflict between the organisation and an individual who is willing and able to seek personal gain at the organisation's expense	8.346	Factor one represents 30.910 percent of the total variance in initial eigenvalues and 12.125 of the total variance after rotation. There are five variables in this factor. The first variable focused mainly on the conflict between the organisation and its employees as a result of the cultural clash. Similarly, the second variable also reflected some sort of conflict. If the organisation culture tolerates unethical behaviour, this will significantly affect the employees' behaviour, which at the end could lead to conflict between the organisation and employee. The third variable reflects the motivation for the individual, while the remaining two variables reveal the ability of the individual to commit the threat. This circumstances affect the name of factor one; thus, this factor called "conflict between the organisation and an individual who is willing and able to seek personal gain at the organisation's expense".	Cultural clash between employees and the organisation	.719	Cultural factors
			Organisational culture that tolerates unethical behaviour.	.618	
			Insiders being unduly motivated by financial gain.	.614	Motivation
			Insiders' knowledge of the potential value of the organisation's information.	.612	Insider's knowledge
			Technically skilled insiders who violate the security for personal gain.	.551	Technical skills

Factor Name	Eigenvalues	Description	Variables	Loading	Original factors from the candidate HIT model
Insufficient security policy	2.209	Factor two consisted of three variables. Although it represents 8.180 percent of the total variance in initial eigenvalues, it represents 10.003 percent of the total variance after rotation. The three variables constituted the insufficient security policy factor. This is because the first and second variables focused mainly on security policies, in term of implementation and updating. In addition, the third variable focused on policy training and awareness. Therefore, inadequate security policy was the common theme among the variables in factor two.	The implementation of inappropriate information security policy.	.787	Information security policy
			Out-dated information security procedures or policies.	.643	
			Insufficient information security policy training and awareness.	.556	

Factor Name	Eigenvalues	Description	Variables	Loading	Original factors from the candidate HIT model
Giving high trust to underachieving employees	1.863	Factor three included two variables with 6.902 percent of the total variance in initial eigenvalues and 8.571 percent of the total variance after rotation. In factor three, the first variable reflects the characteristics of the underachieving employee. While, the second highest loading variable focused on the high levels of trust. Low performance employees with high level of trust will increase the risk of insider threat.	Inappropriate or concerning behaviour prior to the incident such as delays, absences and poor job performance.	.813	Individual characteristics
			High levels of trust given to employees.	.688	Access and level of trust

Factor Name	Eigenvalues	Description	Variables	Loading	Original factors from the candidate HIT model
Outside influence on the employees	1.527	Factor four represents 5.656 percent of the total variance in initial eigenvalues. On the other hand, it represents 8.134 of the total variance after rotation. First variable addressed the background of the employees. Sometimes the background and where the individual comes from could influence their behaviour. Hence, the background of the employees is considered as an outside factor that influences their behaviour towards the work or the organisation. Second variable in factor four also considered as an outside factor, since the coercion by outsiders on the employees could influence them to behave in an appropriate way. Outsider's coercion could be through commercial pressure or blackmailing insider employee to perform the attack. Therefore, the influence of the outside attributes on the employees was the common theme among the above variables.	Employees from backgrounds where acceptable practices differ.	.841	Cultural factors
			Insiders being vulnerable to coercion by outsider.	.574	Motivation

Factor Name	Eigenvalues	Description	Variables	Loading	Original factors from the candidate HIT model
Liberal access	1.296	Even though factor five represents 4.801 percent of the total variance in initial eigenvalues, it represents 8.019 percent of the total variance after rotation. Both variables in factor five focused on unnecessary access or more access given to the employees than what they actually need to perform their job, either by allowing mobile device to access the organisation's network remotely or by giving employees a high level of access that is more than required.	Allowing authorized mobile device to access organisational information from outside the organisation's physical boundary.	.776	Remote access
			High levels of access to IT systems given to employees.	.609	Access and level of trust

Factor Name	Eigenvalues	Description	Variables	Loading	Original factors from the candidate HIT model
Loyalty of employees	1.144	Factor six created from two variables, describes 4.236 percent of the total variance in initial eigenvalues and 7.521 percent of the total variance after rotation. Both variables within this factor focused on loyalty of employees towered an organisation. Outsourcing and remote access of organisation's information affect the loyalty of employees simply because "Home is where the heart is". Although it is true that the employees work for an outsourced company, their loyalty to their original company may still remain. Moreover, accessing the organisation's data remotely may reduce the loyalty of the employees since they are outside the workplace environment which assists them to abuse the organisation whether intentionally or not.	Giving employees remote access to organisational information.	.739	Remote access
			Granting access to third-parties contracted to conduct work within the organisation.	.617	Outsourcing

Factor Name	Eigenvalues	Description	Variables	Loading	Original factors from the candidate HIT model
The perfect crime	1.047	Factor seven represents 3.879 percent of the total variance in initial eigenvalues, and represents 7.262 of the total variance after rotation. Variables in factor seven are considered as essential attributes to commit a perfect crime. The first variable describes the knowledge of the insiders, especially their awareness about the methods used to detect insider threat behaviour. While, the second variable relates to the insiders' level of technical skills which help them to carry out the attack. Both variables allow the insiders to avoid being detected when they launch an attack.	Insiders' knowledge of the methods used to detect insider threat behaviour.	.751	Insiders' knowledge
			Employees' level of technical sophistication.	.55	Technical skills
Socially isolated employees	1.021	Factor eight included two variables with 3.781 percent of the total variance in initial eigenvalues and 6.710 percent of the total variance after rotation. In factor eight, the common theme among the variables is social isolation. For instance, employee may prefer to work from their homes or any isolated areas. Such constant behaviour may indicate signs of depression, leading to social frustration. In such cases, social isolation could lead to serious inappropriate behaviour.	Employees working from home.	.749	Remote access
			Psychological factors such as social frustrations or computer dependency.	.589	Individual characteristics

5.5.2 Reliability

The Cronbach alpha was obtained for the eight improved factors after factor analysis. The Cronbach alpha of the data ranged from 0.70 to 0.90. The highest was 0.90 indicating conflicts between the organisation and an individual who is willing and able to seek personal gain at the organisation's expense, while the lowest internal consistency was 0.70 for the perfect crime. The high internal consistency values for all the constructs confirm the reliability of the measurement model. The results of the reliability test are presented in Table 5.20.

Table 5.20: Cronbach's alpha

Factors	Alpha Reliability
Conflict between the organisation and an individual who is willing and able to seek personal gain at the organisation's expense	0.90
Inadequate security policy	0.83
Giving high trust to underachieving employee	0.80
Outside influence on employees	0.89
Liberal access	0.76
Loyalty of employees	0.86
The perfect crime	0.70
Socially isolated employees	0.78

The sample consisted of 100 security specialists.

5.6 Enhanced HIT Model and the Improved Factors

As discussed in section 5.4, due to the mixed results from the primary analysis of each factor, the researcher decided to conduct factor analysis. Factor analysis helped the researcher to organise the variables in order to extract an improved list of factors which reflected a more consistent interpretation of the data than the original grouping. Moreover, factor analysis showed the relationship between factors and presented a crystal clear set of factors. The outcome of the factor analysis is a list of

improved factors that contribute to insider threat behaviour. The variables were grouped into eight factors, all of which together form the enhanced HIT model (see table 5.19). Figure 5.14 presents the enhanced HIT model.

The improved factors extracted using the factor analysis method are listed below:

- ***Conflict between the organisation and an individual who is willing and able to seek personal gain at the organisation's expense***

Conflict can be defined as *"the disagreement between at least two persons or groups on specific issues, or it is a process in which one party perceives that its interests are being opposed or negatively affected by another party"* (Nouman, Khan, and Khan 2011, 618). A study found that a majority of employees (85%) experience conflict with their organisation and about 27%of these conflicts transform into personal attacks, and 25% of the avoidance of conflict resulted in sickness or absence from work (Hayes 2008).

Conflict in organisations occurs for numerous reasons; usually, it is the outcome of a culture clash between employees, different personalities and the organisation's culture. According to Nouman, Khan, and Khan (2011), the most common causes of the conflicts arising between organisations and individuals are a lack of communication, misperception, difference in opinions, and discrimination. Moreover, a workplace conflict could also be affected by personality clashes, stress, high workloads and culture clash (Weinhold and Weinhold 2004; Hayes 2008; Sarala 2010). This workplace conflict may lead to revenge, as stated by CERT (2006), since more than half of the insider attacks were launched as a result of dissatisfaction of employees, and most of them acted out of revenge related to some conflict or negative event with the organisation. This could include, for example, disputes with the employer, clashes with supervisors and co-workers, new supervisors, high workloads, transfers or demotions and dissatisfaction with salary increases or bonuses. A conflict with a supervisor may cause an employee to become an insider threat. For example, an employee attempted to pass his organisation's trade secrets to its competitors because he was furious with his manager. Another

employee was concerned over company practices and decided to send an e-mail to 180,000 employees detailing his frustration with his organisation's health record system. This e-mail uncovered secret projections of the organisation's future outcomes which resulted inthis employee being fired (Kirkpatrick 2008).

Culture and personality clashes increase the likelihood of conflict as employees often see a clash of values as a significant cause of conflict (Weinhold and Weinhold 2004; Hayes 2008). Acceptable traditions for doing business differ according to region and area. According to these various regional circumstances, the pressure of external sources on insiders could be easier to apply, either directly or indirectly, through sophisticated methods such as social engineering (Colwill 2009). Royds (2009) stated that most of the data losses reported by the government of the UK show that only 5% occur because of technology issues, while 95% occur as a result of cultural factors or people's behaviour.

Furthermore, organisational cultures can also contribute to the conflict; if the conflict is ignored or managed poorly by the organisation's culture, this exposes the organisation to higher levels of accidents, lowered productivity, and depression and dissatisfaction of employees, which simply leads to inappropriate behaviour (Bond 2004; Casali and Day 2010). Organisations should define appropriate and inappropriate behaviour in the workplace. If organisational culture tolerates unethical behaviour, there is a high probability that conflicts will occur (Bond 2004; Casali and Day 2010). Organisational culture is defined as *"the shared values, norms and expectations that direct the way people approach their work and interact with each other"* (Colwill 2009, 5). Another definition stated that "*as the system that penetrate values, belief and norms in each organization. Organisational culture able encourage and discourage the effectiveness depend on the value characteristic, belief, and norms"(Syauta et al. 2012, 70).* Good organisational culture usually aligns the values of the organisation with those of its employees. On the other hand, poor organisational culture expresses values and behaviours different from the shared values of employees and the adopted organisational values (Casali and Day 2010; Vosloban 2012). According to Royds (2009), most of the data losses reported

by the government of the UK show that only 5% occur because of technology issues, while 95% occur as a result of cultural factors or people's behaviour. The culture of an organisation can influence the behaviour of employees and eventually contributes to the effectiveness of an organisation. The conflict will worsen if the insiders are unduly motivated by financial gain and they may use their knowledge and technical skills to violate the security for personal gain.

- ***Insufficient security policy***

An inadequate security policy can be described as an overall inadequate level of protection against insider threat. The implementation of inappropriate information security policy, out dated security policy and lack of training and awareness are considered to be essential aspects that can affect the insider threats (Pramanik, Sankaranarayanan, and Upadhyaya 2004). Implementing a suitable information security policy, making it up-to-date and providing appropriate training and awareness are vital tasks which require more than just writing a security manual. Each organisation needs to know who has access to the data, what their own access policies are, and what actions they take to access data. Clear and updated security policies as well as training and awareness are considered very essential to all organisations to protect their assets from misuse (CERT 2006).

The implementation of insufficient information security policies and procedures could significantly increase the insider threat. According to Randazzo et al. (2004), in 70% of the cases, insiders had broken through systemic vulnerabilities in processes, procedures and policies to carry out their attacks. Meanwhile, Kowalski et al. (2008) claim that in half of the incidents they examined the insiders exploited the vulnerabilities in established business processes or controls, such as insufficiently enforced policies for separation of duties. Organisations need to implement suitable security policies and all employees should follow the security policy to minimise the risk and to respond to any security incidents effectively. Moreover, an out-dated security policy can expose organisations to serious risk (Canavan 2007; Karyda, Kiountouzis, and Kokolakis 2005). Security policies should be updated based on organisational changes, in for example, the case of organisations merging or any

other changes in the structure of the organisation. In both situations, security policies should be updated because of the change (Zafar 2013).

Moreover, training and awareness is an important process that should be undertaken in order to minimise the insider threat. According to Furnell (2006), the problems faced by organisations from internal threats are being reported along with matching evidence of insufficient security training and awareness. Security training and awareness is one of the areas on which an organisation must focus and apply so as to reduce the insider threats (Crossler et al. 2013). Awareness among all levels of employees is vital to the successful performance of any organisation's information security policy (Albrechtsen and Hovden 2010).

- ***Giving high trust to underachieving employees***

This factor generally focused on the high level of trust which is given by the organisation to their underachieving employees. An underachiever is an employee who is working much less than their potential and who exhibits inappropriate or concerning behaviour. Underachievers are the employees who do not regularly apply effort to their work and are working far below the organisation's expectations. Employees' performance and productivity are very important to an organisation's success. Employees who are not using their abilities, skills, time and resources effectively are costing the company money (Joseph 2009).

Performance is *"work results that achieved by someone or group in organization, suitable with the authority and responsibility, in effort to reach the Organisational goals legally, not violate the law, and suitable with moral and ethics."(Syauta et al. 2012, 71).* Employee performance is *"work outcome in quality and quantity that achieved by someone in conducting his responsibility"(Syauta et al. 2012, 71).*

The performance of organisations' employees can be influenced by several factors. For example, role ambiguity and role conflict can negatively affect an employee's performance and impede his/her normal work (Zou 2011). According to Vosloban (2012), personal motivation is considered one of the key factors that influences the

level of employees' performance. This includes employees' level of commitment to completing tasks, their abilities, their communication skills, and their attitude. Additionally, the employees' performance is influenced by other factors such as workplace environment, tasks clarity, rewards, opportunities and frequency the relationship with colleagues. The workplace environment plays a significant role in motivating employees to perform their assigned tasks efficiently. Financial reward alone is not a sufficient motivator in encouraging the high performance required within the organisations (Chandrasekar 2011).

Moreover, Syauta et al. (2012) and Md Zabid Abdul, Sambasivan, and Johari (2003) confirmed that organisational commitment influences employee performance: the higher the organisational commitment, the higher the employee performance. Organisational commitment is the *"degree to which an employee believes in and accepts Organisational goals and desire to remain with the organization"(Syauta et al. 2012, 70).*

Vosloban (2012) consider that employees' performance management is an essential aspect of the organisation's productivity. Organisations' managers should be responsible for developing high performance in their employees. *"The performance management is a systematic process of the workload planning and expectations setting, of the continuous performance monitorization, development of the performing capacity, periodically performance evaluation and high performance recompensation*"(Vosloban 2012, 661). Organisations should ensure that they offer their employees the necessary knowledge required to carry out their jobs in order to achieve the desired performance (Vosloban 2012; Joseph 2009).

Noticeable concerning behaviours were shown by the employees in the insider threat cases including decline in performance, delays, or unexplained absenteeism (CERT 2009). Organisations should be aware of their employees' performance, especially if these employees have been given a high level of trust.

- ***Outside influence on employees***

All external surroundings that may affect employee behaviour are considered the outside factors. The influence of the external environment could include many factors such as employees' background, values, economic motivator and employee coercion by outsiders (Mathur and Gupta 2012). These factors sometimes can negatively direct the insiders' behaviour against their organisation. While organisations' internal environment can be controlled and managed, the individual external environment is outside the control of organisations (Mathur and Gupta 2012).

Sometimes, individuals' backgrounds are considered to be an external factor affecting the employees' behaviour toward their organisation. Mathur and Gupta (2012) stated that:

> *"It is a common belief that people who are brought up with lot of parental care, concern, love and affection exhibit good demeanour with respect and high regard to everyone. Since they are brought up in a protected environment, in turn offer the same to their peers and subordinates. Conversely, people coming from broken families with chequered childhood are much unsecured, suspicious, and less jovial and lack sound decision making skills."*

This clarifies why personal family background is a very important factor affecting employee behaviour. The different backgrounds of employees may have different professional implications (Mathur and Gupta 2012). Similarly, attitudes and propensities towards crime and acceptable practices for doing business differ significantly according to employees' backgrounds and regions. As stated by Colwill (2009, 191) "*Practices that are considered illegal in the Western world, for instance the giving of substantial gifts (namely bribes), may be a common and accepted practice in some regions where the wheels of business need to be oiled"*.

Moreover, employees' concerns include issues of life that are often beyond their control and that can affect their behaviour and attitude toward the organisation.

These concerns include family, health and financial problems (Mathur and Gupta 2012). Sometimes, an outside influence can be exerted on an employee through coercion by an external entity to force them to launch the attack; this coercion could take the form of commercial pressure or blackmail. Likewise, critically problematic financial situations such as struggling to make ends meet, and large credit card debts, make the insider greedy for money. In these cases, insiders are motivated mainly by the desire for financial gain. Employees could steal information to sell it, or be paid by outsiders to modify data or modify information to obtain financial benefits. Some employees were motivated to provide additional income for their relatives, partner or friends (Willison and Warkentin 2013).

- ***Liberal access***

Liberal access can be defined as unnecessary access or more access given to the employees than what they actually need to perform their job. This may occur when an organisation offers increased access facilities in several ways by, for example, allowing mobile devices to access the organisation's network remotely or by giving employees a high level of access to IT systems.

A high level of more than needed access can lead to insider threat (Willison and Warkentin 2013). Many organisations offer their employees more access than what they essentially need to perform their job (Cole and Ring 2005). Misuse of access is one of the most difficult types of attack to detect and prevent, since the insider uses his or her authorised access rights to perform illegal tasks (Bellovin 2008).

Moreover, mobile devices with remote access to organisation networks increase the risk of insider threat as stated by Aldhizer and Bowles (2011, 59) *"The proliferation of powerful conventional mobile devices … with remote access to internal networks has raised significant new security concerns.".* Although the use of mobile devices such as smartphone or PDA device and enabling employees to work remotely facilitate the mobility, it can lead to data loss or theft through the physical loss of the device or leakage of data outside the network. (Steele and Wargo 2007, 25). Employees may access or load sensitive data on their mobile devices remotely

thereby exposing the data to risk, since the data on mobile devices is usually not encrypted or backed up. According to Sarkar (2010, 120),*"any device like a laptop, a PDA or a mobile that accesses a corporate network or store data is a potential risk to intellectual property or sensitive customer data. These portable devices are a great source of data leakage"*. The increased number of powerful mobile devices with remote access to internal networks has raised significant new security concerns (Aldhizer and Bowles 2011).

- ***Loyalty of employees***

The absence of employee loyalty can negatively affect the employees' work efficiency and the organisation's security (Bridges and Harrison 2003). Employee disloyalty could increase the possibility for an internal organisational clashes and problems. According to Schrag (2001), employee disloyalty weakens organisational productivity and security. Many organisations are concerned about their employees' loyalty. Employee disloyalty can be manifested in different ways such as a deliberate failure to perform tasks, accepting benefits that belong to the organisation, dishonesty and theft. Former employees' disloyalty also can affect the organisation as they can take with them confidential information and proprietary products.

Furthermore, outsourcing and remote access may influence employee loyalty (Bridges and Harrison 2003). An outsourced employee may be less loyal to the organisation: *"The growing culture of open and interconnected world combined with transfer of jobs overseas, downsizing, outsourcing, and increased hiring of part-time workers to avoid paying benefits are shaping the employees' sense of job security and loyalty to employer"*(Sarkar 2010, 115). A single outsourcing contract can change the position of several 'outsiders' to 'insiders' and may blur the difference between an organisation's employees and members of the third party. Outsourcing could increase the organisation's vulnerability to loss of intellectual property and the possibility of transferring a high value or high impact knowledge to a competitor or other external sources (Colwill 2009; Whitworth 2005). Organisations are increasingly outsourcing critical business functions. Consequently, external individuals could have full access to an organisation's policies, information and

systems, while access had been previously granted only to organisation's employees. Organisations should be aware that if they dealing with outsourced employees, then insiders are no longer just the employees within their four walls. Organisations should ensure that the outsourced employees are managed carefully, allowing them access only to information they need to fulfil their contractual obligations and terminating their access when it is no longer needed.

In addition, remote access provides a good opportunity for insiders to attack with less risk. It is easier to attack the organisation remotely, since the insider is outside the boundaries of the organisation and no-one can witness hem. **A**ccessing the organisation's data remotely can lead to a decrease in the loyalty of the workers since they are not in the workplace environment (Sarkar 2010). This will give them the chance to abuse the organisation whether intentionally or not. According to CERT (2009), most insiders used remote access outside the work place to carry out their attack.

- ***The perfect crime***

"Think I can avoid being detected" refers to the employees' confidence that they will not be revealed by the organisation. Employees could use their knowledge ability and technical skills against their organisation. According to Padayachee (2012, 673), *"The insider threat is even more dangerous than external threats, as an insider may easily misuse the skills and knowledge gained through legitimate work duties for illegitimate gain".* The insiders' knowledge, especially their awareness about the methods used to detect insider threat behaviour, and insiders' level of technical skills both can facilitate the insider attack. Some researchers refer to an insider as *"anyone who has intimate knowledge of internal operations and processes"(Steele and Wargo 2007, 20).* In addition to their free access to documents and data, insiders have a broad knowledge of their organisation's system and procedures (Wood 2000). Employees commonly have a great knowledge about their organisation; they are usually familiar with some or all internal process of their target systems (Dallaway 2008). Furthermore, the most serious threat situation to the organisation's system and networks is the technically skilled insider who violates security policies for personal gain. Employees sometimes use their technical skills to harm an organisation'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 they are familiar with which may increase their opportunity to compromise these systems. The level of employee sophistication is considered as a potential factor which can influence their ability to perform insider misuse. According to Padayachee (2012, 673), *"The insider threat is even more dangerous than external threats, as an insider may easily misuse the skills and knowledge gained through legitimate work duties for illegitimate gain".* Thus, insiders' knowledge and skills are considered essential for committing a perfect crime.

- ***Socially isolated employees***

This relates to the character or personality of the employee. Sometimes socially isolated employees prefer to work from home or in isolated work areas. Some employees prefer to be socially isolated when working, indicated by their preference for working from their homes or in isolated areas. If this behaviour is consistent, it may be an indication of depression, leading to social frustration. In such cases, this could lead to serious, inappropriate behaviour (Colwill 2009). According to Gely and Bierman (2006, 299) *"Employees need to be able to communicate with each other for workplace social engagement to flourish".*

Working from home or any isolated areas can lead to insider threat. According to CERT (2009), insiders have acknowledged that it is easier to conduct malicious actions from home because it reduces the concern that anyone in the office could be observing the malicious behaviour or actions. Furthermore, social frustrations may include childhood abuse and neglect. Such individuals tend to exhibit anger, isolation from the community, poorer social skills and a desire to "strike out at the system" (Steele and Wargo 2007). Lack of social skills and a tendency to social isolation increase the probability of inappropriate behaviour, since if these individuals face any difficulties, they will not address these in a positive manner (Shaw 2006). Often if the insiders are loners with low social skills, they feel a general antagonism towards management and a tendency to infringe the organisation's policies. Socially

isolated employees are usually poor team players, whose primary interests are: exploring networks, breaking into secure systems, cracking code, and challenging and outfoxing security professionals (Sarkar 2010).

The enhanced HIT model presented in Figure 5.14 will be utilized in the preparation of the interview method in Chapter Six. The qualitative phase of the study will validate the factors in the enhanced HIT model. The outcome from the interviews is the final HIT model with the factors that influence the insider threat behaviour. Thus, an enhanced HIT model is the foundation for the qualitative phase of this study.

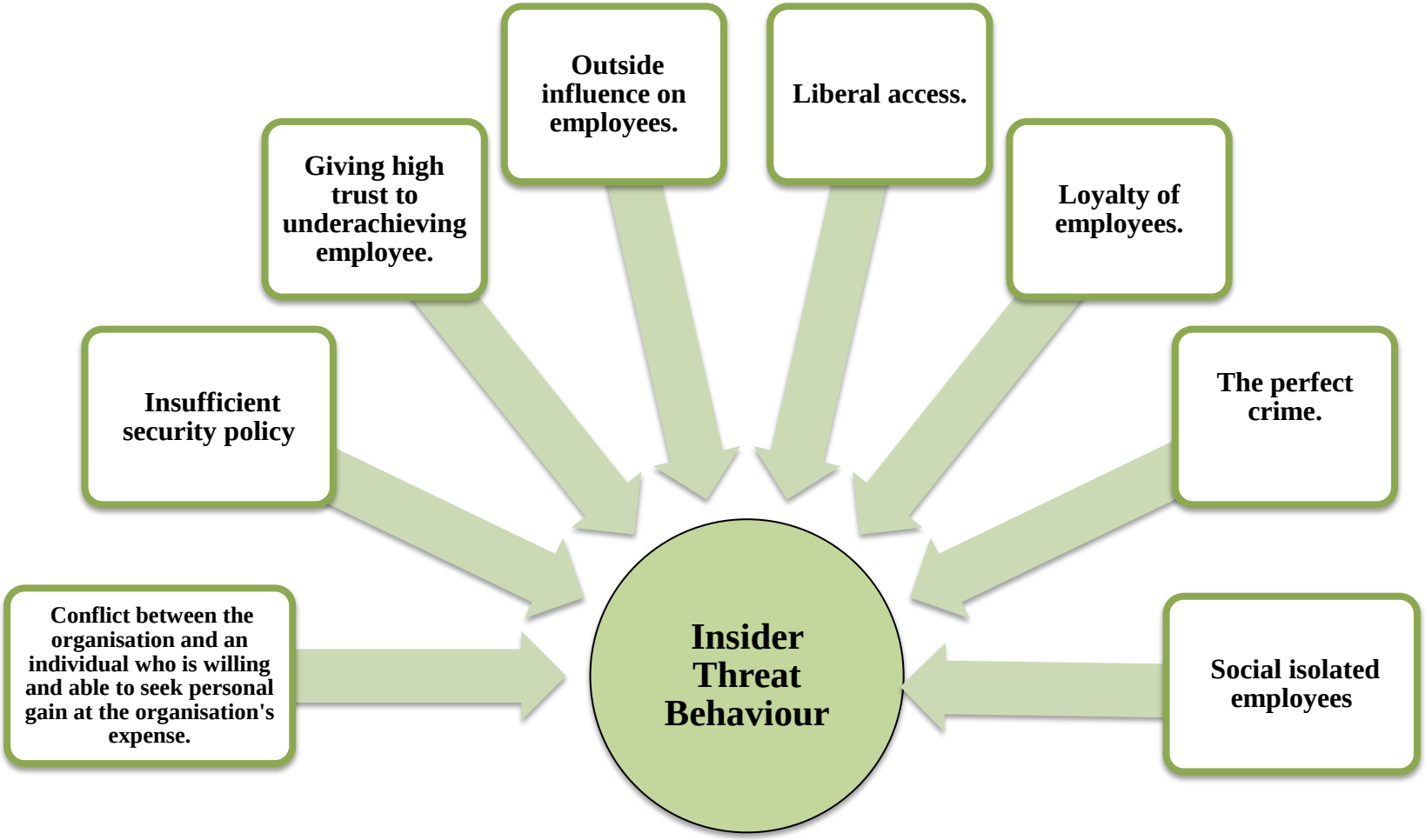


Figure 5.14: Enhanced HIT model

5.7 Summary

This chapter provided a general overview of the first evaluation of the candidate HIT model. The focus of the quantitative phase was on validating the factors identified in the academic sources, IT industry publications and published reported incidents. Furthermore, the intention was to discover an improved set of factors that could further enhance the candidate HIT model. In this chapter, the researcher discussed the survey design, targeted population, a Web-based survey and finally the data analysis. The researcher surveyed 100 security specialists with the following job titles: IT Security Manager, Principal Cyber Security Manager, Security Systems Administrator and Senior IT Security. The data was collected through a Web-based survey and analysed by SPSS.

The preliminary analysis did not present a robust list of factors contributing to the insider threat. While there is strong support for some factors (such as information security policies), support for other factors (such as outsourcing and remote access) was mixed. Results of the preliminary analysis indicate that the presented factors required further analysis. The factor analysis technique was utilized to identify groups of inter-related factors to produce a new set of robust factors. At the end, Chapter Five covered the main points of the changes made to the candidate holistic insider threat behaviour model and how the survey results led to the enhanced holistic insider threat behaviour model.

CHAPTER SIX: QUALITATIVE PHASE AND FINAL RESEARCH MODEL

6.1 Introduction

Chapter Five provided a general overview of the quantitative method applied to the survey responses. It covered the main points of the changes that were made otp the candidate HIT model and how the survey results led to an improved list of factors. At the end of this chapter, an enhanced HIT model will be presented. Chapter Five Chapter provided the groundwork for this phase of the study.

This chapter describes the evaluation of the enhanced HIT model. It gives a general overview of the qualitative approach in this research. As discussed in section 4.2, this study collected the data sequentially in two phases. The quantitative method conducted first provides a wide view of the research problem followed by the qualitative method to evaluate, refine and enhance the result. The interviews have been conducted to support two outcomes. The first is to evaluate the enhanced HIT model resulting from the survey to confirm the answers to the first research question. The second is to provide material for the second research question of the thesis. The data from these interviews will be analysed and a summary of the interviews will be presented to illustrate the main concepts that cover the feedback regarding the enhanced HIT model. At the end of this chapter, the final HIT model will be presented.

6.2 Interview Design and Decisions

This section discusses the interview design, the reasons for choosing in-depth semi-structured interviews over other interviews methods and interview analysis and coding, as well as the number of participants together with their experiences and job titles.

Qualitative researchers have established a number of qualitative data collection techniques. One of the most common qualitative data collection methods is the interview (Lincoln and Guba 1985; Maykut and Morehouse 1994). In the light of undertaking a qualitative method, this research aims to explore essential meanings through humans' accurate description of their experiences as well as the quantitatively calculated relationships in the previous section. The interview method was divided into two parts. The first part was to evaluate the enhanced insider threat behaviour factor from the survey method. While, the second part in the interviews was to obtain the participants' comments and thoughts regarding how each factor can be managed. The research in this section will explain and present the interviews' design which demonstrates each step taken to conduct this phase.

Table 6.1: The interviews design

Process	Action taken
Development of the objectives	The objectives of the interviews method are: • To evaluate the new outcome model from the survey. • To obtain some guidelines which help to minimise the insider threat issue.
Development of interview questions	Developed the interview questions according to each factor in the enhanced model from the survey phase. Questions were developed and checked by supervisors for editing.
Identification of the participants	The researcher searched for Information Security Specialists who have ten years of experiences or greater in the information security field.
Interviews	• There were three rounds of data collection: the first round collected six interviews, the second round collected two interviews and the final round collected three interviews. • Five of the participants preferred to be interviewed through Email, four of the participants were interviewed through Skype and two via phone.

Process	Action taken
Transcription	Interviews transcribed and checked.
Coding	• Thematic content analysis with the coding done in NVivo • Paper coding through mapping techniques and revisiting the interviews. • Returning to NVivo for a holistic approach to coding.

6.2.1 Obtaining Interviewees

To carry out the interviews, the researcher prepared an invitation letter that contained the following:

- Introduction to the researcher
- General information about the research
- The purpose of the interviews
- The benefits of the research
- The researcher's willingness to conduct the interview in the manner most convenient for the interviewee, such as email, phone or Skype
- A statement stating the researcher's willingness to provide the results of the study at the end of the research
- A statement assuring that confidentiality and privacy will be maintained.

The researcher distributed the invitation letter (attached in Appendix 3) in October 2012 through LinkedIn to 60 Information Security Specialists who have ten years or more of experience in the information security field. LinkedIn is a business focused social network Website for people in professional occupations. The advanced search ability in LinkedIn helped the researcher to locate the target participants based on specific criteria such as locations, job title, the industries in which they worked, and where they were educated (Bradbury 2011). Participants were given one week to respond, and then a reminder letter was sent to the non-responding individuals to remind and encourage them to participate in this study. Table 6.2 shows the three rounds of the interview, the number of participants who agreed to be interviewed and the actual numbers who completed the interview. The number of participants who

commenced the interview was less than those who originally expressed interest in the study.

Table 6.2: The interviews' three stages

Round	No. of participants	Invitation letter	Reminder letter	No. of participants who expressed interest in the study	No. of participants who were interviewed
One	35	1 Oct 2012	8 Oct 2012	10	6
Two	15	29 Oct 2012	5 Oct 2012	5	2
Three	10	26 Nov 2012	3 Dec 2012	5	3

Twenty participants were interested in the study and agreed to contribute to the interview, and eleven completed the interview questions. The theory saturation was achieved after the last interview in round two as the data became redundant and most of the themes and criteria were mentioned and confirmed by more than one participant. Therefore, the researcher decided to stop after the eleventh interview. According to Thomson (2011, 47) saturation is achieved when *"no new or relevant data seem to emerge regarding a category".*

Table 6.3 provides a brief description of the interviewees. Some individuals did not proceed with the interview because they refused to release any information and others were busy. The time difference between the researcher's country and the participants' country also proved to be an obstacle for the respondents. Therefore, five of the participants preferred to be interviewed through Email, four of the participants were interviewed through Skype and two via phone calls (see Table 6.4).

Table 6.3: Interviewees and their description

Participants	Description
Participant A	Participant A is a key informant male. He is a Chief Information Security Officer with over 24 years of experience in in Information Security and IT. He has held several positions including: • Chief Information Security Officer • Head of Information Security • Director, Office of the CTO and Strategic Consulting • Director of Information Security at • Global Security Solutions Leader • Commander, Information Technology Participant A hold a Master degree of Science in Computer and Information Systems Security/Information Assurance.
Participant B	Participant B is a key informant male. He is a Chief Information Security Officer with 24 years' experience in Information Security and IT. Participant B has held several positions including: • CEO • Chief Software Officer, Director Algorithmic and Secure Software design and code analysis • Chief Information Security Officer He holds a Master degree of Science in Information Security Engineering, and another Master degree in Information Systems Security.
Participant C	Participant C is a male. He is an Information Security Officer with over 10 years' experience in Information Security and IT he is the founder and CEO. He holds a Bachelors' degree in Computer Science majoring in System and Network Engineering (SNE) with a minor in Information Security. Currently, he is undertaking an Executive MBA. Furthermore, he holds a host of professional certifications recognized by the industry including ISC2 CISSP, EC-Council Certified Ethical Hacker, MCITPro 2008, MCSE and many more. Participant C is a Specialist in: Cyber Security and Cyber Warfare SME, Strategic and Tactical management, Business Process (re)design and Security/ Infrastructure design.

Participants	Description
Participant D	Participant D is a key informant male. He is a Chief Information Security Officer with over 20 years' experience in Information Security. His current and previous executive positions include Chief Security Officer, Chief Information Security Officer and advising Chief Information Officer, currently he working as Chief Information Security Officer. Participant D holds an Executive Juries Doctor in Cyberspace Law, a certified MBA in IT Management and undergraduate in IT Security. He is specialist in: Cyber-Law, IT Governance, IT Risk • Cloud Security, Social Networking Security, IT Security, Security Architecture Management Project/Program Management Threat & Incident Management, IT Security Software Development, Identity & Access Control, Change Control Management Forensics and E-Discovery. Participant D has held several positions including: • Chief Information Security Officer • Chief Information Officer - Director of Security Services • Information Security, DR and Compliance Audit Consultant • Information Security Consultant, Project Management. • Senior Information Security Engineer, Project Manager
Participant E	Participant E is a male. He is a Senior IT Security Manager with over 12 years' industry experience and 10 years' experience in Security Consulting & Management. Participant E is currently working as Senior IT Security Manager, and he has held several positions including: • Project Manager and Senior Consultant • System Analyst/Lead Developer
Participant F	Participant F is a male. He is a Manager of information Security and Services with 10 years' experience in information security and over 15 years' experience in information technology. He holds a Bachelor of Science in Information Technology and he is a specialist in: IT Governance, IT Risk, Cloud Security, IT Security, Security Architecture Management, Project/Program Management, Threat & Vulnerability Management and Technical Security Operations. Participant F is currently working as Security Administrator (Manager of Security Services), and has held several positions in the past including: • Director of Information Security • Director of Security Services • Systems Engineer • Senior Security Engineer • IT Security Consultant • Senior Technical Support

Participants	Description
Participant G	Participant G is a key informant male. He is a Global Chief Information Security Officer and has been working in the information security field for over 35 years. Participant G has a broad background in multiple facets of security including IA, physical, technical, personnel, and operations security and he is a specialist in Certification and Accreditation, Counterintelligence, Public Key Infrastructure (PKI), Physical Security Design and Implementation and Information Systems Security and Management. Participant G has held several positions including: • President & Principal Consultant • Adjunct Professor and Lecturer • Assistant Executive Director • Chief Information Security Officer and Senior Consultant • Security Analyst He holds a Master of Business Administration with a Concentration in Technology Management, Business.
Participant H	Participant H is a key informant male. He is an accomplished information security, risk management and technology leader with over 17 years' experience in information security and approximately 22 in technology. He holds a Master of Science (M.S.) in Information Systems and Technology Management, Information Assurance and Security. He is currently working as a Chief Information Security Officer, and has held several positions in the past including: • Solutions Strategy & Development Manager • Director, Integration Services
Participant I	Participant I is a key informant male. He is in IT and IT Security fields for more than 30 years. Currently, his job title is Sr. Vice President of Network and Technical Services and Chief Security Officer. He holds a Master of Science (M.S.) in Computer Science. He has held a number of positions including: • Sr. Vice President - Application Development and Ancillary Applications. • Senior Manager - Risk Consulting Group • Chief Information Officer
Participant J	Participant J is a key informant male. His job title is Chief Information Security Officer. He had been involved in the security industry for over 30 years, and obtained certifications in both the traditional/physical and IT security environments (CPP and CISSP designations). Participant J holds a degree in Computer Systems Technology. He has held several positions related to security including: • Information Systems Audits Principal • Manager, Information Systems Operations – Security • Senior Security Advisor

Participants	Description
Participant K	Participant K is a key informant male. He has been working in security for the past 22 years, with the past 12 years in commercial and corporate security. He has executive and management level experience in security audits, security reviews, security operations management, risk assessments, travel safety and security strategies, protective security operations, security guard services, physical security, security management, security provider reviews, security budgeting and commercial security sales and service. Currently he is working as a Security Manager and Consultant as well as Security Professional and Security Advisor. Participant K has held many positions related to security in the past including: • Director Security Services Asia Pacific for Travel Health, Safety & Security, Security Consultant • General Manager National Security Operations and Security Technical Advisor • Team Leader Protective Security and Travel Security • Security Team Leader • Security Manager-Project • Team Leader and Security Manager • Soldier and Security Professional

Table 6.4: Interview methods

Round	No. of participants	Interviewee name	Interview method
One	6	Participant A Participant B Participant C Participant D Participant E Participant F	Phone Email Email Skype Skype Email
Two	2	Participant G Participant H	Email Skype
Three	3	Participant I Participant J Participant K	Email Skype Phone

The main objective of the interview questions was to evaluate the insider threat factors in the enhanced model obtained from the survey and to obtain some guidelines and ways to minimise the insider threat problem. The researcher wanted to ascertain whether or not these factors would contribute to insider threat behaviour.

Before the beginning of each interview, a copy of the information sheet and the consent form was sent to each participant (attached in Appendices 4 and 5). Each interviewee was requested to read and sign the consent forms, thereby agreeing to participate in the interview and having it recorded if it was conducted through Skype or phone. The eleven interviewees were very positive in their responses to the interview. They shared with the researcher their knowledge and experiences regarding the insider threat cases, and they provided significant comments on the insider threat contributing factors and the proposed model. Positive feedback was received from the participants regarding the proposed model. For example, participant D stated: *" I'd love to get a copy of your thesis when it's available since I find the subject quite interesting and I also like learning new things. You have obviously done your research and the questions were thought provoking and holistically applicable in my opinion".* Participant F stated "*Your model describes the many factors which might lead to insider threats – most of the factors are robust".* Participant J stated: *"As for your model - I really like it. I do not think I would add or subtract from the model or its definitions. I think it encompasses the components of*

insider threats, and identifies the most common aspects of how an organisation is impacted by the insider".

All the Skype and phone interviews were recorded using a digital voice recorder and then downloaded to the computer for transcription. The email interviews were already in written text, allowing the researcher to analyse them directly. Skype and phone interviews typically lasted between 35 minutes to one hour, while the email interviews took between one to two weeks with each participant. Some interviewees took more time than others since they provided extra information including examples. The transcriptions were stored in both hard and soft copies.

6.2.2 Data Analysis and Coding

Data analysis in the qualitative study requires some flexibility and creativity in analysing the data. According to Creswell (1994, 153):

> *"Data analysis requires that the researcher be comfortable with developing categories and making comparisons and contrasts. It also requires that the researcher be open to possibilities and see contrary or alternative explanations for the findings."*

According to (Zhang and Wildemuth 2009), content analysis is a commonly used method for analysing interview transcripts in order to disclose people's thoughts. Qualitative content analysis *"involves a process designed to condense raw data into categories or themes based on valid inference and interpretation"*(Zhang and Wildemuth 2009, 2). Miles and Huberman (1994) recommend starting the qualitative content analysis process during the early phases of data collection. This early application of content analysis will assist the researcher to move back and forth between themes development and data collection, and can it direct the data collection toward information that is more useful for addressing the research questions.

In light of the confirmatory nature of this phase, the deductive content analysis (Mayring 2000a) process guided the data analysis. According to Mayring (2000b, 4), the main idea of the deductive content analysis is *"Deductive category application works with prior formulated, theoretical derived aspects of analysis, bringing them in connection with the text. The qualitative step of analysis consists in a methodological controlled assignment of the category to a passage of text"*. The interviews were analysed using deductive content analysis with the coding done through NVivo. Coding is a process whereby the researcher edits and reorganises the data into pieces to visually map it out into a holistic model that tells a story (Ryan 2006; Monette, Sullivan, and DeJong 2007).

The researcher followed the two steps recommended by Miles and Huberman (1994) in order to analyse the interview data. Step one is the analysis of individual scripts while stage two analyses all the scripts. The detailed sequential process of step one is illustrated in Figure 6.1; the sequential process of step two is illustrated in Figure 5.2.

Step one is the analysis of each script individually; the process of content analysis detailed by Tesch (1990) was utilised in order to analyse each interview. Firstly, the researcher prepares the data by transcribed all recorded interviews using respondents' words to represent their thoughts. The eleven transcribed interviews yielded 110 pages of transcripts. A sample of the transcript is included in Appendix 7. While the email interviews were already written, the researcher reformatted these so that all the transcribed data was consistent in format.

Secondly, the researcher used individual themes as the unit for analysis. According to Zhang and Wildemuth (2009), *"when using theme as the coding unit, you are primarily looking for the expressions of an idea. Thus, you might assign a code to a text chunk of any size, as long as that chunk represents a single theme or issue of relevance to your research question*".

Thirdly, since this phase of the study utilised deductive content analysis to analyse the interview data, themes for this phase were developed according to the pre-defined categories (factors) from the quantitative phase (survey). Miles and Huberman (1994) claim that researchers, when performing deductive content analysis, can use preliminary categories or themes generated from previous research phases, theory or model as a basis for their themes. They can produce an initial list of categories from a previous research model, and they may adjust the model if any new categories emerge from the analysis. The researcher closely read the eleven transcripts. During this stage, the researcher looked for the pre-defined themes, highlighted them, and matched the relevant data to each theme. Once the main themes had been identified, the fourth step was to eliminate any overlap if one segment of text was coded into more than one theme (Creswell 2008). Finally, the researcher constantly reviewed the data and the developed themes to allow any new themes to emerge. For validation, the interview transcripts were revisited many times in order to compare the results with the matching factors derived through the quantitative phase.

The second step is the cross analysis of all the transcripts to combine the themes. The combined themes were checked in order to identify the similarities and differences between them. Similar themes were combined under the same name. After all the themes had been determined, they were organised into codes creating a holistic approach to the key findings. Further analysis of the combined themes resulted in eight main factors which constitute the final research model for this study.

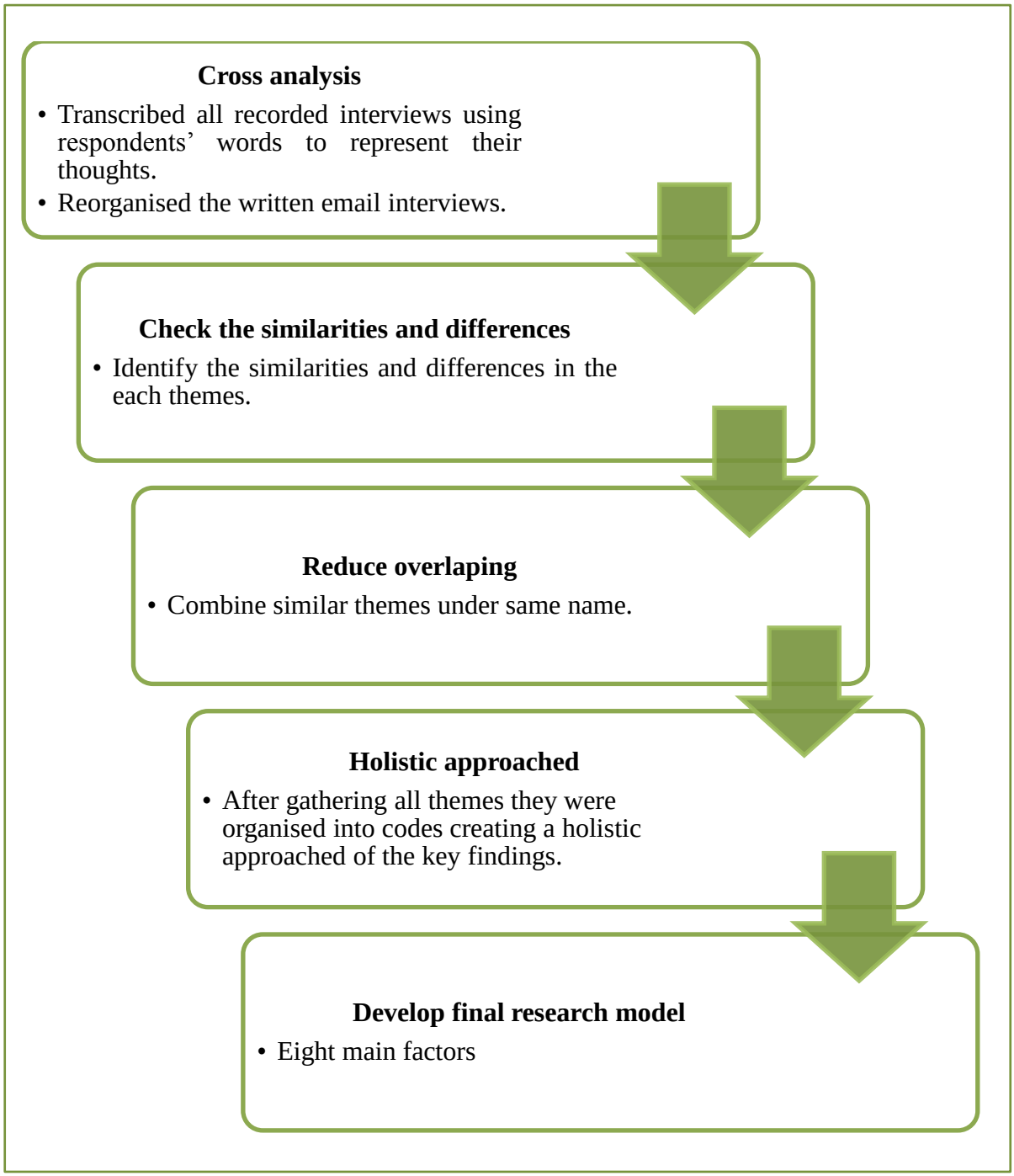


Figure 6.1: Step one - analysis of individual scripts

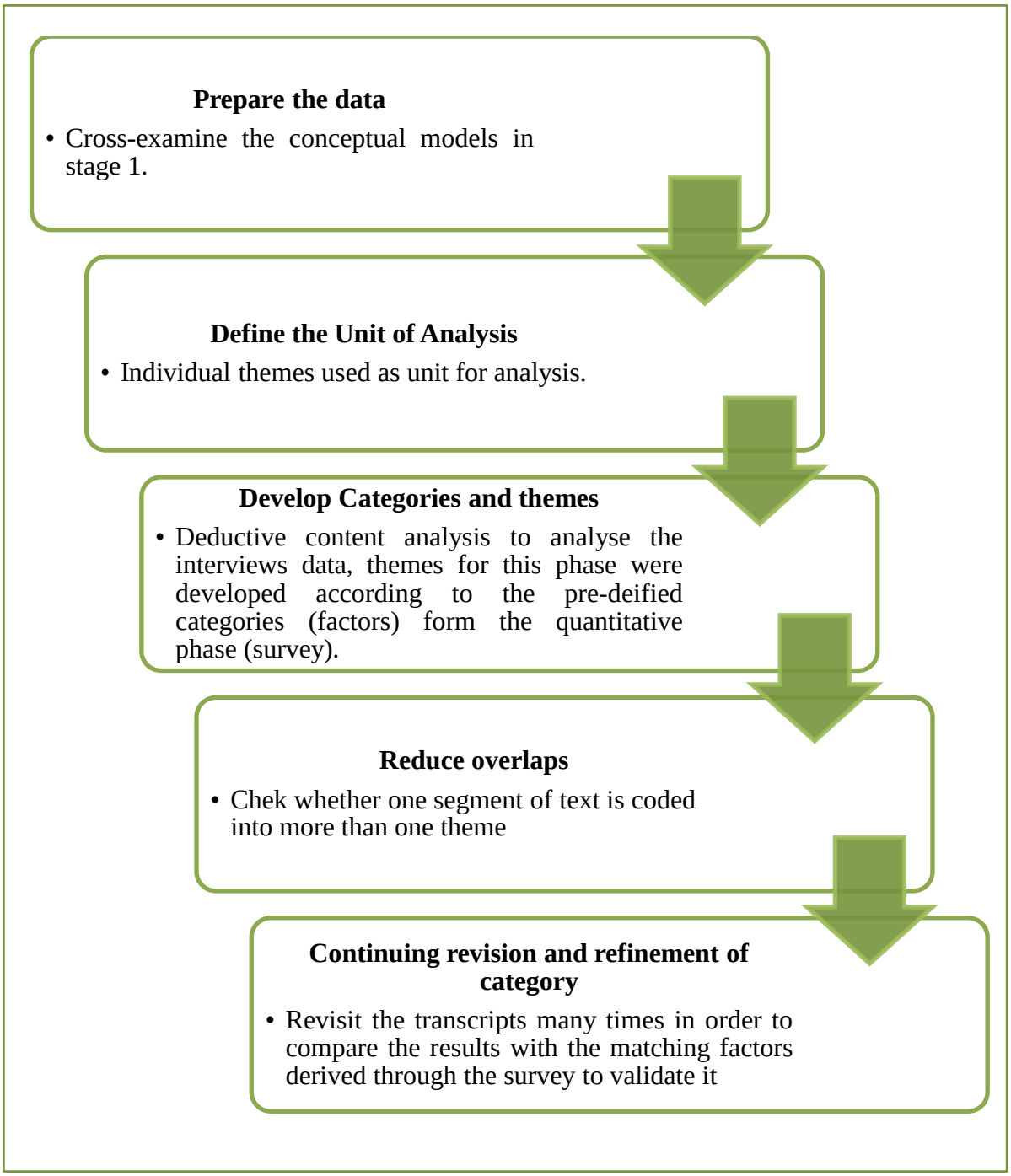


Figure 6.2: Step two - cross analysis of all transcripts

6.2.3 Rigour, Validity and Reliability

According to Golafshani (2003, 601), *"validity and reliability are two factors which any qualitative researcher should be concerned about while designing a study, analysing results and judging the quality of the study".* An open-ended perspective in a study gives validity and reliability to the study by allowing participants to explicitly express their opinion and experiences regarding a topic which assists the researcher in the data collection. Furthermore, recording the interviews will lead to more valid and reliable data (Golafshani 2003).

Rigour keeps the study valid in terms of utility, truth, and reliability (Morse 2002). According to Lincoln and Guba (1985), trust and credibility are important criteria. This research followed a mixed methods approach which has a strong interpretive aspect. The researcher first reviewed the literature in order to produce the candidate HIT model. The second results from the factor analysis were interpreted by the researcher to produce the enhanced HIT model. Hence, to ensure this was done in a credible and trustworthy manner, interviews were conducted to establish credibility. Further, to ensure that the interviews themselves were trustworthy and credible, the following decisions were made for the purposes of validity and reliability:

- The researcher used semi-structured interviews with open-ended questions. All interviews were carefully transcribed using respondents' words to represent their thoughts.
- Credibility was ensured mainly through member checking. Member checking was utilised in numerous ways during data collection and analysis:
    1. The researcher discussed the interview questions with the participants at the end of each interview during the pilot study.
    2. During formal interviews, the researcher shared the ideas and information extracted from other interviews to obtain further clarification of new points that emerged.
- Constant comparisons were made by ongoing review of data with continuous checking of the themes to compare meanings.

- Saturation was achieved as the data became redundant when most of the themes and criteria were mentioned and confirmed by more than one respondent.
- Participants' comments were written in italics and between bracketed quotes to clearly help the reader distinguish between the researcher's words and the respondent's words. According to Whiteley (2002), achieving rigour in studies means that the reader must be able to recognise the respondents' words as distinct from the researcher's words.
- Ongoing checking regarding research decisions, findings and process.

6.3 Results and Interpretations (Cross Analysis)

The participants were asked the same questions within a flexible framework. They were encouraged to talk about their experiences, thoughts and opinions through open-ended questions and they were asked to provide examples from their experience. According to Dearnley (2005), the open-ended questions were intended to encourage strong and in-depth discussion and lead to the emergence of new concepts.. The validity of the study was increased by the collection of data that were rich in detail and analysis (Hussey and Hussey 1997).

The respondents were asked 15 questions (see Appendix 6) which were divided into four categories. The questions are included in the interview presented below for clarity.
The categories into which questions were divided included:

- Demographics questions: questions 1 and 2.
- General Insider threat questions: questions 3 and 4.
- Insider threat contributing factors questions: questions 5 - 13.
- Enhanced HIT model evaluation questions - questions 14 and 15.

As previously mentioned, the interview method was divided into two parts. This section presents the questions asked in the first part of the interviews; the second part of the interviews will be discussed in Chapter Seven.

6.3.1 Demographics Questions

The information collected from respondents which related to demographics included their gender, experience and their current job title. All the participants were males with 10 or more years' experience in the information security field. The uneven gender distribution in these roles within the organisations and also the required experience years could explain why all the participants were male.

6.3.2 General Insider Threat Questions

The researcher asked the interviewees several general questions regarding their perspective and experience about insider threat behaviour that included:

- how they define the insider threat
- whether they had experienced insider threat cases
- their opinion of the risk factors associated with inside threat

Each participant defined the insider threat from different angles but all of them made almost the same points. For example, participant A stated that *"Threats that occur within the parameter of the network. Threats are a combination of people, motives and opportunities."* Similarly, participant B stated *"Any internal threat from within the organisation. This includes: staff/employees, contractors, external agencies (accountants/ lawyers etc.) and partners."* Participant K stated *"Persons, employees, vendors and affiliates that have access to internal physical or electronic resources not usually available to the public or consumers."* All participants perceived the insider threat as a threat that was posed by an entity with internal access to the organisation.

It was noticeable that all of the participants had experienced insider threat cases throughout their working life. Respondents were very cooperative in sharing with the researcher the insider threat cases they had encountered; only one interviewee (participant B) chose not to answer this question. Most of the perpetrators mentioned by the participants were mainly motivated by the desire for financial or personal gain.

Responses to Question 4 highlighted the importance of some indicators as clues that someone might be an insider threat, such as financial problems and insider behaviour. Moreover, there were different views regarding the risk factors which contribute to the insider threat. Some of the participants argue that all staff pose a threat to the organisation. Participant B believed that "*All staff are insider threats as an example. Whether a threat evolves into an incident is a separate issue. All staff, all contractors etc. are threats. Some are accidental. Some are intentional, but there always remains a risk and there is not an absolute means to remove this.",* similarly participant G assumed *"All the in-house staff are insider threat"*. On the other hand, other participants' comments regarding risk factors focused on issues related to access, remote access, loyalty and lack of frequent monitoring. Some participants considered access as a very important risk factor. Whether accessing resources to which an employee should have no access, or using access to perform unauthorized tasks, both constitute a high risk to any organisation.

6.3.3 Insider Threat Contributing Factors Questions

This section presents the participants' comments about the insider threat contributing factors to ascertain whether or not these factors influence the insider to behave inappropriately with regards to security. The researcher has divided this section into two sub-sections; the first one deals with the eight themes that are driven from the interviews, and each theme discusses one of the proposed factors which facilitate the analysis. The second section discusses the most common risk factor according to the participants' experiences.

6.6.2.1 Factors contributing to insider threat

This section will discuss the eight factors presented in section 5.6 that contribute to inappropriate insider threat behaviour that emerged from the survey and were validated by the interviews. These factors include: conflict between the organisation and an individual who is willing and able to seek personal gain at the organisation's expense; giving high trust to underachieving employees; outside influences on employees; the perfect crime; inadequate security policy; socially isolated employees; liberal access and loyalty of employees.

- ***Conflict between the organisation and an individual who is willing and able to seek personal gain at the organisation's expense***

As discussed in section 5.6, the most common causes of the conflicts between organisations and individuals are a lack of communication, differences of opinion, personality clashes, stress, high workloads and culture clash as employees sometimes see a clash of values as a significant cause of conflict.

From the interviews, the researcher observed that all of the participants agreed that conflict between the organisation and an individual is an important factor in insider threat behaviour. This is illustrated by the following comments:

> *"Any type of conflict between an individual and organisation always has the tendency to increase risk of insider threat. For example, if an individual is seeking for promotion who he/she thinks he/she rightfully deserves and this promotion is granted to somebody else, this individual will carry a risk of being an insider threat." (Participant I)*

> *"My personal experience, from previous positions, is that an insider with a real or perceived conflict with an organisation is a greater threat than from an outside party. A motivated actor with inside access to assets, etc. has greater opportunity to impact an organisation."* (Participant J)

> *"The motives of the individual in question will change as soon as a conflict starts, and this may in turn motivate this individual to seek personal enrichment." (Participant C)*

Participants provided the researcher with examples of cases they have encountered in which the employees abuse the organisation as a result of the conflict. The following comments illustrate the participants' experiences:

> *"I have faced it [conflict between the organisation and an individual], and there are people that misuse computer resources". (Participant A)*

> *"In previous organisation s, I dealt with an inside threat stemming from an employee who took advantage of the organisation while on sick leave. The employee had justified the offense by stating they were upset at the organisation not providing full benefits while on leave, and then took advantage of the corporation by working for a competitor. While we were unable to fully estimate the damage, we did identify that some information was missing and eventually attributed the loss to the employee." (Participant J)*

> *"I have experienced individuals that feel the company "owes" them something due to a conflict, usually around position and remuneration. Therefore they will seek to extract compensation, justified by this mindset, as a means of self-regulation and justice especially in larger companies." (Participant K)*

In addition, some participants provided general examples about conflict and how it could affect the organisations as noted below:

> *"Organisations that host hostile, competitive or oppressive cultures will invite ethical and moral conundrums. For example, if compensation one employee receives is directly in competition to another employee, the drive to win may increase the likelihood that one or both employees will cheat*

> *to get ahead. Another example might be where an employee's contributions are not properly and fairly acknowledged which leads to employee frustration which leads to retention issues and employee misconduct." (Participant D)*

> *"Using justice studies (my undergrad minor), we see meat eaters and grass eaters in law enforcement. That is, grass eaters take a discounted meal whereas meat eaters use their position for more direct gain. The same holds true for the individual. In all cases, except for someone lacking common sense, the organisation usually means conflict with individuals. The perpetrator becomes disillusioned and begins rationalization of treat behaviours. Once rationalized, conflict drives action." (Participant H)*

Although one of the participants had not encountered any cases of conflict, he was aware of some employees who had attempted to benefit personally from a conflict between themselves and their organisation, stating:

> *"To date, I have not experienced this personally. However, I am aware of certain employees who have attempted to make personal gain at the organisation's expense because of the conflict. Unfortunately, there was no strong disincentive to not attempt the hurt the organisation." (Participant G)*

In summary, the factor of conflict between the organisation and an employee was supported by 100 per cent of the participants. Therefore, this factor was incorporated in the final research model. All of the participants agreed that conflict between organisation and employee increases the risk of insider threat.

- ***Insufficient security policy***

This factor mainly focuses on insufficient or inadequate policies that include: the implementation of an inappropriate information security policy, out-dated information security policy and lack of training and awareness (inadequate security policy is described in detail in section 5.6).

From the interviews, it appeared that three participants were less worried about policy as they believed that even if there is a strong policy, it will not prevent or minimise the risk of insider threat because individuals might not follow it as indicated by the following comments:

> *"The policies nowadays, they don't make a big difference. I mean, they are there so you can punish people or deal with people, but they're not really there as an education mechanism unless you teach people about it training and awareness as appropriate." (Participant A)*

> *"In my experience, policy is like law. It only keeps honest people honest. It does very little to prevent people from breaching security. Training and awareness are aids, but dishonest people don't follow rules." (Participant H)*

> *"Sure, it is important to let your employees know what behaviour is expected, but I do not believe that it actually prevents anything. People will do what they can get away with, eventually. Policy is then just a means of being able to respond to the full extent because you have given fair warning." (Participant C)*

On the other hand, most (eight) of the participants agreed that an inadequate policy does contribute to insider threat behaviour. The following comments express their opinions:

> *"Yes Insufficient policies increase the risk of insider threat. Without knowing what is acceptable people test what they can do." (Participant B)*

> *"Yes, you increase the unintentional inside threat by not employing sufficient controls and you lack sufficient deterrents for the intentional inside threat." (Participant D)*

> *"The most effective ways to avoid leakages are sufficient policies and security procedures. These are pillars to avoid*

insider threats. Without them, no measures could be practical & effective." (Participant E)

"Definitely Yes Insufficient policy increases the risk of insider threat since it makes the organisation vulnerable. We need to ensure that security is taken seriously by management and staff and invest adequate time to develop security rules, standards, policy and procedures and to implement proper tools." (Participant I)

"Absolutely insufficient security policy has been one of the most telling indicators of potential insider threat – the lack of policy, training etc." (Participant J)

"Policy is documented evidence of what plans are in place or implemented. If you are not able to document it, it doesn't exist ... Policy is not a panacea but the absence of such documentation certainly accelerates negative outcomes." (Participant K)

Further, interviewees believed that strong policies as well as sufficient training and awareness are vital to minimise the risk of insider threat. They suggest that if the employees are aware that policies and security are strong, and they are sufficiently trained and educated, they are less likely to become involved in any malicious activities, as shown by the following comments:

"If the individual knows that security is strong and they are being monitored, this individual is far less likely to engage in any malicious activities. Through proper security awareness, training, policy, logon banners, etc., we are telling this potential insider threat that we are watching, and it's going to be very difficult to get away with unauthorised behaviour… Policy layer – we must have strong policies in place (and educate users on them) which dictate classification levels of data along with the restrictions on what can be shared. Design and implement (and train users on) a comprehensive Policy set are essential."(Participant F)

> *"Yes [Insufficient security policy increase the risk of insider threat]. If employees do not know what the framework is in which they must work, I believe they are more likely to take inappropriate actions … All organisation should ensure that policies are integrated into the organisation. Ensure that routine training is in place that highlights the requirements … A lack of policy will ensure that the organisation is not signaling its desire as to what actions are acceptable. This will ensure that employees may even unwittingly take actions that are detrimental. Solid policies that are well-advertised are crucial." (Participant G)*

> *"Yes [Insufficient security policy increase the risk of insider threat]. Insider threats are both intentional and unintentional actions. Training and written policies keep honest people honest and reduce accidental treats or ones where the person lacked common sense" (Participant H)*

In the summary, most of the interviewees agreed that an inadequate security policy had an influence on insider threat. Seventy-two per cent of participants confirmed the importance of implementing an appropriate information security policy to decrease the risk of insider threat behaviour. Hence, this factor is included in the final research model.

- ***Giving high trust to underachieving employee***

As discussed in section 5.6, underachievers are those employees who do not regularly apply effort to their work and working far below the expected performance. Most often the problem is not their ability, but attitude; they often engage in inappropriate or concerning behaviour prior to the incident such as delays, absences and poor job performance. Most of the participants agreed that giving high trust to underachievers increases the risk of insider threat, although none of the academic literature discusses this issue.

The interviews indicated that the high level of trust and access, especially for underachievers, could increase the insider threat behaviour. Below, excerpts from the transcripts provide some participants' opinions on this issue:

> *"Yes it does [giving high level of trust to underachiever increases the risk of insider threat]. The probability of risks from employees with low performance and lack of core capabilities is very high. The problem becomes even greater if they had a high degree of trust and access." (Participant E)*

> *"Giving high trust to an employee already underachieving should not be allowed. That is to say, we do not elevate someone's privileges if they are known to be underachieving. If someone has elevated privileges and then becomes an underachiever, we immediately reduce privileges because they demonstrate a risk." (Participant H)*

> *"Yeah [giving high level of trust to underachiever increases the risk of insider threat], so for example if you give all the employees like a default level of access, there is risk, you are raising your exposure to the risk. It doesn't have to be malicious behaviour on their part. It can be incorrect behaviour that will be a risk. For example, if they have access to deleting entire directories, they may delete it inadvertently." (Participant A)*

The highlighted risk factor that underachieving employees may cause an increasing risk of the insider threat was confirmed by all interviewees. However, some participants further added that organisations should investigate the causes of this underachievement.

> *"Agree giving high trust to underachiever increases the risk of insider threat behaviour. However, for this one, we need to investigate the root cause for underachievement and take necessary actions to remedy the situation if possible. Their underachievement may be the result of not investing on them, not providing them the adequate training, or setting them fail with only limited knowledge on a project or a process." (Participant I)*

> *"I agree giving high level of trust to underachiever increases the risk of insider threat. They are certainly markers to pay attention to. What is the underlying reason for that underachievement? Could it be that education or job support and empowerment doesn't exist? There are many personality types and a company that identifies them and then is able to adapt to this is important." (Participant D)*

Moreover, a group of participants suggested that underachieving employees constitute a risk to the organisation even if they have optimum trust.

> *"Yes underachiever increases the risk of insider threat; it all comes to the person and the governance of that person. If they are not provided opportunity then it could make them perform more." (Participant B)*

> *"Yes. If they are underachieving, the position or the organisation may not be a good fit. They may not have the organisation's best interest in mind – if the opportunity presents itself they may be inclined to take advantage for their own gain." (Participant F)*

> *"Yes, I feel that underachieving employees are not as invested in the organisation, so they may feel that what they do that might hurt the organisation is not as critical." (Participant G)*

> *"The concept of "least access privilege" is something all organisations should strive to achieve. I'm convinced that threat changes based on the performance of the employee as well as other attributes. Employee low performance is indicator to identify potential insider threats." (Participant J)*

In brief, most of the participants agreed upon the influence of giving high trust to underachieving employee factor. Eighty-one per cent of the interviewees confirmed the significance of inappropriate behaviour such as delays, absences and poor job performance in increasing the risk of insider threat. Hence, this factor is incorporated in the final research model.

- ***Outside influence on employees***

As discussed in section 5.6, the influences of the external environment could include employees' background, values, economic motivators and employee coercion by outsiders. Hence, organisations have minimal control over the outside influences on their employees.

During the interviews, all participants agreed that outside influences on employees can cause serious problems as highlighted by the following comments.

> *"Outside influence aids in rationalizing the issues, pressure and hence motive." (Participant B)*

> *"Bribery or other methods of coercion may entice an individual to turn to malicious insider." (Participant C)*

> *"Temptations are everywhere. It varies from person to person. Succumbing to temptation is inevitable and the thresholds vary again form person to person. I believe all employees can be influenced by outside factors, everyone has their price ultimately." (Participant D)*

However, some of the participants' opinions varied about who can be affected by outside influences. They suggested that employees with ethical lapses, less training and financial struggles are much likely to be influenced by external factors.

> *"Outside influence increased risks in weak values and less moral personalities." (Participant E)*

> *"People who are the candidates for insider threat behaviour but don't have the proper training, knowledge or tools to act on it can easily be coerced by outside influence that are capable to do so." (Participant I)*

It was revealed that desire for money, greed and financial situation are considered to be emotional triggers that make the employees more prone to the influence of external factors.

> *"Money. Money. Money. If the employee is stressed over money, feels they are not being compensated appropriately, or feels their income is threatened in any way they can be influenced by the external factors " (Participant H)*

> *"In my experience, employees who are facing some type of coercion (i.e. a physical threat, the threat of losing your home, unable to provide for your family, etc.) will react differently and accept some personal risk to achieve a personal goal. If an employee justifies the need to steal because their family is wanting, an employee will unconsciously seek opportunities to steal." (Participant J)*

One of the participants had limited experience with the highlighted risk factor, but nevertheless suggested the immediate termination of employees' employment if they are influenced by outside sources.

> *"I have very limited experience with outside influences having had an effect on employees. I would guess that influences such as gambling, debt, illicit substances, etc. could have a great risk on the personal behaviour... The employee should be removed from his trusted position as soon as it became apparent that the influence could affect his trustworthiness. This rendered the outside influence moot." (Participant G)*

In the summary, all interviewees (100 per cent) confirmed the significance of outside influences on employees in the behavioural insider threat model. Thus, this factor is incorporated in the final research model.

- ***Liberal access***

Liberal access relates to unnecessary access or more access given to the employees than what they actually need to perform their job. This arises in different ways such as allowing mobile devices to access the organisation's network remotely or by giving employees a high level of access to IT systems and sensitive data. Many

organisations offer their employees more access than what they essentially need to perform their job (liberal access described in detail in section 5.6).

Many participants provided their own definition of liberal access and most of these definitions matched that of the researcher. The following are some of their definitions:

> *"Liberal access sounds like to me that access to company resources exceeds the business needs of the employee." (Participant D)*

> *"Unnecessary open-minded access to facilities allowed to employees. Sometimes given for convenience, and sometimes just for nothing." (Participant E)*

> *"Liberal access would be opposed to minimal access – minimal access is the proper way to grant access to any resource. Liberal access would be something in excess of what is required to do their job." (Participant F)*

> *"Access above or beyond that which is necessary." (Participant H)*

> *"In my opinion, "liberal" access is typically access to resources above what is required for your day-to-day activities." (Participant J)*

One participant asserted that he does not believe that liberal access causes intentional malicious behaviour as demonstrated by the following comment:

> *"I am not sure it is an influence for malicious behaviour. However, it could influence negligent, accidental, or errant behaviour." (Participant H)*

Nevertheless, it is apparent from the interviews that the majority (ten) of the interviewees agreed that unnecessary access or more access being given to the

employees than what they need increases the risk of insider threat as indicated by the following comments:

> *"Of course liberal access increases the risk. In fact it is encouraging people to access things that are beyond what they need to do in order to perform their job. So once you do that, you increase the risks for the enterprise… The biggest abuse happens when people with appropriate access is used it inappropriately, because that is a violation of trust. So you trust people to, for example, perform their job, but when they are not performing, or performing religiously, and then you have issues that you need to handle" (Participant A)*

> *"Liberal access simply enables people to do wrong and thus entices them to do so." (Participant C)*

> *"Facilitating access by any device or facilitating access by providing excessive access is the direct result of instituting a liberal access environment. ALL people eventually will bend or break, intentionally or unintentionally the expected norms of the organisation." (Participant D)*

> *"If they have this amount of access, the temptation may be there to use it outside the boundaries of their job." (Participant F)*

> *"I think this type of access can provide a (potentially) false sense of entitlement in an employee, which may lead to inappropriate behaviour or unintentional behaviour. If I use the IT environment, providing an employee unfettered access to the Internet, or allowing an employee to gain access to an entire file structure system can be problematic for an employer. Employees with this level of access may "expect" to have access to other resources, and then see there is a potential benefit to having this access. That benefit may be anything from a financial reward from a competitor, to using information gained by this access to further their careers in the organisation." (Participant J)*

One of the participants assumed that liberal access can be considered as presenting a great opportunity for the insiders.

> *"Liberal access can be opportunity. Self-rationalisation and economic motivators can influence even the most pious of individuals. Not to mention and expectation of success without consequence." (Participant K)*

Other participants agreed that liberal access increases risk, and they suggest that a minimum level of access should be granted to all employees and this should be based on their job.

> *"The minimum level of access should be the appropriate standard for all employees, even those trusted employees. Giving employees unnecessary access accomplishes nothing, and provides an opportunity for employees to take inappropriate actions." (Participant G)*

> *"This is not a wise decision which will invite ill intentions for those who have the tendency and skills to cause harm or disclose/leak sensitive information to others. Access should be granted based on the job functions performed and continuously monitored by entitlement review process." (Participant I)*

Furthermore, interviewees believed that remote access creates a great risk for any organisation, since the employees can access confidential information from outside the workplace. The following comments clarify this belief:

> *"Accessing network remotely during vacation. The point here is doing things unnecessarily must raise red flags. Why some employee would, during his vacation back in his home country, connect to company's network? Was it really needed or that urgent? Is he trying to copy some files/data/trade secrets?" (Participant E)*

> *"Insider threat increased by increased attempts to access confidential files/folders from outside the department … increased use of remote access software, during off business hours… increased file transfer activity during off business*

hours, either on premise or via remote connection. " (Participant J)

Some interviewees believed that mobile devices could pose a threat to the organisation in general; however, if the organisation stops it, this will cause some inconvenience. The following comment illustrates this:

"With pure information security point of view, liberal access especially mobile device is sometimes simply wrong and sometimes it's very wrong. Mobile devices for malicious insiders are more convenience to share the confidential info to anyone they like. But the most immediate disadvantage of stopping it is killing the convenience. So we must control it, not stop it in full. For example I'm checking my mail 24/7 on my iPhone. If they stop my access, I'll have to stay in my office to check my mail. This is impractical for people like me who have to play versatile roles in my company. (Participant E)

"Mobile devices pose external threats too. For example, what if an authorised smartphone is stolen?"(Participant E)

However, another participant stated that mobile devices do not increase the risk of insider threat unless the organisations do not use the suitable security policy:

"Mobile Devices will not pose a threat if there are proper security procedures built in around those and an effective Mobile Device Management (MDM) solution is activated." (Participant I)

In brief, the majority of participants agreed that liberal access increases the risk of insider threat. Ninety-one per cent of the respondents confirmed that unnecessary access or more access given to the employees than what they actually need to perform their job can increase the insider threat. Hence, this factor is included in the final research model.

- ***Loyalty of employees***

The absence of loyalty can negatively affect an employee's work efficiency and could expose the company to serious security risk as discussed in section 5.6.

From the interviews, the researcher observed that all of participants agreed that employee loyalty can influence the insider to behave in an inappropriate way as demonstrated by the following comments:

> *"Yes, of course, loyalty can affect whether or not somebody will do something on purpose. The more disaffected and unhappy an employee is the less he or she will be protective of the organisation. And that will lead to increased risk and eventually increased vulnerability." (Participant A)*

> *"Employee disloyalty limits rationalisation and creates an insider group mentality" (Participant B)*

> *"The reason behind insider threats sometimes distributed Loyalty – Working at two similar places for example." Loyalty affects the insider threat behaviour hugely much more than any other factors. Loyalty is not something we can impose onto someone. It has to come from inside the personality of the recruited and appointed person." (Participant E)*

> *Loyalty keeps the insider at bay, until his or her trigger event. That is to say, the insider may have only exhibited loyalty, but it was not part of their personality. Their true nature is revealed under the pressure of a trigger event. (Participant H)*

> *"If workers are forced to work in unjustified and unwanted situations, this may invite inside threat behaviour. But, it can definitely affect in a positive way if organisations can develop loyalty of their employees by doing the right things and treating them fairly in every aspect. Loyal employees will not seek harm to organisations." (Participant I)*

> *"If an employee does feel some fealty to the organisation, they are less likely to do something inappropriate". (Participant I)*

Concerns about the loyalty of outsourced employees were raised by some of the participants during the interviews. Loyalty of the outsourced employees was considered as a significant factor affecting the insider threat behaviour as indicated by the following comments:

> *"Outsourcers may steal information. Also outsourced resources are less careful (why should they care?) so thy less loyal." (Participant E)*

> *"It is the insider that appreciates the value of their compromise; therefore they specifically target an outsourced entity with an offer."(Participant K)*

Some participants declared that accessing the organisations' network remotely could decrease the employee loyalty:

> *"It's my gut feeling that somebody who remotely accessing the organisation network would be less loyal and more likely to share data on the internet, or to use the same equipment for internet access, which of course raises the risk." (Participant A)*

> *"Remote access essentially places a layer between their moral code and perceived consequences. Since they are "out of sight, out of mind" they may be more easily motivated to misconduct." (Participant D)*

> *"If an employee is disengaged from the workforce, or doesn't find some way to bond with co-workers, the employee may act upon emotions or perceived threats. This "acting out" may lead to insider threats, even if the actions are only to harm a specific work unit or team." (Participant J)*

In summary, the loyalty of the employees was verified by all interviewees. One hundred per cent confirmed the significance of employee disloyalty in increasing the risk of insider threat. Hence, this factor is included in the final research model.

- ***The perfect crime***

As explained in section 5.6, the perfect crime is when employees think they can avoid being detected. This factor relies on two important elements which facilitate and enable the insider to attempt the perfect crime: the knowledge possessed by the insiders and their level of technical skills.

Participants' opinions regarding this factor were divided: some of them completely agreed with the researcher while others did not. Two participants totally disagreed with regard to the importance of the knowledge in increasing the insider threat behaviour.

> *"No, I believe that knowledge of how insiders may be identified should they take unethical actions should reduce the desire to do so." (Participant G)*

> *"No. Having knowledge is unlikely to encourage or influence the insider to behave "inappropriately". If anything, it will deter inappropriate behaviour, to a point. Only a small percentage of people are deterred by overt and suspected deterrents. Others require monitoring or physical barriers." (Participant K)*

On the other hand, the majority (nine) of participants supported the importance of the knowledge and skills as a risk factor as shown in the following comments:

> *"Certainly knowledge and skills increase the insider threat behaviour. If they know how to defeat the system, they may very well try." (Participant C)*

> *"Yes knowledge and skills increase the insider threat behaviour. A person who is indeed intent on being a threat*

will do their best to circumvent existing controls. Conversely, a person who is considering misconduct may think twice about doing so if controls offer a sufficient deterrent… If there is a perfect crime, it would be because it went undetected and unpunished due to the combination of contributing factors like: Deliberate intent of the perpetrator and Inadequate control environment due to incompetent security practitioners, the absence of a genuine holistic risk assessment and or complacency." (Participant D)

"Obviously knowledge and skills increase the insider threat behaviour. If the insiders know how their posed threats or actions are detected, they'll find out ways to compromise the measures taken." (Participant E)

"Absolutely – having insider knowledge and technical skill is a huge risk to the organisation – it provides someone with intelligence they shouldn't have – intelligence they can leverage in an attack." (Participant F)

"Definitely agree on this [knowledge and skills increase the insider threat behaviour]. They will try to react to inflict damage sooner." (Participant I)

Two participants mentioned that if the insiders have the knowledge and skills as well as the motivation and opportunity, they are more likely to engage in inappropriate behaviour.

"Yes, I believe an insider's knowledge about existing controls (or lack thereof) can influence behaviour. If an insider has the requisite motivation and opportunity, and if they learn that there is a limited chance of being detected." (Participant J)

"Opportunity, so yes knowledge and skills increase the insider threat behaviour." (Participant B)

The perfect crime factor that includes the insider's knowledge and skills was acknowledged by the majority of the participants; however, two participants only partially agreed with the researcher as they believed the insider's knowledge was not an important risk factor as they claimed below:

> *"The short answer would be to some level, but not really the knowledge and skills increase the insider threat behaviour. If somebody is determined to perform something, for example fraud, they will create a mechanism around the known safeguards to use."(Participant A)*

> *"Theoretically, this is true. That is, if a person knows the systems it makes it easier. However, knowledge is not necessarily the motivator. Negative insider behaviour generally not driven by the person's knowledge. Their knowledge facilitates the behaviour after the fact." (Participant H)*

Hence, the majority of respondents confirmed the influence of the perfect crime factor. Eighty-one per cent of participants believed that insider knowledge and technical skills is a critical risk factor in the behavioural insider threat model. Meanwhile, both insider knowledge and technical skills were confirmed by the literature review. Consequently, this factor is included in the final research model.

- ***Socially isolated employees***

As discussed in section 5.6, socially isolated employees most often prefer to work from home or in isolated work areas. Such employees are commonly socially frustrated, isolated from the community, have poorer social skills and are poor team players.

Participants' attitudes and feelings towards socially isolated employees attracted a number of comments. The comments varied, with some interviewees agreeing that the social isolated worker increases the risk of insider threat behaviour and they support their agreement with examples, while others disagreed.

Two participants appeared less concerned about this factor as they believed that working from an isolated area such home does not increase the insider threat. Moreover, they claimed that social isolation does not relate to security. The following comments express this assertion:

> *"Working from home is relatively common. It does not necessarily correlate to security. Social isolation, in and of itself, also does not correlate to security." (Participant H)*

> *"Isolation does not correlate to access and opportunity. It is often easier to misappropriate from within a crowd where your actions and intentions can be hidden, rather than have the confidence to go ahead alone. If this demographic were true, nearly every policeman, nurse and emergency services officer would be an insider threat." (Participant K)*

On the other hand, the majority (nine) of the participants supported this factor as noted in the following comments:

> *"Yes, they are more likely to rationalise… They are an out group and do not see the others as a part of their own "community." (Participant B)*

> *"Yes. Socially isolated workers are greater threats. The reason behind in my view is the personal factors which is the major cause of leakages." (Participant E)*

> *"I would suggest that socially isolated workers may feel they have no investment in the organisation so they are more likely to take inappropriate actions." (Participant G)*

> *"Yes I do believe it could lead to feelings of disconnect or even more negative emotions, in turn leading to a lower bar for threat behaviour." (Participant C)*

> *"I would agree that the socially isolated insider does pose a potentially greater risk to the organisation. (Participant D)*

> *"There is a risk that socially isolated (or even physically isolated) workers increase the potential for insider threats to be realized. (Participant J)*

One participant recommended that the organisation needs to have policies that address working from home and ensure that policies do not create social frustrations.

> *"Yes since they may feel like an outcast and blame management for not taking proper actions. Work from home policies and HR. Policies should be complete and properly tested to ensure not to allow social frustrations." (Participant I)*

Briefly, the socially isolated employee factor was confirmed by the majority of participants. Eighty-one per cent of the respondents supported the significance of the social isolation factor in contributing to the insider threat. Therefore, this factor is included in the final research model.

6.6.2.2 Common risk factors

The researcher asked the participants to determine which of the discussed factors appeared to be more common than others based on their experience. The following comments are indicative of their opinion:

> *"Without a doubt, liberal access. Excessive access coupled with a lack of a governance framework based on a proper IT security risk assessment.)" (Participants D)*

> *"The most common failure in organisation s is the failure to restrict access. Many companies don't understand or wish to undertake the effort to institute a proper access control policy. This fact leads to employees getting "liberal" access – much more access than is needed to do their jobs." (Participants F)*

> *"I believe different types of Conflict between organisation s and employees, Liberal Access, and Insufficient Security Policy Implementation would trigger more Insider Threat Behaviour than others."(Participants I)*

> *"I would say that the user with higher privileges "snooping" around the network seems more common, in my experience. Granted, I've investigated employee breaches where someone was compromised by money or threat, and I've seen how unfulfilled employees can sabotage a company. It's just that I've seen more employees with higher levels of access cause havoc in systems - either with intent or inadvertently." (Participants J)*

It was noticeable that most of the participants consider liberal access, insufficient policy and security, and conflict between organisation and employees as being the most common factors contributing to insider threat.

6.3.4 Enhanced HIT Model Evaluation Questions and Changes in the Model

This section provides further explanation and justification for the inclusion of each individual factor in the final HIT model. It provides an overview of the participants' responses to the enhanced HIT model and their feedback. During the interviews, the researcher discussed with the participants the enhanced HIT model. Generally, positive responses were given by the interviewees, which encouraged the researcher to carry on with this research.

Positive feedback is illustrated by the following comments:

> *"You have obviously done your research and the questions were thought provoking and holistically applicable in my opinion." (Participant D)*

"Your model describes the many factors which might lead to insider threats – most of the factors are robust". (Participant F)

"As for your model - I really like it. I do not think I would add or subtract from the model or its definitions. I think it encompasses the components of insider threats, and identifies the most common aspects of how an organisation is impacted by the insider". (Participant J)

"I am interested in your work and the model development process" (Participant H)

It was noticeable after analysing all eleven interviews that the majority (nine) of the participants agreed with all the proposed insider threat factors. Hence, the outcomes from this phase provided an answer to the first research question of this study:

RQ_1: What factors influence the insider to behave inappropriately with regard to security?

The interviewees were asked two questions:

- If you were to add any other factors to the proposed model, what would they be? Why?
- If you were to delete any factors from the proposed model, what would they be? Why?

Responses to these questions revealed that most (nine) of the participants agreed with all factors introduced by the model and they did not wish to add or remove any factors. However, ten of the participants suggested changing the name of one factor to make it more general. After the researcher considered all participants' comments and feedback, a decision was made to change the name of one factor. This was the only adjustment resulting from the interviews. The other factors remain the same as described in section 5.6. Table 6.5 summarises participants' suggestions and the actions taken.

Table 6.5: Participants' suggestions and the actions taken

Participant	Suggestions	Action
Participant A	He suggested adding another factor to the model. This factor is lack of awareness.	**Suggested factor was not added.** Lack of awareness is already discussed in the information security policy factor, which has a logical sequence there according to the majority (ten) of participants.
Participants H and K	They suggested that socially isolated employees need to be removed from the model.	**The factor was not removed**. The researcher decided to keep this factor since all the other nine participants agreed that this factor is important and does contribute to the model.
Participants A, C, D, E, F, G, H, J and K	They suggested changing the name of the *'conflict between the organisation and an individual who is willing and able to seek personal gain at the organisation's expense'* factor. Participants believed that any conflict between organisations and the employee may lead to insider threat. Hence, they thought that a conflict that occurs may be enough for some individuals to launch their attack. Even if the insider has nothing to gain, he will still be committed to the threat out of a desire for revenge. In such cases of conflict, even if the insider does not have the required skills or abilities, he will possibly find other ways to revenge himself.	**The factor's name was changed.** The participants' suggestion was taken into consideration, so the *'conflict between the organisation and an individual who is willing and able to seek personal gain at the organisation's expense'* factor was changed to *'conflict between the organisation and an employee'***.**

6.4 Final HIT Model

The final HIT model is the outcome of successive steps starting with the combination of all the factors derived from the three sources (academic literature, IT industry publications and reported incidents reports) in the candidate HIT model. The candidate HIT model was evaluated by 100 security specialists using the survey method and resulted in the enhanced HIT model. The enhanced HIT model was

evaluated by eleven Chief Information Security Officers through in-depth interviews resulting in the final HIT model. As a result of the interviews, all the suggested factors from the previous phase were confirmed by the participants. The factors that were chosen after careful validation were consolidated into the final HIT insider threat behaviour model.

The HIT Model consists of factors that are validated by the qualitative data analysis and confirmed by the previous research steps. The integration of a realistic worldview of participants added valuable insights regarding the model and the factors. This integrative approach is intended to establish a holistic and integrated coherent insider threat model with greater explanatory power, to help organisations minimise insider threat behaviours. Figure 6.3 illustrates the final HIT model representing the factors that influence the insider threat behaviour. This HIT model will be utilized in the next chapter for the development of best practices to manage and minimise the insider threat.

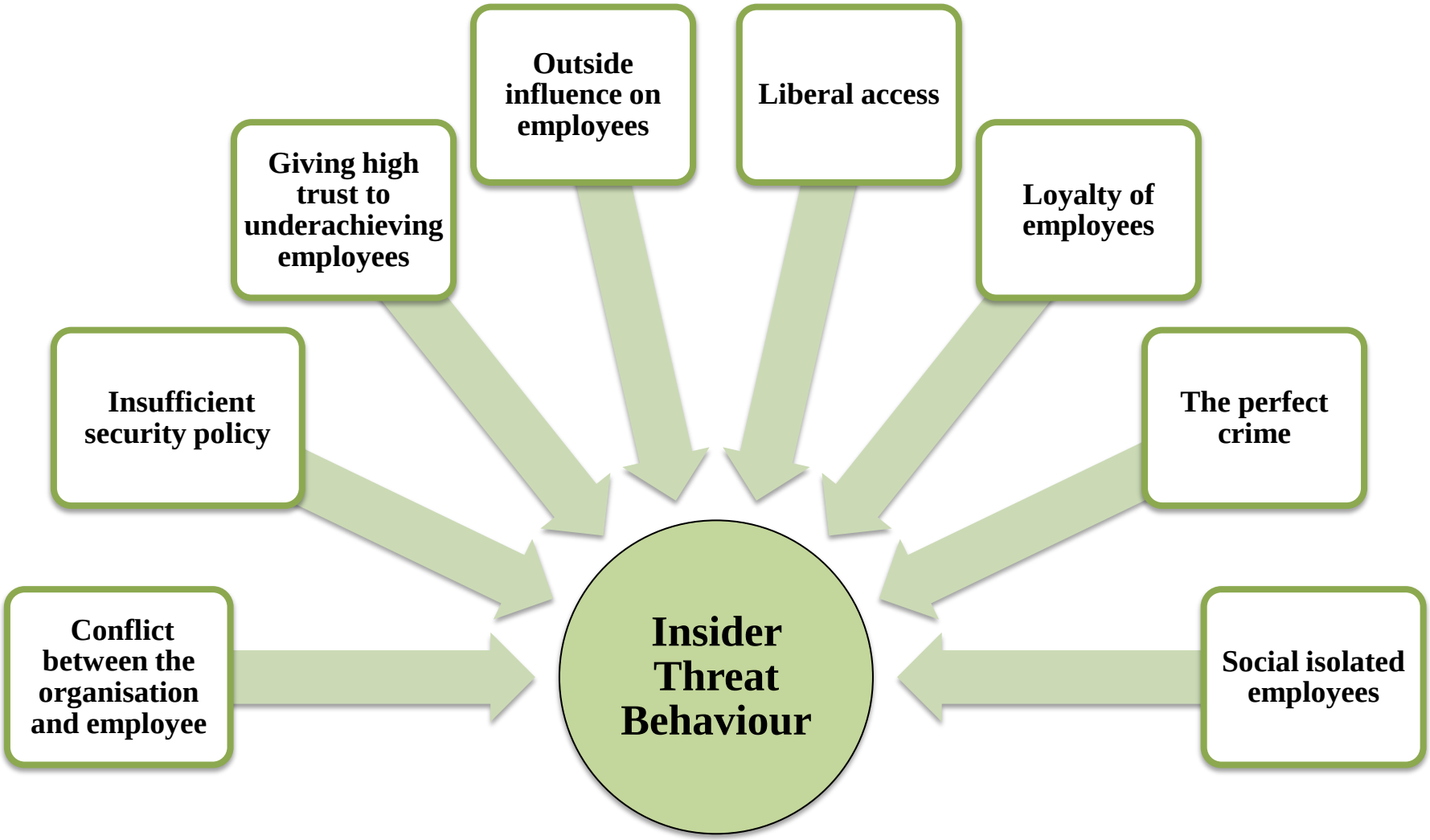


Figure 6.3: HIT model

6.5 Summary

This chapter dealt with the qualitative method and described the evaluation of the enhanced HIT model resulting from the survey responses. In this chapter, the researcher described how the data from the interviews were analysed, and provided a summary of the interviews illustrating the main concepts that reflect the feedback regarding the enhanced HIT model. The purpose of the qualitative method was to evaluate the enhanced HIT model presented in section 5.6 and to confirm the factors identified by the factor analysis. Furthermore, it was used to determine the changes that could further improve the enhanced HIT model. As a result of the interviews, all the suggested factors from the previous phase were confirmed by the participants. The factors that were chosen after careful validation were consolidated into the final HIT model.

The outcome from this phase was the final HIT model which represents a comprehensive set of factors that influence the behaviour of insider threat. The conceptual model provided the groundwork for the following phase of the study. Therefore, the next chapter will outline the development of the best practices to manage the insider threat behaviour based on the factors in the holistic insider threat behaviour model.

CHAPTER SEVEN:
DESIGNING BEST PRACTICES

7.1 Introduction

The previous chapter (Chapter Six) presented the final HIT model which provides the foundation for this phase of the study. This comprehensive model was developed through several stages including the extensive review of the literature (academic sources, IT industry publications and published reports incidents), and quantitative and qualitative data analyses.

This chapter addresses the second research question by describing the management and controls for the factors produced in the final HIT model via the best practices. This chapter presents a list of extra guidelines that complement CERT best practices, which can be used to minimise insider threats. The proposed best practices will be useful in different organisations and for audiences who are aware of organisational security issues such as Chief Information Security Officers (CISOs).These best practices will help CISOs to better manage insider threat behaviour.

7.2 Method Used to Develop the Best Practices

This section discusses the process of developing the best practices to manage insider threat behaviour. Best practices are a set of security measures to manage insider threat behaviour based upon the factors in the HIT model. These measures were developed by combining the CERT best practices for each factor together with other

sources. The researcher followed three steps in order to develop the best practices to manage the eight factors in the final HIT model (figure 6.3). The steps are:

1. Use CERT best practices as an initial baseline
2. Identify any gaps in CERT best practices
3. Supplement these gaps with other sources
    - Interview data
    - Academic sources

CERT generated a list of practices for minimising the insider threat. These guidelines suggest protection measures to help an organisation to mitigate insider risk and enable early detection of the insider attacks. These best practices are used by the researcher as a starting point to develop the best practices to manage the eight factors described in section 5.6. A summary of the CERT best practices are presented in the following section (section 7.2.1). The researcher discusses each of these practices and how they address most of the factors presented in the final HIT model. Although CERT best practices cover most of the factors in the final HIT model, they fail to address several other factors in the model. Thus, CERT best practices will be supplemented with other sources to address these gaps. These sources include the interview data and academic sources.

7.2.1 CERT Best Practices to Minimise the Insider Threat

Carnegie Mellon University's Computer Emergency Response Team CERT outlined significant steps for organisations that could improve their security against insider threats. They generated three reports (Common Sense Guide to Prevention and Detection of Insider Threats) explaining the practices that would help to prevent or detect malicious insider threats. The first version of the Common Sense Guide to Prevention and Detection of Insider Threats was published in 2005. This report was based on the insider threat research performed by CERT, primarily the Insider Threat

Study1 conducted jointly with the U.S. Secret Service. The second version of the report was published in 2006; it contained new and updated practices based on new CERT insider threat research funded by Carnegie Mellon CyLab2 and the U.S. This report includes a new type of analysis of the insider threat problem focused on policies, practices, technology, insider psychological issues, and organisational culture. The third version of the Common Sense Guide was published in 2009 and includes new and updated practices based on an analysis of new cases CERT (2006; 2009). The fourth edition of the Common Sense Guide to Mitigating Insider Threats that includes the latest CERT best practices was published in 2012 and is a result of continued case collection and analysis. In the title of the fourth edition, the words "Prevention and Detection" have been replaced by "Mitigating" since mitigation covers prevention, detection, and response (CERT 2012).

7.2.1.1 PRACTICE 1: Consider threats from insiders and business partners in enterprise-wide risk assessments.

All organisations need to identify and prioritise their critical business assets, the risks to those assets and the associate impact if the assets are compromised; and finally, they use the assessment results to develop or improve the overall approach to securing the organisation's assets. The purpose of risk assessment is to help organisations to assess the insider threat environment, organisational vulnerabilities that enable the threat and possible impacts (including financial, operational and reputational) that could produce insider incidents. In order to develop a good risk assessment procedure, organisations need to include as insiders all employees who have access to the organisation include current or former employees, outsourcing or business partners. Organisations should spot the possible risk posed by their employees' knowledge and access and specifically include that threat as part of their risk assessment.

Insider threats often influence the integrity, availability or confidentiality of organisations' critical data. Employees can affect the integrity of their organisations' data in several ways by, for example, using customer financial information or damaging their employers' websites. They can also violate the confidentiality of the data by stealing trade secrets or private customer information. Moreover, employees can influence the availability of the data by deleting data, sabotaging entire systems and networks, destroying backups and launching other types of denial-of-service attacks.

Risk assessment is essential for all organisations; firstly, they need to determine the critical assets which include financial data, confidential information, intellectual property and critical systems. Secondly, they need to develop a risk management procedure to protect their critical assets from insiders.

Solutions recommended by CERT (2012, 9) are as follows:

- *Conduct a risk assessment of all organisations' systems to identify critical data. Organisations need to ensure that insiders and trusted business partners are part of the assessment.*
- *Have all employees, contractors, and trusted business partners sign nondisclosure agreements upon hiring and termination of employment or contracts.*
- *Background investigations on all employees include trusted business partner and on all acquired employees during a merger or acquisition required, at a level appropriate with the organisations own policy as a contractual obligation.*
- *Prevent sensitive data from being printed if they are not essentially required for business purposes since electronic documents can be easier to track.*
- *Avoid direct access for trusted business partners to organisation's internal network if possible.*

- *Limit access to the system backup process to only administrators.*
- *Implement a clear separation of duties between regular administrators and those responsible for backup and restoration, and prohibit regular administrators' access to system backup media or the electronic backup processes.*
- *Prohibit personal devices in secure areas because they may be used to hide or copy organisation property and data.*
- *Implement data encryption solutions to encrypt data and limit encryption and decryption tools to authorised users.*

7.2.1.2 PRACTICE 2: Clearly document and consistently enforce policies and controls.

Organisations should develop clear, efficient and adequate policies and controls since the development of ambiguous, misleading or inadequate policies can potentially increase the risk of insider threat. All organisations should ensure that their policies and controls are clearly documented and consistently enforced. Moreover, organisations should have fairness policies in place for all employees and provide regular employee training regarding the policies and their justification, implementation, and enforcement. Clearly documented policies and controls can help organisations to avoid employee misunderstandings of the policy that can lead to unmet expectations. Moreover, consistently enforced policies can help organisations to prevent employees feeling that they are being treated differently from other employees. Policies should be clear on several points including the acceptable use of the organisation's assets, ownership of information, performance evaluation including the needs for promotion and bonuses, and processes for handling employee complaints. Every employee inside the organisation should receive a copy of

organisational policies that clearly state what is expected of them and what the consequences are of violations.

Solutions recommended by CERT (2012, 16) are as follows:

- *Ensure that senior management advocates, enforces, and complies with all Organisational policies. Policies that do not have management buy-in will fail and not be enforced equally. Management must also comply with policies. If management does not do so, subordinates will see this as a sign that the policies do not matter or they are being held to a different standard than management. Your organization should consider exceptions to policies in this light as well.*
- *Ensure that management briefs all employees on all policies and procedures. Employees, contractors, and trusted business partners should sign acceptable-use policies upon their hiring and once every year thereafter or when a significant change occurs. This is also an opportunity for your organization and employees, contractors, or trusted business partners to reaffirm any nondisclosure agreements.*
- *Ensure that management makes policies for all departments within your organization easily accessible to all employees. Posting policies on your organisation's internal website can facilitate widespread dissemination of documents and ensure that everyone has the latest copy.*
- *Ensure that management makes annual refresher training for all employees mandatory. Refresher training needs to cover all facets of your organization, not just information security. Training should encompass the following topics: human resources, legal, physical security, and any others of interest. Training can include, but is not limited to, changes to policies, issues that have emerged over the past year, and information security trends.*
- *Ensure that management enforces policies consistently to prevent the appearance of favouritism and injustice. The Human Resources department should have policies and procedures in place that specify the consequences of*

particular policy violations. This will facilitate clear and concise enforcement of policies.

7.2.1.3 PRACTICE 3: Incorporate insider threat awareness into regular security training for all employees.

Security awareness and training is essential for all organisations, since all employees should understand the need for policies, procedures, and technical controls. Employees need to be aware of security policies and procedures and the consequences of any violations. In addition, they need to be aware that some individuals may try to force or persuade them to abuse their organisation. All organisations' employees need to fully understand the security policies and the process for recording policy violations. Likewise, employees should be informed that system activity is monitored, particularly system administration and privileged activity. All employees should be informed about their personal responsibilities such as protection of their own passwords and work products.

All employees need to be aware that insider attacks do occur and can cause serious damage. It is essential for employees to understand that malicious insiders do not fit a specific profile. Their technical skills are varied and could range from minimal to advanced, and they can be from different age groups. Although there is no way to identify the malicious insider through a demographic profile, nevertheless there are ways to identify higher risk employees by their behaviour. Training programs should generate a culture of security suitable for the organisation and include all employees and they should be conducted at least once a year.

Solutions recommended by CERT (2012, 21) are as follows:

- *Develop and implement an enterprise-wide training program that discusses various topics related to insider threat. The training program must have the support of senior management to be effective. Management must be seen participating in the course and must not be exempt from it, which other employees could see as a lack of support and an unequal enforcement of policies.*
- *Train all new employees and contractors in security awareness, including insider threat, before giving them access to any computer system. Make sure to include training for employees who may not need to access computer systems daily, such as janitorial and maintenance staff. These users may require a special training program that covers security scenarios they may encounter, such as social engineering and sensitive documents left out in the open.*
- *Train employees continuously. However, training does not always need to be classroom instruction. Posters, newsletters, alert emails, and brown-bag lunch programs are all effective training methods. Your organization should consider implementing one or more of these programs to increase security awareness.*
- *Establish an anonymous, confidential mechanism for reporting security incidents. Encourage employees to report security issues and consider incentives to reporting by rewarding those who do.*

7.2.1.4 PRACTICE 4: Beginning with the hiring process, monitor and respond to suspicious or disruptive behaviour.

Prospective employees' concerning or suspicious behaviour should be investigated before they are hired; monitoring should also occur in the workplace. This includes

frequent policy violations, serious criminal activity or personal and professional stressors. Organisations should do a better job of screening potential employees. All organisations should perform background checks for all employees, including contractors, to check and evaluate employees according to the information received. Background checks should include examining previous criminal convictions, any credit issue and clarification from previous employers regarding the individual's ability to deal with workplace issues. In addition, this information should be used as part of a risk-based decision process in determining whether or not it is appropriate to give the new employee access to critical, confidential, or proprietary information or systems.

Organisations should train managers to identify and respond to conflict and suspicious behaviour by the employees. It is essential to thoroughly investigate and respond to all violations that are committed. Organisations should consistently monitor their employees, especially those employees with financial struggles or an unexplained increase in finances, since financial gain is the main motivation for many insider thefts or modifications of information.

Policies should consider the reported concerning or suspicious behaviour by co-workers. After suspicious or concerning behaviour is reported, numerous steps could help an organisation to managing the risks of malicious activity. Firstly, the organisation should assess the employee's access to critical information assets and network. Secondly, the organisation should carefully review the logs to examine recent online activity by the employee. When this is done, the organisation should help and provide options to the employee for handling this behaviour, possibly through access to a confidential employee assistance program.

Solutions recommended by CERT (2012, 21) are as follows:

- *Thoroughly background investigation includes a criminal record and credit check.*
- *Encourage employees to report suspicious behaviour to appropriate personnel for further investigation.*
- *Investigate and document all issues of suspicious or disruptive behaviour.*
- *Enforce policies and procedures consistently for all employees.*

7.2.1.5 PRACTICE 5: Anticipate and manage negative issues in the work environment.

The existence of policies alone is not enough. Prospective employees need to be made aware of organisational practices and policies that encompass appropriate workplace behaviour, dress code, working hours, career development and conflict resolution, before the actual day of commencement. Hence, all employees should be aware of the existence of such policies and the consequences and the penalties for violations.

Promotions can have a large influence on the workplace environment, particularly when employees expect promotions but are not given them. If an organisation is not able to offer promotions as expected, managers should notify employees as soon as they know and provide them with an explanation if possible.

Organisations should have an open door policy enabling employees to discuss work-related problems and outside problems including financial and personal stressors with a member of management or human resources, or it could be useful to provide a service such as an employee assistance program (EAP) for employees. Such programs offer confidential counselling that can help employees to restore their work

performance or general wellbeing. These programs exist to minimise employee criminal actions which they may consider as alternative solutions to deal with the financial and personal stressors.

Solutions recommended by CERT (2012, 30) are as follows:

- *Enhance monitoring of employees with an ongoing personnel issue, according to the organisational policy and laws.*
- *Enable additional auditing and monitoring controls outlined in policies and procedures.*
- *Regularly review audit logs to detect activities outside of the employee's normal scope of work.*
- *Limit access to these log files to those with a need to know.*
- *All levels of management must regularly communicate organisational changes to all employees. This allows for a more transparent organisation, and employees can better plan for their future.*

7.2.1.6 PRACTICE 6: Know your assets.

Organisations should be aware of their physical assets as well as their information assets and consider how to secure their most valuable and sensitive information and equipment. Physical assets, such as servers and workstations, are easier to track and protect than information assets. To protect sensitive data assets, organisations must be thoroughly conversant with the types of data they process, where they process it, and where they store it.

Risk assessment is the best way for organisations to understand their assets and protect them from insider attack. Conducting a risk assessment will help an organisation to know about its data types, its system's processes, who uses the data, and where it is stored.

Organisations should know the types of data they process (medical information, personally identifiable information or credit card number), the types of devices that process this data (servers, workstations or mobile devices) and the location where the data is stored, processed, and transmitted (single location, geographically dispersed or foreign countries).

In order to identify critical assets, physical inventories of equipment and the data they house can help organisations either by a service-based technique or hardware-based technique. Some organisations may have a service catalogue that covers the information services an organisation needs to achieve its tasks. A service based inventory *"establishes a hierarchy of assets, starting with a top-level service, branching into the information assets that support it, branching again into the assets that support them, and so on. The organization then inventories the bottom level assets"(CERT 2012, 32).* However, the hardware-based technique does not create a complete inventory. For a hardware-based inventory "*Organisations need to work closely with system administrators to become fully aware of the logical assets contained within each piece of hardware. The organisation should produce a hardware asset hierarchy similar to the software asset inventory, starting with the top-level hardware asset and branching successively"* (CERT 2012, 32).

Once the organisation has identified the critical information assets, and added any unidentified assets, all the inventory information should be summarised and recorded on a spread sheet. In order to determine the priority of assets, the organisation should assign each asset a set of attributes. The attributes should include: environment, security categorisation and criticality.

Solutions recommended by CERT (2012, 34) are as follows:

- *Conduct a physical asset inventory. Identify asset owners' assets and functions. Also identify the type of data on the system.*

- *Understand what data your organization processes by speaking with data owners and users from across the organisation.*
- *Identify and document the software configurations of all assets.*
- *Prioritize assets and data to determine the high-value targets.*

7.2.1.7 PRACTICE 7: Implement strict password and account management policies and practices.

Insiders have an opportunity to compromise computer accounts, even though organisations try to prevent insider attacks. Password and account management policies and practices should apply to employees, contractors, and business partners. Organisations should ensure that all activity from any account is attributable to the person who performed it. Appropriate computer account management with access control will ensure that access to the organisation's critical electronic assets is controlled, and unauthorised access is difficult. In addition to that, the access is recorded and monitored and thus suspicious access can be easily detected and the computer account and the employee associated with that account can be identified. Password policies should enforce strong passwords and ensure that employees change their passwords frequently and do not share their passwords with any person inside or outside the organisation. Moreover, password policies should ensure that all computers automatically perform password-protected screen savers after a fixed period of inactivity. In addition, a reporting mechanism should be available to report attempts of unauthorised account access including social engineering. Daily audits should be carried outto identify and disable unauthorised or expired accounts.

Solutions recommended by CERT (2012, 38) are as follows:

- *Establish account management policies and procedures for all accounts created on all information systems. These policies should address how*

accounts are created, reviewed, and terminated. In addition, the policy should address who authorises the account and what data they can access.

- *Perform audits of account creation and password changes by system administrators.*
- *Define password requirements and train users on creating strong passwords.*
- *Ensure all shared accounts are absolutely necessary and are addressed in a risk management decision.*

7.2.1.8 PRACTICE 8: Enforce separation of duties and least privilege.

Separation of duties and least privilege must be implemented for all organisational tasks to mitigate the insider threat risk. Separation of duties requires dividing tasks between employees to limit the capability that one employee could steal information without the assistance of another. The two-person rule is one type of separation of duties principles that is often used. It requires two employees to perform a task so that it is done effectively. For instance, two bank officers are required to sign large banker's checks, or proof of source code is required before the code is executed. Generally, if an employee collaborates with another to perform a task, this makes them less likely to launch a malicious task.

Sufficient separation of tasks requires implementation of least privilege, allowing employees to access only the resources needed to perform their job. Least privilege is a mechanism that minimises an organisation's risk of confidential or proprietary information theft. Employees are subject to promotions, transfers, relocations, and demotions; thus, organisations need review their employees' required access to information and information systems. An ongoing process is essential to manage the least privilege technique, especially when employees move throughout the

organisation. This helps to monitor the employees' access to information according to their job tasks.

Access control based on separation of duties and least privilege is essential to minimise the insider threat. These principles need to be implemented in both a physical and the virtual manner. Role-based access control generally prevents employees from gaining physical or technical access to resources not required by their work roles. Examples include scientists requiring access to their laboratory space but not requiring access to human resources file cabinets. Similarly, human resources employees require access to staff records but do not require access to laboratory facilities.

Solutions recommended by CERT (2012, 42) are as follows:

- *Carefully audit user access permissions when an employee changes roles within the organisation to avoid privilege creep. In addition, routinely audit user access permissions at least annually. Remove permissions that are no longer needed.*
- *Establish account management policies and procedures.*
- *Require privileged users to have both an administrative account with the minimum necessary privileges to perform their duties and a standard account that is used for every day, non-privileged activities.*
- *Review positions in the organization that handle sensitive information or perform critical functions. Ensure these employees cannot perform these critical functions without oversight and approval. One person should not be permitted to perform both backup and restore functions.*

7.2.1.9 PRACTICE 9: Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.

It is essential that all organisations provide data access control and monitoring in any agreements with cloud service providers. Cloud services help organisations to start up numerous infrastructure devices and services quickly and at low cost by providing data and infrastructure services to the organisation. By using a cloud service, organisations can extend their network perimeter and significantly increase the opportunities for new attacks to be launched including malicious insider attacks. It is important that the same defences the organisations use to secure their data and infrastructure should cover the service provider.

It is essential that all organisations understand how the cloud service provider protects data and assets before entering into any agreement. Before using a cloud service, organisations should assess and understand the service's physical and logical access and security controls. They need to know what measures are in place to mitigate any risks as well as who has access to their data and infrastructure. Moreover, they need to conduct a risk assessment of the data and services that they plan to outsource to a cloud service provider before entering into any agreement. Organisations must check that the cloud service provider poses an acceptable level of risk and has applied mitigating controls to manage the remaining risks. Moreover, it is important that organisations carefully examine all aspects of the cloud service provider to guarantee that the service provider meets the organisation's security practices.

Organisations should regularly audit and monitor a distributed infrastructure's behaviour to ensure that it meets security configuration requirements. Furthermore, organisations need to check the cloud service provider's recruitment policy to make

sure it performs thorough background checks on all prospective employees (operations staff, technical staff, janitorial staff, etc.). Additionally, organisations should ensure that the cloud service provider conduct a periodic credit investigation in order to identify any problem or changes in an employee's life situation which can lead to unacceptable risks.

Solutions recommended by CERT (2012, 47) are as follows:

- *Conduct a risk assessment of the data and services that organization plans to outsource to a cloud service provider before entering into any agreement.*
- *Verify the cloud service provider's hiring practices.*
- *Control or eliminate remote administrative access to hosts providing cloud or virtual services.*
- *Understand how the cloud service provider protects data and other organisational assets before entering into any agreement. Verify the party responsible for restricting logical and physical access to your organisation's cloud assets.*

7.2.1.10 PRACTICE 10: Institute stringent access controls and monitoring policies on privileged users.

System administrators and privileged users such as database administrators have the technical ability and access to perform malicious activity. System administrators and privileged users have a higher access level than other users to systems, networks, or applications. This higher access level is usually associated with higher risk. For example, they can hide their actions since they can log in as other users and modify system log files.

Furthermore, technically skilled employees constitute a significant risk to any organisation. They can use sophisticated methods to carry out their malicious attacks. Examples of such methods include writing or downloading scripts or programs (including logic bombs or password crackers), creating a backdoor account, using remote system administration tools and adjusting system logs.

The following techniques can be implemented by organisations to reduce the damage and promote the detection of malicious system administrator and privileged user actions:

- Separation of duties: Require multiple privileged employees in order to modify critical functions. In other words, network, system and application should be designed, created, executed and enforced by multiple employees.
- Two-man rule for critical system administrator functions: No single employee should be allowable or be technically able to produce changes to any critical functions without action by a second employee. These practices could significantly help to prevent an insider from introducing a logic bomb without this being recognised by another employee.
- Non-repudiation of technical actions: This ensures that online activities taken by any employees including system administrators and privileged users can be attributed to its owner.
- Encryption: Technologies such as encryption can be applied to prevent system administrators and privileged users from reading or modifying sensitive data that is available within their domains but they should not have access to it.
- Disabling accounts upon termination: Organisations should immediately deactivate access for former employees, especially system administrators and technical or privileged users.

Solutions recommended by CERT (2012, 51) are as follows:

- *Conduct periodic account reviews to avoid privilege creep. Employees should have sufficient access rights to perform their everyday duties. When an employee changes roles, the organization should review the employee's account and rescind permissions that the employee no longer needs.*
- *Implement separation of duties for all roles that affect the production system. Require at least two people to perform any action that may alter the system.*

7.2.1.11 PRACTICE 11: Institutionalize system change controls.

Control processes help minimise risks associated with technology use, thereby providing assurance for information and services. Change controls are processes that check the accuracy, integrity, authorisation and documentation of all modifications made to computer and network systems. Many insider cases rely on unauthorised modifications to the organisation's systems; hence, stronger change controls are needed as a mitigation strategy. System administrators or privileged users can install backdoor accounts, keystroke loggers, logic bombs, or other malicious programs on the system or network. Such attacks are sneaky and therefore difficult to detect ahead of time, although the implementation of technical controls can help with early detection. To support this, a baseline for software and hardware configurations should be identified by the organisations. As soon as configurations are identified, hardware and software that makes up those configurations should be characterised. Assessment of current configuration can detect differences by comparing them against the baseline copy and alert managers to take action.

The organisation should describe different roles within the change management process for configuration and validation and allocate them to different employees, which make it difficult for one person to make a change without being noticed by

others. For instance, different employees from the one who made the configuration changes should validate the configuration. Moreover, protecting change logs and backups is very important so that organisations can identify unauthorised changes and restore the system to its previous valid state if required.

Solutions recommended by CERT (2012, 51) are as follows:

- *Periodically review configuration baselines against actual production systems and determine if any discrepancies were approved. If the changes were not approved, verify a business need for the change.*
- *Implement a change management program within the organization. Ensure that a change control board vets all changes to systems, networks, or hardware configurations. All changes must be documented and include a business reason. Proposed changes must be reviewed by information security teams, system owners, data owners, users, and other stakeholders.*
- *The configuration manager must review and submit to the change control board any software developed in-house as well as any planned changes.*

7.2.1.12 PRACTICE 12: Use a log correlation engine or security information and event management (SIEM) system to log, monitor, and audit employee actions.

Logging, monitoring, and auditing can help an organisation to early investigate any suspicious actions by their employees. Auditing refers to the review and verification of logs and data in various networks, systems and applications. However, the logging and auditing of all online activities are not sufficient to protect an organisation's infrastructure from insider threat because of the volume and complexity. Relating events will create more applicable alerts and better informed decisions. To overcome the barriers of volume and complexity, organisations should precisely identify which

of their data are critical. Organisations should consider collecting and correlating some events such as firewall logs, unsuccessful login attempts, intrusion detection systems/intrusion prevention system logs, Web proxies, antivirus alerts and change management. The correlation of events from these devices in many CERTS' cases of insider threat offers valuable information enabling organisations to identify the attacker.

A security information and event management system allows any organisation to monitor their employees' actions continuously, and it allows the organisation to create a baseline level of normal action as well as detect abnormal action. Organisations can use a SIEM system to perform more desirable monitoring of privileged accounts. SIEM system is able to highlight any abnormal actions, such as installing of software or disabling security software. By increasing the monitoring and auditing level for certain actions, records that must be reviewed will be increased as well. However, the SIEM system will facilitate sorting through these events by highlighting those that need further review and discarding background noise.

Organisations should develop monitoring policies before starting any monitoring program, and all organisations' employees should be informed that they are monitored. This is normally achieved through security awareness training provided to employees before using a system.

Solutions recommended by CERT (2012, 59) are as follows:

- *Implement rules within the SIEM system, to automate alerts.*
- *Determine the volume of logs (number of reported events per second) and the needs of the organization before selecting a SIEM tool.*
- *Create a log management policy and procedures. Ensure they address log retention (consult legal counsel for specific requirements), what event logs to collect, and who manages the logging systems.*

- *Ensure that someone regularly monitors the SIEM system. Depending on the environment, this may involve one or more dedicated personnel who monitor employee activity full-time.*

7.2.1.13 PRACTICE 13: Monitor and control remote access from all end points, including mobile devices.

Remote access can help insiders to attack their organisation with less risk. If employees are trained and monitored, and accounts are protected from compromise, the insiders will think twice before compromising the organisation's systems or networks from work. Insiders regularly use legitimate access to attack their organisations remotely. Vigilance is important and recommended when remote access is granted to sensitive data, processes or information systems. Many employees have admitted that it is easier to perform malicious actions remotely or from home, since it reduces the concern that someone could be physically observing the malicious activities. Therefore, organisations need to carefully design and implement remote access policies and procedures. Multiple layers of defence should be in place if an organisation allows remote access. Moreover, organisations should be careful when granting remote access to their employees as they may offer remote access to email and non-critical data; however, they should strongly consider limiting remote access to the most critical data and tasks. Thus, accessing sensitive data that could cause major threat to the organisation should be limited to employees physically located inside the workplace. Remote system administrator access should be limited to the smallest group practicable, if not prohibited overall.

Mobile devices such as PDAs and smartphones have the same ability and capability as a desktop computer. Organisations should be aware of the mobile devices' capabilities and how they are used in the enterprise. The organisation risk assessment should include mobile devices and consider specific items such as cameras,

microphones, remote access, applications, wireless capabilities and huge storage capabilities. Mobile devices can be used to transfer data. Most of the phones have built-in cameras and microphones that could be used to capture sensitive data. These data can be stored on the phone or via email or Multimedia Messaging Service to any other device; moreover, the data can also be synchronised to cloud storage or social media services. Organisations should be aware of smartphone applications that allow remote management of servers, workstations, and network infrastructure devices and who has installed and has access to these applications. It is essential to disable the employee's access to these applications once the employee leaves the organisation.

If remote access to critical and sensitive data and information is considered necessary, the organisation needs to offset the added risk by requiring that connections be made only through organisation devices and closer logging and frequent auditing of remote transactions. If the organisation limits remote access only via their devices, this can improve the organisation's ability to control and monitor access to their information and networks. Organisations should audit and log all remote login information such as login account, date/time connected and disconnected and IP address. Monitoring remote access could be more manageable and effective if authorisation for remote access to critical data is kept to a minimum. Remote access logs, IP addresses and phone records often help to identify employees who launch remote attacks. Disabling remote access is essential for terminated employees. Employee termination processes should include important actions such as retrieving all organisation devices, terminating remote access accounts, disabling all remote management capabilities, changing the passwords of all shared accounts, and closing all open connections.

Solutions recommended by CERT (2012, 64) are as follows:

- *Disable remote access to the organisation's systems when an employee or contractor separates from the organisation. Be sure to disable access to VPN service, application servers, email, network infrastructure devices, and*

remote management software. Be sure to close all open sessions as well. In addition, collect all company-owned equipment, including multifactor authentication tokens, such as RSA SecurID tokens or smart cards.

- *Include mobile devices, with a listing of their features, as part of the enterprise risk assessment.*
- *Prohibit or limit the use of personally owned devices.*
- *Prohibit devices with cameras in sensitive areas.*
- *Implement a central management system for mobile devices.*
- *Monitor and control remote access to the corporate infrastructure.*

7.2.1.14 PRACTICE 14: Develop a comprehensive employee termination procedure.

All organisations need to have a termination policy and procedure that disables all of the departing employee's access points to the organisation's physical locations, networks, systems, applications and data. Disabling access for a terminated employee requires fast action including disabling all employee paths of access including physical and technical access such as computer system accounts, shared passwords, and card control systems. Organisations should retrieve their physical property from the employee as part of the termination process. This property includes badges, access cards, keys, two-factor authentication tokens, mobile devices and laptops. Such items, if not retrieved by the organisation, could enable the former employee to attack the organisation. Collecting these items cannot completely prevent such attacks, but it does mitigate the risk. Moreover, organisations should review the terminated employee's online actions during the 30 days prior to termination. This review should include email activity to guarantee that the employee has not emailed any sensitive data to any parties outside the organisation. The organisation should review the terminated employee's desktop computer and system logs to check that no

software has been installed that can allow the employee back into the organisation's systems. As soon as any employee leaves the organisation, the HR department should inform all other employees about this so as to minimise the possibility of insider threat. If employees do not know about their colleague's departure, they may accidentally release sensitive information to him/her.

Solutions recommended by CERT (2012, 67) are as follows:

- *Develop an enterprise-wide checklist to use when someone separates from the organization.*
- *Establish a process for tracking all accounts assigned to each employee.*
- *Reaffirm all nondisclosure and IP agreements as part of the termination process.*
- *Notify all employees about any employee's departure, where permissible and appropriate.*
- *Archive and block access to all accounts associated with a departed employee.*
- *Collect all of a departing employee's company-owned equipment before the employee leaves the organisation.*
- *Establish a physical-inventory system that tracks all assets issued to an employee.*
- *Conduct an inventory of all information systems and audit the accounts on those systems.*

7.2.1.15 PRACTICE 15: Implement secure backup and recovery processes

Regardless of the all defences implemented by an organisation, employees sometimes can and do launch insider attacks successfully. Thus, implementing and testing secure backup and recovery processes is essential for all organisations.

Backup and recovery policies should consider control access to the facility where the backups are stored and limit access to the physical media. For example, no one employee should have access to both online data and the physical backup media. Moreover, backup policies should include separation of duties and the two-person rule when modifying the backup process.

Multiple copies of backups should exist when possible and stored offsite in a secure facility. Different employees should be responsible for the protection of each copy as it would be difficult for multiple employees to collaborate and compromise the backup copies. Encryption could be an additional level of protection for the backups, especially if the backup copies are managed by a third party vendor at the offsite secure facility. To manage the encryption keys, a two-person rule should be utilised in order to control the decryption process in case one of the employees responsible for backing up the information leaves the organisation.

Solutions recommended by CERT (2012, 71) are as follows:

- *Store backup media off-site. Ensure media is protected from unauthorised access and can only be retrieved by a small number of individuals.*
- *Ensure that configuration of network infrastructure devices (e.g., routers, switches, and firewalls) are part of the organisation's backup and recovery plan as well as the configuration management plan.*
- *Implement a backup and recovery process that involves at least two people: a backup administrator and a restore administrator. Both people should able to perform either role.*
- *Regularly test both backup and recovery processes.*

7.2.1.16 PRACTICE 16: Develop a formalized insider threat program

All organisations should consider the possibility of threat from their employees; thus, they need to pay special attention to insider threats. The trust that organisations give to their employees can expose them to malicious insiders who use specific methods to hide their illegal actions. Any organisation should apply commensurately specialised action in order to effectively detect, prevent, and respond to the threat from insiders. It is essential to develop a process for dealing with insider threats before they occur.

An insider threat program is an established forward-looking program that defines the roles and responsibilities of employees. It is important that all employees participating in the program obtain specific awareness training. The program must have criteria and inceptions for conducting inquiries, referring to investigators, and requesting prosecution. It is essential to control the inquiries by a process that guarantees privacy and confidentiality since the employees involved will be a trusted group involved in monitoring and resolution. Management's support is important if the program is to be successful.

A well-founded insider threat program should include policies and procedures for Human Resources, Legal, Security, Data Owners, Information Technology, Software Engineering, and Contracting. It is important that organisations develop an insider incident response plan to control the harm caused by malicious insiders. Organisations need to differentiate between an incident response plan for insider incidents and a response plan for incidents caused by an external attacker.

Such programs help organisations to detect, prevent, and respond to an insider threat incident. An insider threat program team includes members of different teams from across the organisation and does not need to be a separate, dedicated entity. It is

essential to identify the team member and their roles before an insider incident happens. This team is similar to a standard incident response team in handling the incidents; however the insider threat team responds to the incidents that involve insiders. The organisation needs to reduce the probability that the insider offender will be assigned to the response team or be aware of its progress. This process could be challenging since the same employees allocated to a response team may be among the most likely employees to think about using their technical skills and knowledge against the organisation. The main insider threat team should include at least one member from each of these areas: Physical Security, Personnel Security, Information Assurance, Human Resources and Legal teams as well as someone who is a C-level executive (or equivalent) to lead the insider threat main team.

Solutions recommended by CERT (2012, 81) are as follows:

- *Ensure that legal counsel determines the legal framework the team will work in.*
- *Establish policies and procedures for addressing insider threats that include HR, Legal, Security, management, and IA.*
- *Consider establishing a contract with an outside consulting firm that is capable of providing incident response capabilities for all types of incidents, if the organisation has not yet developed the expertise to conduct a legal, objective, and thorough inquiry.*
- *Formalize an insider threat program that can monitor for and respond to insider threats.*
- *Implement insider threat detection rules into SIEM systems. Review logs on a continuous basis and ensure watch lists are updated.*
- *Ensure the insider threat team meets on a regular basis and maintains a readiness state.*

7.2.1.17 PRACTICE 17: Establish a baseline of normal network device behaviour

Organisations should create a baseline of normal network activity in order to detect irregularities in network activity. The organisation need to choose the data points of interest, how long it will monitor these points to develop a baseline and what tools it will use to collect and store the data. The longer the organisation monitors the chosen data points, the more reliable the baseline will be. The organisation must justify the normal activity points as part of the baseline so that it precisely reflects the organisation's operations. Baseline data points to be monitored include: communications between devices, virtual private network (VPN) users, ports and protocols and normal firewall and IDS alerts.

A network's computers usually need to communicate to only some devices; for example, a computer may need access only to a domain controller, file server, email server and print server. If this computer accesses any other device, it could be either misconfigured or someone could use it for illegal activity. In order to allow only authorised devices to communicate, organisations need to configure host-based firewalls which can prevent malicious insiders from accessing an unauthorised network device.

Organisations should carefully monitor the VPN usage because it permits employees to access organisational networks from outside the organisations. It is important that organisations have policies defining permitted times for network access since monitoring access times or enforcing access policies will support the organisation spot insider action. Organisations should permit VPN connections only from countries where a business need exists. Access controls for VPN are essential; organisations should limit access to file shares on a server to control how data can leave the organisation and they should limit the VPN access to only organisational-

owned devices. In addition, organisations should carefully monitor VPN access for any abnormal activity such as a download of data that exceeds normal usage.

Organisations need to review firewall and IDS logs to identify normal behaviour. A SIEM tool can help security staff to examine the logs and establish a baseline of normal firewall and IDS behaviour. Any changes in the number of alerts might indicate abnormal behaviour and need further investigation.

Solutions recommended by CERT (2012, 85) are as follows:

- *Use network monitoring tools to monitor the network for a period of time to establish a baseline of normal behaviours and trends.*
- *Deny VPN access to foreign countries where a genuine business need does not exist. White list only countries where a genuine business need exists.37*
- *Establish which ports and protocols are needed for normal network activity, and configure devices to use only these services.*
- *Determine which firewall and IDS alerts are normal. Either correct what causes these alerts or document normal ranges and include them in the network baseline documentation.*
- *Establish network activity baselines for individual subunits of the organisation.*
- *Determine which devices on a network need to communicate with others and implement access control lists, host-based firewall rules, and other technologies to limit communications.*
- *Understand VPN user requirements. Limit access to certain hours and monitor bandwidth consumption. Establish which resources will be accessible via VPN and from what remote IP addresses. Alert on anything that is outside normal activity.*

7.2.1.18 PRACTICE 18: Be especially vigilant regarding social media

Insiders who use social media sites can deliberately or accidentally pose a threat to their organisation data and information systems. Training, policies and procedures should be provided by all organisations regarding how all employees, including business partners and contractors, should use social media.

People can share information about themselves with others through social media websites. Such information includes everything about them from birthdays and family members to business affiliations and hobbies. Social media websites such as Facebook and LinkedIn can be used to determine who is employed by a specific organisation. Such websites can also be used to identify who inside an organisation may be more vulnerable or willing to contribute to an insider attack. For instance, if any employee uses a social media website to post any negative comments about his or her work or organisation, attackers may take this as a sign that the employee is dissatisfied and could possibly contribute to any malicious insider activity against the organisation. Attackers can identify people in high-value roles (C-level executives, financial personnel, etc.) by using these Websites to map an organisation's employee structure.

All organisations should have policies and procedures to address what is and is not acceptable employee participation in social media websites. Organisations need to consider what their employees could post even if this information is not deemed harmful. For instance, a social media policy might prohibit the organisation employees from posting any of the organisation's projects or even organisation affiliations since social engineers or competitors could use this information against the organisation.

Every organisation needs to include social media training as part of the organisation's security awareness training program and they need to carefully monitor social media websites.

Solutions recommended by CERT (2012, 89) are as follows:

- *Establish a social media policy that defines acceptable uses of social media and information that should not be discussed online.*
- *Include social media awareness training as part of the organisation's security awareness training program.*
- *Encourage users to report suspicious emails or phone calls to the information security team, who can track these emails to identify any patterns and issue alerts to users.*
- *Consider monitoring the use of social media across the organisation.*

7.2.1.19 PRACTICE 19: Close the doors to unauthorised data exfiltration.

All organisations should know where their information systems are exposed to data exfiltration and implement mitigation strategies. Information systems provide many means of sharing information such as USB flash drives, printers and email. Each sort of device presents unique challenges for preventing data exfiltration. In order to minimise the threat of sensitive information being attacked by any insider, organisations should know where and how data can leave their systems. Since many kinds of technologies could become exit points for data, organisations must be aware of all devices connected to their system as well as all physical and wireless connections to their systems such as Bluetooth, removable media enclave exit points, internet services, printers, fax machines, copiers and scanners.

All organisations should be aware of how their employees use cloud computing services or software as a service. Such services offer another opportunity for data exfiltration. Carefully monitoring and restricting access to these services is important in order to minimise the threat. Monitoring the use of printers, photocopiers, faxes and scanner devices is also important. Organisations could examine audit logs from these devices to discover and respond to any irregularities. All organisations should develop a removable media and data transfer policy and implement technologies to enforce it. Such policy can allow sensitive organisation data to be removed from systems only in a controlled way. Organisations need to restrict and limit data transfer protocols to employees with a reasonable task need, and carefully monitor their use.

Solutions recommended by CERT (2012, 94) are as follows:

- *Establish a cloud computing policy.*
- *Monitor the use of printers, copiers, scanners, and fax machines.*
- *Create a data transfer policy.*
- *Establish a removable media policy.*
- *Restrict data transfer protocols, such as FTP, SFTP, or SCP.*
- *Isolate development networks and disable interconnections to other systems or the internet.*

7.2.2 Relating the CERT Best Practices to the Holistic Insider Threat (HIT) Model

This section explains how the eight factors (described in section 5.6) in the final HIT model are linked to some of the existing CERT best practices. The researcher followed a systematic approach in order to relate the CERT best practices to the factors in the final HIT model presented in figure 6.3. Firstly, keywords were used for each factor to search the CERT best practices document. Relevant occurrences of

each keyword were then used to identify CERT best practices that address each of the factors in the HIT model, at least in part. Secondly, the researcher read the document from cover to cover using the eight factors as a lens to focus the attention.

CERT's best practices addressed most of the factors in the final HIT model. The ways in which the HIT model factors are addressed are described below. However, some aspects of several of the factors have not been covered by the CERT best practices. To propose best practices that fill these gaps, the CERT best practices were supplemented with suggestions collected from interviews and also from other academic sources.

7.2.2.1 Factor 1: Conflict between the organisation and employees

In order to find the CERT best practices relating to the highlighted factor, several search terms were used: 'conflict', 'difference in opinions', 'clash', 'culture clash', 'misperception' and 'lack of communication'. Moreover, the reading using this factor as the lens concludes that CERT best practices provided several recommendations in order to detect and respond to the conflict between organisations and their employees.

CERT recommended monitoring and responding to any suspicious or disruptive behaviour. As discussed in section 7.2.1.4, organisations should frequently monitor their employees' behaviour and train managers to identify and respond to any sort of conflict or suspicious employee behaviour. CERT encourages employees to report suspicious behaviour to appropriate staff and document all issues of conflict or abnormal behaviour, which in turn can help provide a quick response to the conflict and reduce its harm. Furthermore, organisations need to manage negative issues in the work environment immediately. All employees must be aware of workplace behaviour, career development and reason for conflict. In section 7.2.1.5, CERT provides solutions to manage the negative and suspicious behaviour that could

include the conflict. They recommend improved monitoring of employees exhibiting continuing conflict or behaviour problems; improved auditing and monitoring controls; frequent checking of audit logs to discover any actions outside the employee's task scope and restricting access to these log files.

Although, CERT provides some practices to detect and respond to the conflict, they do not offer solutions to prevent the causes. CERT practices overlooked some of the causes of conflict such as culture clashes between the employees, lack of communication, and discrimination. According to Nouman, Khan, and Khan (2011), the most common causes of the conflicts between organisations and their employees are: lack of communication, misperception, difference in opinions and discrimination. Cultural clashes and cultural differences can significantly increase the conflict as employees often see a clash of values as a major cause of conflict (Weinhold and Weinhold 2004; Hayes 2008). In order to address this gap, the researcher used the data from the interviews as well as several academic sources.

Interviewees offered several suggestions to address some of the causes of conflict between organisations and their employees. The researcher observed that most of the participants emphasised that fairness, equality and communication as well as better managers with conflict resolution skills are essential to minimise the causes of conflict within organisations. The following comments are pertinent to this issue:

> *"Organisation should treat their employees equally. They also need to be more open and fair in handling their employee affairs and management. Managers should not be making bias and unfair decisions which in turn can adversely affect the business for the long term. Therefore, managers should receive adequate training on how to handle employee affairs in a correct manner and they should be trained about the consequences of their failures which may include insider threat." (Participant C)*

> *"Organisation should also be training managers of employees or other partners more effectively communicate with employees to handle any sort of conflict." (Participant D)*

Two participants suggest that organisations should listen to their problems and try to help them to solve these problems.

> *"Keep the employees happy. Build with them an air of trust & rapport; keep listening from them through weekly casual social meetings if they are having any rough times or complaints against the organisation." (Participant E)*

> *"One must address conflict and sources of conflict directly. I find that dismissing an employee's concerns even if, leads to further conflict. Listening and attempting to walk the employee through a solution tends to reduce the conflict. That is to say, I ask them to help design a solution to their problem. (How do you think we should fix it?) (Do you feel the only way to solve the problem is doing X?)." (Participant H)*

While interviewees' responses addressed some of the causes of conflict, several academic sources have been used to address the remaining conflict causes. Most of the academic studies emphasised the influence of cultural differences on an organisation and how these may increase the insider threat. Cultural differences usually exist between different communities, nations and geographic regions. According to Ofori-Dankwa and Ricks (2000), organisations need international managers to pay attention to cultural differences between employees. All organisations should acknowledge the differences in culture and pay attention to the significant impact of cultural differences. By thoroughly considering these differences, international managers will possibly acquire a greater understanding of other cultures, act appropriately and reduce the risk of clashes (Ofori-Dankwa and Ricks 2000).

Luo and Shenkar (2011) recommend four principals for managing cultural differences between employees within an organisation, namely communication, acculturation, socialization and staffing; they call this the preparation and regulation of system members.

- Communication is *"a process that increases familiarity between organisational systems and acts as "social glue""(Luo and Shenkar 2011, 8).* It provides a powerful connection among all parts of an organisation. Communication can help to mitigate any culture clash and conflict between employees. For effective communication, language and culture training for both local and foreign employees as well as managers can help improve communication. In order to reduce the possibility of cultural clash, the cultural training must be conducted on a specific region or country basis. Such training will increase knowledge of the other culture more than general culture training. Moreover, cultural mentors can improve this knowledge by correcting the wrongful stereotypes. Efficient cross-cultural communication requires great openness and transparency on the part of all organisations members. Thus, as cross-cultural communications improve, cultural clash will decrease.

- Acculturation is the process of learning about another culture that is both introductory and experiential, thus providing both preparatory and ongoing management. Acculturation involves *"changes induced in systems as a result of the diffusion of cultural elements in both directions. It requires effective adjustment and adaptation to a specific culture".* (Luo and Shenkar 2011, 8). Acculturation training includes three related components: understanding of different culture such as its important values and how cultural values are expressed in behaviour; how to adjust to the different culture; and job performance aspects within the different culture, such as how the culture influences attitudes towards work and formal interaction.

Organisations should take a serious step in order to develop and improve their cultural learning ability including a well-designed process for understanding different cultures. Hence, as cross-country acculturation improves, cultural clash will diminish.

- Socialisation *"at the personal level improves mutual familiarity, social cognition, and understanding of each other's cultural norms and behaviours, thus reducing cultural friction"(Luo and Shenkar 2011, 9).* Socialisation can manage cultural clashes by increasing tolerance, respect and personal trust which help to balance cultural differences. Socialisation at the organisational level increases inter-firm trust, connection and mutual support which remove organisational level cultural clashes. By maintaining socially-embedded relationships, organisations become more culturally familiar with each other. Thus, as cross-cultural socialisation confirms, cultural clash will decrease.

- Staffing is the *"process by which Organisational inputs are selected and regulated to avert head-on cultural collision or to curb the cultural profile of a system where potentially colliding with another*" (Luo and Shenkar 2011, 8). Staffing focuses on employing the right foreign employees, rotation or repatriation, evaluation and rewarding as well as local hiring for management positions, softens the cultural clashes with local employees. Hiring foreign employees who are familiar with the host country culture, norms and language can significantly reduce cultural clashes. In the hiring process, organisations should include international experience, cultural knowledge and relational ability among the important criteria for choosing foreign employees to reduce cultural conflicts with local employees. Meanwhile, recruiting indigenous managers with knowledge of international business practices and the related foreign culture will also be useful in limiting cultural clashes. Although, employing the right foreign employees

who are familiar with the host country culture could minimise culture clash, recruiting local employees will eliminate this issue.

According to Fitzsimmons, Miska, and Stahl (2011), multicultural employees sometimes add value to the organisation, only if the organisations execute the necessary processes to use their skills such as recruiting and selection processes as well as career development practices to employ them in the suitable positions where they can be most useful. They suggested three key tips for managing multicultural employees including staffing, training and development, and organisational culture development.

- Staffing: it is essential that each organisation develop a process to identify multiculturals' potential for both recruiting and placement. Multiculturals should be employed in suitable positions which match their abilities and their skills. Organisations should hire people with a great multicultural background, and place them well in appropriate positions. This process will help to move the organisational culture in the right direction.

- Training and development: Organisations need to apply their training and development programs in order to support multicultural employees to become more aware of their skills and abilities, and to improve monocultural employees' skills. Normally, training multiculturals with monoculturals is more likely to help narrow the gap between them. Mentorship and coaching as well as global experiential programs are best suited to achieving such goals.

- Organisational Culture Development: it is essential that each organisation generate observable signs that the company values employees with a multicultural background, and international experience.

Organisations are at risk if they only attempt to manage the conflict without ascertaining its causes. In order to fill this gap in CERT best practices, the following action is recommended:

- *Managing conflict causes:* Organisations should manage the reasons for the conflict as soon as it appears. Organisations have to treat their employees fairly, equally and take advantage of their multicultural employees through staffing, communication, socialisation and training in order to reduce any cultural problems. If each organisation follows the previous steps, the conflict will definitely be minimised. Consequently, in cases where conflict is not managed properly and there is lack of communication, discrimination and cultural clash, CERT does not provide best practices to minimise this factor contributing to insider threat behaviour.

7.2.2.2 Factor 2: Insufficient information security policy

According to Pramanik, Sankaranarayanan, and Upadhyaya (2004), the implementation of inappropriate information security policy, out-dated security policy and lack of training and awareness were considered essential aspects that can affect the security policies and can lead to insider threat behaviour. To find the best practices fromm the CERT's document related to the highlighted factor, several search terms were utilised: 'policy', 'lack of training and awareness' and 'inappropriate information security policy'. Moreover, the reading using this factor as the lens concludes that CERT best practices provided worthwhile solutions to manage inadequate information security police that covers the essential element of security policy.

CERT recommend enterprise-wide risk assessments to prevent threats from insiders and business partners. It is essential to identify and prioritise the critical business assets, the risks to those assets and the associated impact if the assets are

compromised. Organisations can use the assessment results to develop and improve their security policy and the overall organisations' security. All organisations need to clearly document and consistently enforce policies and controls. As mentioned in section 7.2.1.2, they need to develop clear, efficient and adequate policies and consistently enforced them. In addition, CERT recommended incorporating insider threat awareness into periodic security training for all employees. Section 7.2.1.3 discussed CERT solutions regarding training and awareness; they suggest developing and implementing an enterprise-wide training program which includes numerous topics related to insider threat; before giving new employees access to an organisation's system they need to be trained in security awareness, including insider threat; ongoing training should be offered to all employees and contractors.

Interviewees' responses regarding information security policy support the practices recommended by CERT to manage this factor. Responses were mainly focused on the same aspects that are covered by CERT. Participants suggested the implementation of an adequate information security policy and procedure and updating it as well as providing sufficient training and awareness for all organisations' employees. These solutions can help the organisation a great deal to mitigate the risk of insider threat. The following comments encapsulate these guidelines:

> *"Development of efficient and sufficient security policies and procedures. -Concentration of propriety information on the upper nodes of organisation staff. -Periodic management audit of procedures and policies for effectiveness and practice. -Update of policies after regular intervals. Many things happen in passing year. -Policy & Procedure development by people very much experienced in this area (technical and human sciences)."* (Participant J)

> *"Publish solid policies, and advertise them in ongoing training. Ensure that policies are integrated into the*

organisation. Ensure that routine training is in place that highlights the requirements" (Participant G)

"We need to ensure that security is taken seriously by management and staff and invest adequate time to develop security rules, standards, policy and procedures and to implement proper tools" (Participant I)

Additionally, participants suggested that to minimise this issue, the organisations need to assess their security policies to identify the gaps as highlighted by CERT in Practice 1. The following comments confirm this:

"Conduct a proper IT security risk assessment regularly and implement changes based on the prioritized gaps identified to improve the security policy" (Participant D)

"Industry or service templates: measure what you have, what you don't and seek to fill the gaps. Most don't know what they don't have until it is too late. Far too many are overconfident that what they have will last forever and fail to adapt, update and plan ahead." (Participant K)

Hence, CERT best practices provide good solutions to manage inadequate information security which are also supported by the interviewees. CERT suggest that each organisation should conduct a risk assessment as the first step to developing a strong policy and then clearly document and enforce the policy. There should be regular updates of the organisation policy and periodic security awareness training for all employees.

7.2.2.3 Factor 3: Giving high trust to underachieving employees

Several search terms were used to identify the best practices from the CERT's document relating to the highlighted factor. Keywords included: 'underachieving employees', 'underachiever', 'low performance', 'poor performance' and 'underperforming employee'. Moreover, the reading using this factor as the lens concludes that although CERT best practices provided guidelines to address some of the suspicious or disruptive behaviour, they did not address the issue of underachieving employees.

They suggested several actions to respond to and manage any suspicious or disruptive behaviour beginning with the hiring process, and monitoring and responding to suspicious or disruptive behaviour. As discussed in section 7.2.1.4, all organisations should perform background checks on all employees. Background checks should include clarification from previous employers regarding the individual's ability to deal with workplace matters. Organisations should regularly monitor their employees' behaviour and train managers to identify and respond to any suspicious behaviour by the employees. In section 7.2.1.5, CERT provides guidelines on managing any negative and suspicious behaviour by regularly monitoring the employees with continuing behaviour problems and regularly auditing their logs.

However, useful recommendations have been obtained from the interviews regarding the low performance of the employees. Participants' responses regarding this factor were mainly focused around how the organisation can increase the employees' performance if they are underachieving. The participants believed that organisations need to check the background of the employee before hiring. This process could reveal the employee's attitude towards work.

> *"When we hire, we perform background checks to determine if the individual has any previous employment issues." (Participant F)*

Then they suggested that each organisation should work with their employees to improve their performance by investigating the reasons for their low performance and providing the support required to improve.

> *"I think we need to research the factors causing their underachievement and need to ensure that this employee was given the proper time, tools, and knowledge to do their job. If not, they will easily be underachiever." (Participant I)*

> *"Deal with the employee. Work directly with the employee to improve their work, behaviour or quality of work. This is done, in part, by creating an environment that he/she can thrive. This is dependent on the individual personality and motivations" (Participant H)*

> *"The employee who is underperforming should be warned – at some point the performance is documented and discussed with the employee. The goals of this exercise are two-fold – first we are trying to get the employee to do a better job. Secondly, we are gauging the employee to see if something has changed – has the fit changed – would the organisation be better without this individual. If this process happens consistently and effectively, we can weed-out lower performers and also gauge the risk to our data and services." (Participant F)*

> *"Employing employee individual feedback about themselves coupled with face-to-face assessments will help gauge employee motivators up front before the point of no return is reached." (Participant D)*

Ultimately, if they did not improve their performance, their employment should be terminated.

> *"Underachieving employees should be given an opportunity to increase their performance. Failing that, they should be fired" (Participant G)*

> *"If organisation believes that everything was provided for this person to excel and get ahead and this person didn't have the capacity or motive to do so, he/she should not be employed with the company any longer." (Participant I)*

Furthermore, academic sources have suggested several guidelines to manage employees' low performance. According to Vosloban (2012), organisations need to frequently evaluate the performance for their employees. There are several reasons for organisations to carry out regular individual performance evaluations: rewarding the high performing employees, encouraging the low performing ones, justify decisions to terminate the employees with low or poor performance, offer continuous promotion and development opportunities. In order to encourage employees' performance, organisations need to empower and involve them in different activities. Organisations need to offer benefits and financial incentives to their employees and to reward them according to their productivity (Vosloban 2012; Chandrasekar 2011).

Once low or poor performance has been identified, organisations should immediately investigate the reasons for this low performance (Syauta et al. 2012). Organisations need to explain to the underachieving employees how their performance can influence the organisation's productivity. Finally, organisations need to work with their employees to improve their performance by providing a goal-setting guide. Underperforming employees should be involved in setting meaningful goals and performance measures for their work. These goals should be realistic, achievable and attained within a specific period (Chandrasekar 2011; Syauta et al. 2012).

To sum up, CERT best practices do not address the management of underachieving employees in order to minimise the insider threat behaviour. In order to fill this gap in CERT best practices, the following practices are recommended:

- *Addressing underachieving employees:* Organisations need to manage their underachieving employees in order to reduce the risk of insider attack. All organisations need to frequently evaluate their employees' performance. Once they notice that any of their employees are performing under the required level, they should immediately respond and take some action. Firstly, management should investigate and attempt to find the causes of their low performance and help them to improve by providing a goal setting guide or involving them in different activities such as conferences. If performance does not improve, the employee should be dismissed.

7.2.2.4 Factor 4: Outside influence on employees

A number of keywords were utilised in order to relating CERT best practices to the highlighted factor. These included: 'outside influence', 'external environment', 'employees' background', 'economic motivator', 'outside problems', 'financial stressors' and 'personal stressors'. Moreover, the reading using this factor as the lens concludes that CERT suggested several useful practices to manage this factor.

According to Mathur and Gupta (2012), the influence of the external environment includes factors such as employees' background, values and economic motivators. As discussed in section 7.2.1.4, organisations need to perform thorough background checks for previous criminal convictions or a credit issues. Furthermore, organisations should consistently monitor their employees, especially those struggling financially or a sudden, unexplained financial improvement. Organisations should also allow their employees to discuss outside problems including financial

and personal stressors with a member of management or human resources, or provide a service such as an employee assistance program (EAP) (details in section 7.2.1.5). Moreover, logging, monitoring, and auditing can help an organisation to eliminate outside influence on employees and early investigate any abnormal actions. A security information and event management system allows any organisation to monitor their employee actions regularly in order to reduce any abnormal actions (details in section 7.2.1.12).

Interviewees' responses regarding this factor support the practices recommended by CERT. Participants' comments focused on issues related to background checks and awareness as well as checking and monitoring employees' behaviour and actions.

Comments relating to monitoring and checking employees' activities were among the most discussed solutions for this factor. Participants' comments in regards to monitoring are shown below:

> *"Ideally we eliminate outside influence on employees and human error as much as we can by establish compensating controls to log-audit-report-monitor-etc." (Participant D)*

> *"As security professionals, I need to be much more vigilant and aware of our surroundings, and implement proper processes for frequent monitoring of suspect behaviour and people's activities at work." (Participant I)*

Some participants suggested that background checks for employees can reveal any financial issues that may affect the outside influences exerted on employees. This is illustrated by the following comments:

> *"A thorough background check may help, if there is risk of financial coercion (debts etc)."(Participant C)*

> *"We perform background checks to determine if the individual has any past criminal behaviour, credit issues, or previous employment issues. Through proper interview and screening, we attempt to weed out those who seem to be more concerned with their interests than the organisations" (Participant F)*

Training was also one of the solutions suggested by the participants:

> *"Audit, review, training and making people aware of the security policy help to mitigate the outside influence on employees" (Participant B)*

Other participants offered several suggestions to minimise the effect of outside factors on the employees; these included: paying reasonable wages, providing some flexibility and always supporting them. The following quotations summarised these points well:

> *"• Pay reasonably well. You do not have to be the highest paying employer, but you must pay at least average for the resource and area. Review human resource policy in organisation for bonuses, appreciations and rewards.*
> *• Provide a great deal of flexibility. Allow each person to solve problems with their own skills and creativity. Stifled creativity makes creative people miserable.*
> *• Do not worry about the little things. If the employee needs to be at his/her child's school function, do not worry about getting that time back. Let it go. It causes stress unnecessary stress.*
> *• Back your staff! When pressured from outside the department or from your own management, always support your staff. This is just right and it develops mutual loyalty. Of course, this means support them when they are in the right or have followed the procedures and something still broke." (Participant H)*

To summarise, the main guidelines do manage the outside influence on the employees; both CERT and interview participants suggested that background checks and the monitoring of employee behaviour are essential to minimise the risk of this factor. Background checks can help organisations to discover an individual's previous criminal behaviour or financial problems. In addition, monitoring the employee behaviour and activities in addition to frequent security awareness training for all employees could greatly help an organisation to minimise the incidence of malicious actions. Furthermore, some participants suggested paying reasonable wages; as well as bonuses, appreciations and rewards can minimise the influence on the employee of the prospect of financial gain.

7.2.2.5 Factor 5: Liberal access

To identify the CERT best practices that address the highlighted factor, several keywords were utilised: 'access', 'access control', 'privileges', 'remote access' and 'mobile devices'. Moreover, the reading using this factor as the lens concludes that CERT best practices provided some recommendations in order to manage the employees' access but these practices still did not provide sufficient solutions to address the mobile devices issue.

They suggested that all organisations should identify their physical and information assets and how to secure the most valuable and sensitive information and equipment. A risk assessment will help the organisations to recognise the types of data, who access the data, what their access level and where the data stored (details in section 7.2.1.6). As discussed in section 7.2.1.7, in order to manage insider access, organisations should implement strict password and account management policies. They need to ensure that all activity from any account belongs to the person who performed it. All organisations should establish an appropriate computer account management with access control in order to confirm that access to an organisation's critical assets is controlled and unauthorised access is made difficult. Organisations

also need to define password requirements and train employees on generating robust and strong passwords, in addition to regularly auditing the account and password. Organisations have to enforce separation of duties and least privilege. Separation of duties involves distributing tasks between employees to limit the ability of abusing the system without the assistance of another. Least privilege allows employees to access only the resources needed to perform their job (details in section 7.2.1.8). In addition, organisation should conduct regular account reviews to avoid privilege creep and they need to provide their employees with only necessary access rights to perform their job (details in section 7.2.1.10). The monitoring and control of remote access from all end points, including mobile devices, is also a useful suggestion made by CERT as a means of managing liberal access. As discussed in section 7.2.1.13, organisations must pay more attention when remote access is granted to sensitive data, processes or information systems. All organisations have to design their remote access policies and procedures wisely. CERT recommends that multiple layers of defence be implemented if organisations allow remote access, and limiting remote access to the critical data and tasks. In addition, organisations need to be aware of all sorts of mobile devices, their abilities and how they are used. Organisations should include mobile devices in their risk assessment and consider its specific features such as cameras, remote access, and storage capabilities.

Interviewees' responses regarding this factor support the recommended practices by CERT. Most of the participants suggested that all organisations need to conduct a risk assessment to identify core business assets and the risks to those assets, and establish a risk management strategy for protecting those assets.

> *"Conduct a thorough IT security risk assessment to identify and prioritise core business assets, the risks to those assets, the control gaps associated with those assets and granting the access regarding to this assessment." (Participant D)*

In addition, implementing least access principle is the ideal solution for this problem as well separation of duties and responsibilities must also be in place to reduce this type of risk. Finally, employees should be educated on how to keep the organisation's assets secured. The following quotations summarise these points:

> *"Once anyone employed, grant him the absolute minimum required trust and access but verify. Ensure that you have independent verification and audit of employee access. Most insiders that pilfer information or access systems inappropriately never do anything that would reveal their actions." (Participant H)*

> *"There are a number of controls an organisation can put into place to minimise liberal access risk.*
> - *A solid control framework, focused on the "least access" privilege principle, is an excellent first step to securing access to resources. These resources may be your people, property or information.*
> - *User education and training is another key component for reducing the potential for employees to unintentionally misuse their level of access. Employees should be aware of their roles in keeping information secure, and know how to report potentially suspicious activity like someone gaining inappropriate access to resources.*
> - *Separation of duties and responsibilities must also be in place to reduce this type of risk. Accurately defining a job role and responsibility and then ensuring any corresponding positions have different access will immediately reduce this level of risk" (Participant J)*

Some participants add that access controls and monitoring are also significant in solving the access problem, as shown by the following comments:

> *"Proper access control, regular and random monitoring and verification of access levels and actions taken—trust but verify." (Participant H)*

> *"Proper access authorization should be implemented based on the job functions and should be monitored by proper entitlement review process" (Participant I)*

Although CERT in its fourth best practices edition discussed the mobile devices in practice 13, this practice still did not provide adequate solutions to address the mobile devices issue. This practice only recommends including mobile devices in the organisation's risk assessment. On the other hand, some of the academic sources have suggested more useful ways to manage mobile devices. These sources have been used in order to address this neglected aspect.

Mobile devices with remote access to organisation networks increase the risk of insider threat as stated by Aldhizer and Bowles (2011, 59) *"The proliferation of powerful conventional mobile devices … with remote access to internal networks has raised significant new security concerns".* Mobile devices including laptops, PDAs and smartphones are a crucial element in insider threat behaviour since such devices enable remote access to the organisation network with great storage capabilities. Although mobile devices may increase productivity, new security risks arise by extending the "mobile edge" of the organisation. Mobile devices (PDAs and smartphones) are more vulnerable to penetration and viruses. Even though mobile devices in some situations are important for business needs, there are many tasks that do not require any mobile devices.

Steele and Wargo (2007) suggest managing mobile devices with endpoint security. Endpoint security includes anti-virus, encryptions and data privacy thatrequires a centrally administered solution with sufficient details to determine precisely who is authorised to use devices, what specific devices are acceptable, and how those

devices are used. The sensitive data should be encrypted before it leaves the security perimeter.

Aldhizer and Bowles (2011) recommended two techniques that can help minimise the risk that sensitive stored data on mobile devices may be lost or stolen. Such data can include personally identifiable client information, audit working papers, tax returns and knowledge management data. These techniques include automated wireless security management systems (WSMS) for larger organisations and cost-effective thin computing for smaller organisations.

Automated wireless security management systems (WSMS): large organisations should consider the implementation of an automated WSMS, because the majority of their employees are most likely to use mobile devices to access the internal network applications remotely. To implement such technology, organisations should firstly conduct a feasibility study that includes strategic competitive advantages, business risks, and implementation costs. It is generally conducted as a first step in order to determine whether to allow mobile devices to access the network applications remotely and to implement an automated wireless security solution. Secondly, key stakeholders need to meet in order to reach agreement about the most critical data that need to be protected.

Once critical data within different internal network applications and mobile devices has been identified through a sequence of agreed keyword searches and advanced scanning tools, it will be uniquely tagged. These data should be transferred to dedicated servers where encryption and advanced physical security controls can be applied. In the future, critical data can be automatically tagged once they are created or entered into the organisation's network or mobile devices, and can be automatically moved to suitable dedicated servers. Digital rights management can be used to manage the critical data, whereby the critical tagged data cannot be located in mobile devices and related memory cards, organisational e-mail, or personal e-mail,

instant messaging, the Internet (e.g., the organisational Website, Facebook, LinkedIn, and personal blogs), or printers.

If any employee tries to breach this security procedure by transmitting critical data from the organisation's internal network to a mobile device, the WSMS can automatically terminate the attempt and send an alert to management for direct investigation. Therefore, malicious employees with authorised access to critical data that are available within the internal network will not be able to transfer this data to their mobile devices and selling it.

To further mitigate critical data leakage, large organisations should consider implementing the following WSMS processes:

- Mobile device perimeter security: All mobile devices must have perimeter security controls such as anti-spyware, antivirus software and personal firewalls.
- Device authentication: A record of all appropriately registered and authorised mobile devices is kept to make sure that unauthorised mobile devices will be immediately identified and denied access to the internal network.
- Data encryption: WSMS can automatically force a mobile device to encrypt the data at the point of use.
- Lost or stolen authenticated device protections: In addition to the strong network perimeter security, three automated WSMS controls should be applied to minimise the risk of a lost or stolen mobile: 1) limits on incorrect password guesses; 2) embedded global positioning systems; and 3) limited authorised user access to sensitive data.
- Links to network perimeter security: Before accessing the internal network remotely, the automated WSMS policy server located within the demilitarized zone (DMZ) must be accessed first. At that time, the policy server guides all remote traffic through the network firewall, the intrusion prevention software (anti-spyware and antivirus software) and intrusion

detection software to ensure that it is in compliance with organisational security policies.

- Termination of former employee mobile device and network access: WSMS can automatically deactivate the internal network access through authorised mobile device at the date of termination.
- Third-party access controls: WSMS can also identify any third parties such as outsourced employees. If a recognised third party's mobile device does not meet organisational perimeter security, it can be rejected and not allowed to access the internal network by WSMS. In addition, WSMS sends the third party instructions through e-mail on how to update their security software.

Cost-effective thin computing: small organisations should consider the implementation of cost-effective thin computing to minimise critical data leakage through centralised network control. Small organisations should consider implementing the following automated processes:

- Thin mobile device perimeter security: Thin mobile devices cannot be affected by spyware and viruses since they have little or no operating system and cannot store critical data. On the other hand, such devices can sufficiently access the internal network remotely. Therefore, regular updates to firewalls, anti-spyware and antivirus software can be centralised and monitored at the network level as an alternative to the mobile device level.
- User authentication: Thin computing depends on keeping a record of all authorised employees' user IDs and their complex passwords to make sure that unauthorised employees will be recognized in real time and denied remote access to the internal network.
- Data encryption and lost or stolen device protections: Thin computing can apply central server and data encryption through thin mobile devices. Lost or stolen thin mobile devices are not a major issue since these devices cannot store critical data.

- Termination of former employee's thin mobile device and network access: Thin computing can deactivate the internal network access through a thin mobile device on the date of termination by eliminating the user ID and password from the authorised network listing.
- Third-party access controls: Small organisations that using thin computing could record known third parties' user IDs and complex passwords to make sure that unauthorised third parties can be recognised in real time and denied remote access to the internal network.

Even though CERT best practices provide useful guidelines to manage the access, they do not provide adequate controls to address one of the most important aspects of access which is mobile devices. Therefore, in the absence of security solutions for mobile devices, CERT best practices seem to have missed a significant practice in reducing and preventing insider threat behaviour. In order to fill this gap in CERT best practices, the following practice is recommended:

- *Securing mobile devices:* Organisations must protect all mobile devices. A WSMS solution for larger organisations and a thin computing solution for smaller organisations can help minimise critical data violations through mobile devices.

7.2.2.6 Factor 6: Loyalty of employees

In order to find the best practices from the CERT document relevant to the highlighted factor, several search terms were used: 'loyalty', 'disloyalty', 'loyal employee', 'disloyal employee', 'fair', 'equally', and 'similar'. Moreover, the reading using this factor as the lens concludes that although CERT best practices provide guidelines to address most of the insider threat contributing factors, they did not address the issue of the disloyal employee.

On the other hand, the interviewees added valuable information regarding security management for the highlighted factor. According to Schrag (2001), employee disloyalty weakens organisational productivity and security. Many organisations are concerned about employees' loyalty, especially the loyalty of the outsourced employees and the loyalty of the employees when they are accessing the organisations' network remotely (Bridges and Harrison 2003). Interviewees confirm this and emphasised that employees who access the organisation's network remotely and outsourced employees are more likely to become less loyal to their organisations. Although, CERT best practices address remote access and outsourced employees, they do not consider employee loyalty to be an important factor.
Participants' concerns regarding outsourced employees are shown below:

> *"Outsourcers may steal information. Also outsourced resources are less careful (why should they care?) so thy lees loyal." (Participant E)*

> *"It is the insider that appreciates the value of their compromise; therefore they specifically target an outsourced entity with an offer."(Participant K)*

Some participants declared that accessing the organisations' network remotely could decrease the employee loyalty as noted by the following comments.

> *"It's my gut feeling that somebody who remotely accessing the organisation network would be less loyal and more likely to share data on the internet, or to use the same equipment for internet access, which of course raises the risk." (Participant A)*

> *"Remote access essentially places a layer between their moral code and perceived consequences. Since they are "out of sight, out of mind" they may be more easily motivated to misconduct." (Participant D)*

In order to manage this factor, all participants emphasized that treating employees fairly, equally and with respect will help to increase employee loyalty toward the organisation both if they working remotely or if they are an outsourced employee. The following comments reflect this:

> *"Organisations have to be ensured that an ideal workplace environment is provided to the employees. Employees should be treated fairly and with respect this makes them more comfortable and loyal to the organisation" (Participant A)*

> *"Treating people fairly and similarly (though not necessarily equally) works quite well" (Participant C)*

> *"An organisation that treats employees with respect and dignity will find success in culturing employee loyalty." (Participant D)*

One participant believed that if the top echelon in the organisation is loyal to the employees, this loyalty will be reciprocated:

> *"Loyalty is usually started as a top down issue. If seniors are loyal to the employees, and show that loyalty, then subordinates are more likely to show loyalty back up. If employees are treated poorly, then loyalty up will be very weak" (Participant G)*

Another participant added:

> *"Not only treat each person like they count/matter, but also believe it. Your loyalty to them is required first. You cannot demand loyalty until you are willing to give it." (Participant H)*

To sum up, CERT best practices failed to address the issue of disloyalty of the employee. On the other hand, the interviewees in this study added valuable information to help increase and manage the loyalty of the employees. In order to fill this gap in CERT best practices, the following practice is recommended:

- *Encourage employees' loyalty toward the organisation:* Each organisation has to treat its workers fairly, equitably and respectfully so as to in increase their loyalty to the organisation both if they working remotely or if they are an outsourced employee.

7.2.2.7 Factor 7: The perfect crime

This factor relies on two important elements: the knowledge of the insiders and the level of technical skills. Employees could use their knowledge, ability and technical skills against their organisation. According to Padayachee (2012, 673), *"The insider threat is even more dangerous than external threats, as an insider may easily misuse the skills and knowledge gained through legitimate work duties for illegitimate gain".* In order to discover the relating best practices from the CERT's document to the highlighted factor, several search terms were utilised: 'knowledge of the insider', 'knowledgeable employees', 'technically skilled employees', 'level of technical skills', 'technical skill', 'deterrents', 'sophisticated employee' and 'level of sophistication'. Moreover, the reading using this factor as the lens concludes that CERT best practices provide useful guidelines for managing the perfect crime factor.

CERT best practices suggest that insider threat awareness should be incorporated into periodic security training for all employees. As discussed in section 7.2.1.3, it is essential that employees understand that malicious insiders do not fit a specific profile. Their technical skills are varied and could range from minimal to highly sophisticated, and they are from different age groups. Employees should be informed that system activity is monitored, particularly system administration and privileged activity, and be briefed about the consequences of any breaches. As discussed in

section 7.2.1.10, technically skilled employees create a major risk to any organisations. They can use sophisticated methods to carry out their malicious attack. A number of techniques can be implemented by organisations to reduce the risk of knowledgeable and technically skilled employees. These techniques include: separation of duties, two-man rule for critical system administrator functions, non-repudiation of technical actions, encryption and disabling accounts upon termination. Moreover, CERT recommend using a log correlation engine or security information and event management (SIEM) system to log, monitor, and audit employee actions. Logging, monitoring, and auditing can help an organisation to early investigate any suspicious actions by their employees. Organisations should consider collecting and correlating some events such as firewall logs, unsuccessful login attempts, intrusion detection systems /intrusion prevention system logs, Web proxies, antivirus alerts and change management and use the SIEM system to assist in examining these events (details in section 7.2.1.12).

Interviewees' responses regarding this factor support the practices suggested by CERT. Two participants supported the proposed solutions by CERT in practice 3. They believed that educating and increasing the awareness of organisation's employees is essential to mitigate the perfect crime factor. Employees should be informed that controls are in place and penalties exist for any abusive behaviour:

> *"In many cases, simply educating your staff that controls are in place, and consequences exist, will deter some of the more "opportunistic" behaviour." (Participant J)*

> *"Increase awareness campaigns to help educate users which will positively influence the unintentional inside threat and curtail the intentional inside threat." (Participant G)*

Another participant supports the techniques recommended by CERT in practice 10 in order to minimise the risk of this factor. Referring to a two-man technique, he stated:

> *"Ensure employees are restricted to what they can do in the systems. You may even want to physically separate the Accounts Payable from the Accounts Receivable teams, to reduce the likelihood of collusion. And create a "two-man" rule for major research projects or product launches. Don't simply rely on just one individual – ensure there are others involved in key projects, particularly sensitive projects with a direct impact to the organisation s' wellbeing." (Participant J)*

Organisations need to carefully monitor the employees' actions and behaviour in a random manner as suggested by CERT in practice 12.

> *"The perfect crime could be managed through audit and review without allowing staff to know when and what and randomised checks of controls." (Participant B)*

> *"The perfect crime could be managed by publicised monitoring of employees, followed by actions should employees take inappropriate actions, should reduce the desire to take those actions. Advertise that there is a strong monitoring process. Do not hesitate to take actions against misbehaving employees." (Participant G)*

> *"Inform your staff that monitoring and compliance programs are in place. Layer auditing and control mechanisms into every automated system (i.e. file sharing systems, financial applications). If auditing and logging capabilities are present, enable them and regularly review them for suspicious behaviour will minimise the perfect crime." (Participant J)*

Moreover, interviewees' responses regarding this factor have also added valuable information. The participants emphasised the importance of not sharing all deterrent measures and systems with all employees.

"Security professionals should be careful on utilizing their detection strategies. Detection strategies should only be known and activated by few and should be properly disguised not to draw attention." (Participant I)

"Only the top order employees must have the big picture of the infrastructure. All the rest must have bits and pieces only." (Participant E)

"Not all people need to know all systems. This minimizes the number of people. Major actions that require 2 or more people reduce an individual's ability to act alone." (Participant H)

In summary, CERT and interviewees' responses provided useful practices for managing the main components of the perfect crime factor (insiders' knowledge and technical skills). The suggestions include: security awareness and training, monitoring the employees' actions, auditing employee actions, responding to suspicious activities, enforcing separation of duties and least privilege, paying extra attention to system administrators and technical or privileged users and not to share all deterrents and systems with all employees.

7.2.2.8 Factor 8: Socially isolated employees

To pinpoint the appropriate CERT best practices that address the highlighted factor the following key terms were used: 'isolated employees', 'social frustration' 'working from home', 'isolated areas', 'communication' and 'personal predispositions'. Moreover, the reading using this factor as a lens concludes that while CERT best practices delivered strategies to address suspicious and disruptive behaviour, they failed to address socially isolated employees. Although CERT best practices address working from home as a remote access issue, they do not take this

as a sign of isolation. On the other hand, useful recommendations have been utilised from the interviews regarding this factor.

The participants suggested several solutions to minimise the highlighted factor. Such solutions include connecting socially isolated employees with peers, arranging weekly social gatherings and monitoring the behaviour of those employees, as indicated by the following comments:

> *"Connecting these socially isolated employees with peers is a necessity in my opinion. You may work from home, however, video conferences and voice conferences on a daily basis would help reconnect the isolated worker. Regularly making the isolated worked aware of the expected conduct is also a facilitator to better employee conduct" (Participant D)*

> *"Weekly social gathering (e.g. Breakfast) to add some social spice to the team. And Improve Managers: Train managers (bi-yearly for example) for Team-building, Socialism & Leadership skills (Leading is the best way to Manage)" (Participant E)*

> *"Engaging the workforce on multiple levels is one method of reducing the potential for this type of threat to be realized. Not every employee will engage in every activity, but if employees are valued and they perceive their value to the organisation, the risk of an insider threat being realized will diminish" (Participant J)*

Management should be aware of personal factors such as social frustration and the personal predispositions of their employees and recognise the influence they can have on the organisation. According to some participants, this can be addressed through communication between managers and employees and taking action to prevent employee dissatisfaction when possible. The following quotation expresses this point:

> *"This comes down to a proper management layer – have we thoroughly screened and managed the individual? Are we monitoring their work? Are we meeting with them to see if we can detect any problems, including issues outside of work? Technology isn't the answer for everything – the properly designed and trained Management layer is a critical layer in any comprehensive Information Security program." (Participant F)*

CERT's best practices have missed a significant security solution for socially isolated employees in order to reduce and prevent insider threat. In order to fill this gap in CERT best practices, the following practices are recommended:

- *Handling socially isolated employees:* One of the management solutions to minimise socially isolated employees is to focus on connecting those employees with others in the organisation. This connection could be achieved through periodic meetings or via video or voice conferences for employees who work from home. Additionally, socially isolated employees should be recognised and handled by the manager. This can be achieved through monitoring, communicating and taking action to address employee behaviour.

7.3 Additional Best Practices

In combining the CERT best practices with the best practices presented in the previous section (7.2.1), all the factors that are included in the holistic insider threat behaviour model were covered. The following behavioural and technical best practices and recommendations are provided in response to the eight factors described in section 5.6. This section has addressed the gaps found in CERT best practices and thus illustrates how combining the CERT best practices with those additional practices presented in section 7.2.2 afford greater protections against

insider threat behaviour than CERT alone. This is an original contribution, and provides an answer to the second research question of this study:

> *RQ_2: How can organisations manage the security-abusive behaviour of insiders?*

Additional best practices are:

- ***Managing conflict causes***

As discussed in section 7.2.2.1, organisations should ascertain the reasons for the conflict. Recommended solutions include: fairness, equality, communication and taking advantage of multicultural employees as well as improving management skills with appropriate training so that conflicts can be addressed successfully.

- ***Addressing underachieving employees***

Organisations should manage their low performance employees to mitigate the insider threat as mentioned in section 7.2.2.3. All organisations should regularly evaluate their employees' performance and immediately respond to employees performing under the required level. If any employee becomes an underachiever, the organisation needs to investigate the causes of the low performance and help the employee to improve. Organisations can increase the performance of their employees by using a goal setting guide or involving them in different activities such as conferences.

- ***Securing mobile devices***

Organisations need to secure all mobile devices and should consider it as a crucial element in insider threat behaviour since such devices have great storage capabilities and enable remote access to the organisation's data. Two techniques can help any organisation to minimise the risk that sensitive stored information on mobile devices may be lost or stolen. These include automated wireless security management systems (WSMS) for larger organisations and cost-effective thin computing for

smaller organisations. These two techniques can minimise the critical data violations perpetrated through mobile devices (details in section 7.2.2.5).

- ***Encourage employees' loyalty toward the organisation***

As discussed in section 7.2.2.6, all organisations should treat their employees fairly and equitably and with respect in order to increase employee loyalty.

- ***Handling socially isolated employees***

Organisations need to manage their socially isolated employees in order to minimise the insider threat as mentioned in section 7.2.2.8. Socially isolated employees should be recognised and handled by the managers. This can be done by monitoring, communicating and taking action to address socially isolated employees. Organisations should connect those employees with the others in the organisation. Such connection could be through periodic meetings or via video or voice conferences for employees who are working from home.

Additional best practices have been presented based on the best advice of experienced industry professionals. However, these additional practices should be evaluated in order to truly recommend them. Such a validation might be done by implementing these additional practices as well as CERT best practices in a large multinational organisation and monitoring the usefulness of these additional practices as a means of minimising the insider threat. This evaluation is not within the scope of the current study. However, further research should be done as indicated in section 8.5.

7.4 Summary

This chapter described the management and controls for the factors produced in the final HIT model presented in section 6.5. The best practices were developed through a two-step process: understanding CERT best practices and underling the gaps in it and secondly, using interviewees' suggestions as well as several academic sources to address the gaps found in CERT best practices. Finally, the last section of this chapter presented a list of guidelines that can be used together with CERT best practices to minimise insider threats and to manage the factors in the final HIT model. It will be useful in the future to implement CERT best practices as well as the additional practices provided in this chapter by a large organisation in order to evaluate it.

The next chapter (Chapter Eight) will summarise the research. It will also reveal the research limitations and suggest future research directions.

CHAPTER EIGHT: CONCLUSION, LIMITATIONS AND FUTURE RESEARCH

8.1 Introduction

This chapter presents a summary of this study and provides answers for the research questions posed in Chapter Three. In addition, the theoretical and practical contributions are presented. At the end, the limitations of the study and the future research opportunities are detailed.

8.2 Summary of Research

This researcher studied the factors that influence the insider threat behaviour as identified from three different sources including: academic research, IT industry publications and published reported incidents. In order to develop an integrative model to present the holistic view of the insider threat, all factors that emerged from the three sources were combined. The approach of combining factors from academic research with IT industry publications and published reported incidents factors gave a comprehensive view of insider threat.

A multi-phased mixed method approach comprising both qualitative and quantitative methods was applied to enrich the findings of this study. In the first phase, the literature (which includes academic research, IT industry publications and published reported incidents) was extensively reviewed and analysed and the crucial needed for holistic approach to address all insider threat factors was identified, as none of the

previous models had done so. Once the problem had been diagnosed, the candidate HIT model was developed to combine all factors identified through the literature review.

Then, using the survey method, the candidate insider threat model was evaluated by 100 security specialists with the following job titles: IT Security Manager, Principal Cyber Security Manager, Security Systems Administrator and Senior IT Security . The data collected through Web-based survey and analysed by SPSS. The literature reviewed for this study highlighted the lack of agreement between the three sources on the factors contributing to insider threat. Some sources have strongly supported some factors while other sources have highlighted others. Therefore, the focus of the quantitative phase was to validate the factors identified in the literature. The researcher tested the candidate HIT model through the preliminary analysis of the survey. The preliminary analysis revealed that there is a further debate regarding the factors. Although there is a strong support for some factors, support for other factors was mixed. Therefore, the factor analysis technique was utilized to identify groups of inter-related factors in order to produce a new set of robust factors. The factor analysis offered a new, different list of factors, which is a more consistent interpretation of the data than the original grouping. As a result of this phase, the enhanced HIT model was developed.

The enhanced HIT model resulted from the factor analysis and was evaluated by qualitative method. The researcher interviewed eleven Chief Information Security Officers with at least ten years' experience each. The data for this phase was collected using semi-structured interviews. The recorded data was transcribed and then analysed using the content analysis technique recommended by Miles and Huberman (1994). The data analysis confirmed that the enhanced HIT model contained all the important insider threat contributing factors. The outcome of this phase was the final HIT model which represents a comprehensive set of factors that

influence the behaviour of an employee who could pose an insider threat. This HIT model provided the foundation for the last phase of the study.

The second phase in this study described the management and controls for the factors produced in the final HIT model. The best practices were developed to manage the HIT model's factors through two steps: first, by understanding CERT best practices and underling the gaps in it; and second, by using interviewees' suggestions as well as some academic sources to supplement the gaps found in CERT best practices. At the end of this phase, additional best practices were presented which can be used together with CERT best practices to manage the factors in the final HIT model and minimise the insider threats.

8.3 Answering the Research Questions

This section draws on the results presented in Chapters Six and Seven to answer the research questions presented in Chapter Three. The relationship between objectives, research phases, two research questions and sources of the collected data are presented in Table 8.1.

The first research question is intended to find the factors that contribute to the insider threat.

> *RQ_1: What are the factors that influence the insider to behave inappropriately regard to security?*

The survey and interview revealed that there are eight factors contributing to insider threat behaviour include: conflict between organisation and employee, insufficient security policy, giving high trust to underachieving employees, liberal access, loyalty of employees, the perfect crime and socially isolated employees (details in section 5.6). These factors are rigorous and robust since they were determined by a series of thorough and extensive steps. Moreover, this list of factors is unique since no other

study in the literature to date has offered a comprehensive set of factors contributing to insider threat.

The answer to the first question provides a baseline answer to the second research question.

> *RQ_2: How can organisations manage the security abusive behaviour of insiders?*

To answer this question, it is useful to consider the answer to RQ_1. Once the factors have been identified, it is easy to control and manage the abusive behaviour of insiders through the best practices presented in chapter seven. Chapter Seven (section 7.3) offered five additional best practices to CERT in order to manage and control all the factors in the HIT model. It is recommended that organisations implement the additional best practices with CERT best practices in order to provide greater protection from the insider threat. CERT best practices with the additional practices will incorporate all the essential requirements which are needed by security specialists to mitigate the insider threat.

Table 8.: Relationship between objectives, phases and research questions

Objective	Research questions	Phase of the study	Source of the data
Develop a conceptual insider threat model that can frame a holistic view of insider threat behaviour.	RQ_1: What are the factors that influence the insider to behave inappropriately in regard to security?	Phase 1: Developing a conceptual holistic insider threat model.	- Academic sources, industry publications and published reported incidents. - Web-based survey with 100 security experts with the following job titles: IT Security Manager, Principal Cyber Security Manager, Security Systems Administrator and Senior IT Security. - Semi-structured interviews with 11 Chief Information Security Officers.
Develop a security measures to manage and control the insider threat behaviour.	RQ_2: How can organisations manage the security-abusive behaviour of insiders?	Phase 2: Developing best practices.	- CERT best practices. - Academic sources. - Semi-structured interviews with 11 Chief Information Security Officers.

8.4 Research Significance

This research makes two important contributions: theoretical and practical contributions. In terms of its theoretical significance, this research proposes a new conceptual insider threat model for a holistic view of insider threat behaviour. Moreover, the model is unique in the sense that it has been developed based on data collected from three different literature sources: academic research, IT industry publications and published reported incidents. The significance of this model lies in its understanding of the insider threat factors from a wider perspective instead of single view to ensure that all insider threat factors from different viewpoints were addressed. Thus, the study contributes to the body of knowledge as no previous study from any of the three sources of the literature has proposed a holistic model of the insider threat contributing factors. Another major theoretical contribution is that this holistic model is the first to be thoroughly evaluated by two different methods (quantitative and qualitative) in order to develop a rigorous holistic insider threat model. In addition, the practical contributions of this study are useful for different organisations and for personnel such as the Chief Information Security Officer (CISO) who are aware of organisational security issues. The proposed best practices will manage and minimise the risk of insider threats and increase the awareness of users.

8.5 Research Limitations and Future Direction

Like all studies, this research also has its limitations. However, each limitation and weakness provides an opportunity for future research.

One of the limitations of this study is that the cultural context is restricted to the American culture; this possibly will limit the generalization of the results (Teo, Wei, and Benbasat 2003). However, this absence of generality might not be too much of a drawback because the United States of America is a multicultural country (Fleiner

and Fleiner 2009). Cross-country studies may provide a future direction to the cultural context. A similar study using the same model can be applied to other countries to determine how well the HIT model can be applied in other contexts.

As discussed in section 4.2, one of the limitations of this study is that the HIT model has been evaluated by experienced industry professionals, which is a good means of assessing the model. However, there is a need for further evaluation using real life cases and interviewing the insiders themselves. However, it will require considerable effort to find those insiders. A proposal for future study requires a thorough analysis of a substantial sample of insider threat cases, and data collection could be undertaken by means of in-depth interviews with proven insiders to further verify the existence of these factors and to understand how they work.

Furthermore, the best practices suggested in Chapter Seven have not been evaluated as discussed in section 7.3. However, it will be very useful to validate such practices in order to implement them. In future research, the additional best practices recommended in this study should be tested and evaluated. This evaluation would involve action research case study, implementing the additional best practices and monitoring them to verify their effectiveness in reducing insider threat.

Finally, the comparison with evidence from empirical reported incidents has shown that theoretical academic research has overlooked gender as an important factor, as discussed in section 2.6. Evidence clearly suggests that male gender is a factor in most CERT cases; therefore, further academic investigation in male-gender related issues is needed. However, it must be stressed that such research would need to be mindful of legal constraints, particularly regarding workplace discrimination.

8.6 Summary

This thesis makes a novel contribution to the body of knowledge. It introduces a new, rigorous holistic insider threat model which provides insights into insider threats from a wider perspective. The HIT model enhances our understanding of the insider threat issue and provides an overview of the main factors contributing to insider threat. The transferability of this research was established by rich description and reporting of the research phases and process. The researcher has taken several steps to ensure the research validity and reliability of this study. Following the qualitative method approach, the researcher used several tips to avoid common method bias (details in section 5.2.5). Moreover, Cronbach's alpha coefficient was calculated to determine whether the items in a scale were assessing the same construct. Moreover, the researcher used semi-structured interviews with open-ended questions. All interviews were carefully transcribed so that respondents' words accurately expressed their thoughts, with continuous checking of the data to compare meanings. Furthermore, theory saturation was achieved as the data became redundant (details in section 6.2.4).

Most importantly, this thesis has provided recommendations on ways to manage and control these contributing factors in the HIT model by introducing an additional set of best practices which can be used in addition to CERT best practices to provide a better defence against insider threat. It is expected that the implementation of these additional best practices will support the management and control of internal risk, thereby minimising the likelihood of insider threat.

REFERENCES

Addressing the Insider Threat. 2007. *Community Banker*, 14-14.

Albrechtsen, Eirik, and Jan Hovden. 2010. "Improving Information Security Awareness and Behaviour through Dialogue, Participation and Collective Reflection. An Intervention Study." *Computers & Security* 29 (4): 432-445.

Aldhizer, George R., III, and John R. Bowles, Jr. 2011. "Mitigating the Growing Threat to Sensitive Data: 21st Century Mobile Devices." *The CPA Journal* 81 (5): 58-63.

Alhija, F. A. N. 2010. "Factor Analysis: An Overview and Some Contemporary Advances." In *International Encyclopedia of Education (Third Edition)*, eds Peterson Editors-in-Chief: Penelope, Baker Eva, Eva Baker Barry McGawA2 - Editors-in-Chief: Penelope Peterson and McGaw Barry, 162-170. Oxford: Elsevier.

Althebyan, Qutaibah , and Brajendra 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.

Althebyan, Qutaibah, and Brajendra 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*, eds Sushil Jajodia, Pierangela Samarati and Stelvio Cimato, 557-571. Springer Boston.

Anderson, James. 1980. *Computer Security Threat Monitoring and Surveillance*.

Anderson, Robert H, Thomas Bozek, Tom Longstaff, Wayne Meitzler, Michael Skroch, and Ken Van Wyk. 2000. "Research on Mitigating the Insider Threat to Information Systems." In *In Proceedings of a Workshop Held August 2000, Monica, USA*, 1-132. RAND Corporation.

Ansanelli, Joseph. 2005. Are Employees the Biggest Threat to Network Security? Yes. *Network World*, 56-56.

Ashenden, Debi. 2008. "Information Security Management: A Human Challenge?" *Information Security Technical Report* 13 (4): 195-201.

Assessing the Seriousness of Security Threats from Employee Misuse of It Resources. 2009. *Computer Economics Report*, 18-20.

Band, Stephen , Dawn M. Cappelli, Lynn Fischer, Andrew Moore, Eric D. Shaw, and Randall Trzeciak. 2006. *Comparing Insider It Sabotage and Espionage: A Model-Based Analysis*. CERT.

Bartlett, M. 1954. "A Note on the Multiplying Factors for Various Chi Square Approximations." *Journal of the Royal Statistical Society* 16 (Series B): 8-296.

Bauch, Brad. 2011. The Real Cyber Threat Facing Utilities. *Power Engineering International*, 16-18.

Bellovin, Steven M. 2008. *The Insider Attack Problem Nature and Scope*. Edited by Salvatore J. Stolfo, Steven M. Bellovin, Angelos D. Keromytis, Shlomo Hershkop, Sean W. Smith and Sara Sinclair. Vol. 39, *Insider Attack and Cyber Security*: Springer US.

Berg, Bruce L, and Howard Lune. 2011. *Qualitative Research Methods for the Social Sciences*. 8th ed. Upper Saddle River, NJ: PEARSON

Bertrand, Catherine, and Laurent Bourdeau. 2010. Research Interviews by Skype: A New Data Collection Method *Proceedings of the 9 th European Conference on Research Methodology for Business and Management Studies*,

Besnard, Denis , and Budi Arief. 2004. "Computer Security Impaired by Legitimate Users." *Computers & Security* 23 (3): 253-264.

Bhilare, Dattatraya, S, Ashwini Ramani, K, and Sanjay Tanwani, K. 2009. "Protecting Intellectual Property and Sensitive Information in Academic Campuses from Trusted Insiders: Leveraging Active Directory." In *Proceedings of the 37th annual ACM SIGUCCS fall conference, St. Louis, Missouri, USA*. ACM. doi: 10.1145/1629501.1629520.

Bishop, Matt. 2005. "Panel: The Insider Problem Revisited." In *In Proceedings of the 2005 workshop on New security paradigms, Lake Arrowhead, USA*, 75-76.

Bishop, Matt , Sophie Engle, Sean Peisert, Sean Whalen, and Carrie 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.*, 1-12.

Bishop, Matt, Sophie Engle, DeborahA Frincke, Carrie Gates, FrankL Greitzer, Sean Peisert, and Sean Whalen. 2010. "A Risk Management Approach to the "Insider Threat"." In *Insider Threats in Cyber Security*, eds Christian W. Probst, Jeffrey Hunker, Dieter Gollmann and Matt Bishop, 115-137. Springer US.

Blackwell, Clive. 2009. "Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies." In *Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence, Knoxville, USA* 40-44. ACM.

Blackwell, Clive. 2012. "A Forensic Framework for Incident Analysis Applied to the Insider Threat." In *Digital Forensics and Cyber Crime*, eds Pavel Gladyshev and MarcusK Rogers, 268-281. Springer Berlin Heidelberg.

Blades, Marleah. 2010. The Insider Threat. *Security Technology Executive*, 32-37.

Bloombecker, J 1984. Introduction to Computer Crime *In Computer Security: a Global Challenge North-Holland, Amsterdam*: Elsevier Science Publishers.

Boas, Taylor C, and F Daniel Hidalgo. 2013. "Fielding Complex Online Surveys Using Rapache and Qualtrics." *The Political Methodologist* 20 (2): 21-26.

Bolderston, Amanda. 2012. "Conducting a Research Interview." *Journal of Medical Imaging and Radiation Sciences* 43 (1): 66-76.

Bond, Sue. 2004. "Organisational Culture and Work-Life Conflict in the Uk." *The International Journal of Sociology and Social Policy* 24 (12): 1-24.

Brackney, Richard, and Robert H Anderson. 2004. "Understanding the Insider Threat." In *March 2004 Workshop, Santa Monica, CA, USA*. RAND Corporation.

Bradbury, Danny. 2011. "Data Mining with Linkedin." *Computer Fraud & Security* 2011 (10): 5-8.

Brdiczka, Oliver , Juan Liu, Bob Price, Jianqiang Shen, Akshay Patil, Richard Chow, Eugene Bart, and Nicolas Ducheneaut. 2012. "Proactive Insider Threat Detection through Graph Learning and Psychological Context." In *Security and Privacy Workshops (SPW), 2012 IEEE Symposium on San Francisco*, 142 - 149 IEEE.

Bridges, Sheri, and J. Kline Harrison. 2003. "Employee Perceptions of Stakeholder Focus and Commitment to the Organization." *Journal of Managerial Issues* 15 (4): 498-509.

Bucki, James 2011. Top 6 Outsourcing Disadvantages. Accessed 14 NOV, http://operationstech.about.com/od/outsourcing/tp/OutSrcDisadv.htm.

Buckley, Rob. 2010. Can You Ever Be Wholly Leakproof? *SC Magazine: For IT Security Professionals*, 32-37.

Butts, J.W., R.F. Mills, and R.O. Baldwin. 2005. "Developing an Insider Threat Model Using Functional Decomposition." In *In Proceedings of the Third international workshop on mathematical methods, models, and architectures for computer network security, Petersburg, Russia*, 412-417.

Calandrino, Joseph A. , Steven J. McKinney, and Frederick T. Sheldon. 2007. "Detection of Undesirable Insider Behavior." In *Cyber Security and Information Intelligence Research Workshop (CSIIRW),*.

Canavan, Sorcha. 2007. Information Security Policy - a Development Guide for Large and Small Companies. *Information Security Reading Room*: 1-43,

Cappelli, Dawn , Andrew Moore, and Randall Trzeciak. 2012. *The Cert Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud) Series in Software Engineering*. Upper Saddle River, NJ: Addision- Wesaley.

Cappelli, Dawn, Thomas Caron, Randall Trzeciak, and Andrew Moore. 2008. *Spotlight On: Programming Techniques Used as an Insider Attack Tool*. CERT Program and Software Engineering Institute.

Carroll, M.D. 2006. "Information Security: Examining and Managing the Insider Threat." In *In Proceedings of the 3rd annual conference on Information security curriculum development,, Kennesaw, Georgia (USA)*, 156 - 158.

Casali, Gian Luca B. B. A. M. B. A., and Gary E. Dhsm M. H. M. R. N. E. M. Fchse Day. 2010. "Treating an Unhealthy Organisational Culture: The Implications of the Bundaberg Hospital Inquiry for Managerial Ethical Decision Making." *Australian Health Review* 34 (1): 73-9.

Castle, Ian. 2009. "Beware the Enemy Within." *SC Magazine: For IT Security Professionals* 17-17

Cavana, Robert Y. , Brian L. Delahaye, and Uma Sekaran. 2001. *Applied Business Research: Qualitative and Quantitative Method*: John Wiley & Sons Australia Limited.

CERT, Computer Emergency Readiness Team. 2006. *Common Sense Guide to Prevention and Detection of Insider Threats 2nd Edition* CERT® Program.

CERT, Computer Emergency Readiness Team. 2009. *Common Sense Guide to Prevention and Detection of Insider Threats 3rd Edition* CERT® Program.

CERT, Computer Emergency Readiness Team. 2012. *Common Sense Guide to Mitigating Insider Threats 4th Edition*. CERT® Program.

Chandrasekar, K. 2011. "Workplace Environment and Its Impact on Organisational Performance in Public Sector Organisations." *International Journal of Enterprise Computing and Business Systems* 1 (1): 1-19.

Chickowski, Ericka. 2009. Insider Security Events Mostly Unintentional. *Channel Insider*, 1-2.

Chinchani, Ramkumar , Anusha Iyer, Hung Ngo, and Shambhu Upadhyaya. 2005 "Towards a Theory of Insider Threat Assessment." In *IEEE International Conference, Washington, DC*, 1-10. IEEE Computer Society

Chomeya, Rungson 2010. "Quality of Psychology Test between Likert Scale 5 and 6 Points." *Journal of Social Sciences* 6 (3): 399-403.

Cohen, Fred. 2001. "The New Cyber Gang -- a Real Threat Profile." *Network Security* 2001 (5): 15-17.

Cole, Eric 2008. *Correlating Sim Information to Detect Insider Threats a Sans Whitepaper* http://www.sans.org/reading_room/analysts_program/SIMInfo_June07.pdf.

Cole, Eric, and Sandra Ring. 2005. *Insider Threat: Protecting the Enterprise from Sabotage, Spying, and Theft*. 1st ed: Syngress. (accessed December 1, 2010)

Colwill, Carl. 2009. "Human Factors in Information Security: The Insider Threat - Who Can You Trust These Days?" *Information Security Technical Report* 14 (4): 186-196.

Contos, Brian. 2007. "Insider Threat Monitoring Is Enhanced by Asset Relevance." *Infosecurity* 4 (2): 47-47.

Conway, James M, and Charles E Lance. 2010. "What Reviewers Should Expect from Authors Regarding Common Method Bias in Organizational Research." *Journal of Business and Psychology* 25 (3): 325-334.

Cooper, D. R., and P. S Schindler. 1998. *Business Research Method*. 6th ed. Boston: Irwin/McGraw-Hill.

Cormack, D.S. 1991. *The Research Process*. Oxford Black Scientific.

Cote, Joseph A, and M Ronald Buckley. 1987. "Estimating Trait, Method, and Error Variance: Generalizing across 70 Construct Validation Studies." *Journal of Marketing Research* 24 (3): 315-318.

Creswell, J. W. 2008. *Educational Research: Planning, Conducting, and Evaluating Quantitative and Qualitative Research*. 3rd ed. Upper Saddle River, NJ: Pearson/Merrill Prentice Hall.

Creswell, J. W. 1994. *Research Design Qualitative and Quantitative Approaches*. Thousand Oaks, CA: SAGE Publications.

Creswell, J. W. 2003. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* 2nd ed. Thousand Oaks, CA: SAGE Publications.

Creswell, John W, and Vicki L Plano Clark. 2007. *Designing and Conducting Mixed Methods Research*. Thousand Oaks, CA: Wiley Online Library.

Crinson, Iain. 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.

Cronbach, Lee J. 1951. "Coefficient Alpha and the Internal Structure of Tests." *Psychometrika* 16 (3): 297-334.

Crossler, Robert E., Allen C. Johnston, Paul Benjamin Lowry, Qing Hu, Merrill Warkentin, and Richard Baskerville. 2013. "Future Directions for Behavioral Information Security Research." *Computers & Security* 32 (0): 90-101.

Cummings, Adam , Todd Lewellen, David McIntire, Andrew Moore, and Randall Trzeciak. 2012. *Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector*. CERT® Program.

D'Arcy, John, and Anat Hovav. 2007. Deterring Internal Information Systems Misuse. *Communications of the ACM* 113-117.

Da Veiga, A., and J. H. P. Eloff. 2010. "A Framework and Assessment Instrument for Information Security Culture." *Computers & Security* 29 (2): 196-207.

Dallaway, Eleanor. 2008. "You're Only Human." *Infosecurity* 5 (6): 7-7.

Data Insecurity—Is Not Knowing the Cause Part of Your Problem? 2008. *Security Director's Report*, 4-6.

Dearnley, Christine. 2005. "A Reflection on the Use of Semi-Structured Interviews." *Nurse Researcher* 13 (1): 19-28.

Donaldson, S. I. , and E. J Grant-Vallone. 2002. "Understanding Self-Report Bias in Organizational Behavior Research." *ournal of Business and Psychology* 17 (2): 245-260.

Egan, Jennifer, Lesley Chenoweth, and Donna McAuliffe. 2006. "Email-Facilitated Qualitative Interviews with Traumatic Brain Injury Survivors: A New and Accessible Method." *Brain Injury* 20 (12): 1283-1294.

Financial Institution Security Risks and Concerns: The Top Eight. 2007. *TellerVision*, 1-3.

Fink, A. 2010. "Survey Research Methods." In *International Encyclopedia of Education*, 152-160. Oxford: Elsevier.

Fitzsimmons, Stacey R., Christof Miska, and Günter K. Stahl. 2011. "Multicultural Employees: Global Business' Untapped Resource." *Organizational Dynamics* 40 (3): 199-206.

Fleiner, Thomas , and Lidija R. Basta Fleiner. 2009. "The Multicultural State: The Challenge of the Future." In *Constitutional Democracy in a Multicultural and Globalised World*, 511-650. Springer Berlin Heidelberg.

Fontana, Andre, and James H. Frey. 1994. *The Art of Science., Handbook of Qualitative Research*. London Sage Publication.

Ford, Jason. 2012. Mitigating the Threat of Cyber Crime through Security. *The Engineer (Online).*

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

Furnell, Steven. 2004. "Enemies Within: The Problem of Insider Attacks." *Computer Fraud & Security* 2004 (7): 6-11.

Furnell, Steven. 2006. "Malicious or Misinformed? Exploring a Contributor to the Insider Threat." *Computer Fraud & Security* 2006 (9): 8-12.

Fyffe, George. 2008. "Addressing the Insider Threat." *Network Security* 2008 (3): 11-14.

Gabrielson, Bruce 2006. "Solving the Insider Threat Problem." In *the University of Louisville Cyber Securitys Day, October 2006, Louisville, Kentucky, United States*.

Gafny, Ma'ayan, Asaf Shabtai, Lior Rokach, and Yuval Elovici. 2010. "Detecting Data Misuse by Applying Context-Based Data Linkage." In *Proceedings of the 2010 ACM workshop on Insider threats, Chicago, Illinois, USA*. ACM.

Gaunt, Nick. 1998. "Installing an Appropriate Information Security Policy." *International Journal of Medical Informatics* 49 (1): 131-134.

Gely, R., and L. Bierman. 2006. "Social Isolation and American Workers: Employee Blogging and Legal Reform." *U of Cincinnati Public Law Research Paper*.

Gibson, Lucy 2010. "Using Email Interviews." *Research method* 1-7.

Golafshani, Nahid. 2003. "Understanding Reliability and Validity in Qualitative Research." *The qualitative report* 8 (4): 597-607.

Gonzalez, Jose , and Agata Sawicka. 2002. "A Framework for Human Factors in Information Security." In *2002 WSEAS Int. Conf. on Information Security, Rio de Janeiro, Brazil*.

Gordon, Jeffry S., and Ryan McNew. 2008. "Developing the Online Survey." *Nursing Clinics of North America* 43 (4): 605-619.

Griffin, J. 2009. Stopping Cyber Attacks. *Security Technology Executive*, 10.

Guo, Ken H. 2013. "Security-Related Behavior in Using Information Systems in the Workplace: A Review and Synthesis." *Computers & Security* 32 (0): 242-251.

Hair, Joseph, W Black, B Babin, and R Anderson. 2010. *Multivariate Data Analysis: A Global Perspective*. 7th ed. Upper Saddle River, NJ: Prentice Education, Inc.

Hanley, Michael, Tyler Dean, Will Schroeder, Matt Houy, Randall Trzeciak, and Joji Montelibano. 2011. *An Analysis of Technical Observations in Insider Theft of Intellectual Property Cases*. CERT.

Hanley, Michael, Andrew Moore, Dawn Cappelli, and Randall Trzeciak. 2009. *Spotlight On: Malicious Insiders with Ties to the Internet Underground Community*.

Hanna, Paul. 2012. "Using Internet Technologies (Such as Skype) as a Research Medium: A Research Note." *Qualitative Research Journal* 12 (2): 239-244.

Hayden, MICHAEL 1999. *The Insider Threat to U. S. Government Information Systems*.

Hayes, Jeff 2008. *Workplace Conflict. And How Businesses Can. Harness It to Thrive.*: CPP Global Human Capital Report.

Hitchings, J 1995. "Deficiencies of the Traditional Approach to Information Security and the Requirements for a New Methodology." *Computers & Security* 14 (5): 377–383.

Ho, Shuyuan Mary. 2008. "Behavorial Parameters of Trustworthiness for Countering Insider Threats." In *The Third Annual iConference*.

Holmlund, Lynn , Daniel Mucisko, Richard Lynch, and Joseph Freyre. 2011. *2011 Cybersecurity Watch Survey: Organizations Need More Skilled Cyber Professionals to Stay Secure*: CSO, the U.S. Secret Service, the Software Engineering Institute CERT Program at Carnegie Mellon University and Deloitte.

How to Weed out the New Insider Cybersecurity Threat. 2007. *Security Director's Report*, 1-12.

Hu, Ning , Phillip G Bradford, and Jun Liu. 2006. Applying Role Based Access Control and Genetic Algorithms to Insider Threat Detection. *Proceedings of the 44th Annual ACM Southeast Regional Conference (ACM-SE), New York, USA*: ACM.

Hu, Qing , Tamara Dinev, Paul Hart, and Donna Cooke. 2012. "Managing Employee Compliance with Information Security Policies: The Critical Role of Top Anagement and Organizational Culture." *Decision Sciences* 43 (4).

Hu, Qing, Zhengchuan Xu, Tamara Dinev, and Hong Ling. 2011. Does Deterrence Work in Reducing Information Security Policy Abuse by Employees? *Communications of the ACM* 54-60.

Hu, Yi, and Brajendra Panda. 2009. "A Traceability Link Mining Approach for Identifying Insider Threats." In *Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies, Oak Ridge, Tennessee*, 40-44. ACM.

Hunker, Jeffrey. 2008. "Taking Stock and Looking Forward – an Outsider's Perspective on the Insider Threat." In *Insider Attack and Cyber Security*, eds Salvatore J. Stolfo, Steven M. Bellovin, Angelos D. Keromytis, Shlomo Hershkop, Sean W. Smith and Sara Sinclair, 195-214. Springer US.

Hussey, Jill, and Roger Hussey. 1997. *Business Research: A Practical Guide for Undergraduate and Postgraduate Students*. London: Macmillan.

Huth, CarlyL, DavidW Chadwick, WilliamR Claycomb, and Ilsun You. 2013. "Guest Editorial: A Brief Overview of Data Leakage and Insider Threats." *Information Systems Frontiers* 15 (1): 1-4.

Ivankova, Nataliya V, John W Creswell, and Sheldon L Stick. 2006. "Using Mixed-Methods Sequential Explanatory Design: From Theory to Practice." *Field Methods* 18 (1): 3-20.

Jaikumar, Vijayan. 2005. Insider Threats Mount. *Computerworld*, 12.

Johnson, R Burke, and Anthony J Onwuegbuzie. 2004. "Mixed Methods Research: A Research Paradigm Whose Time Has Come." *Educational researcher* 33 (7): 14-26.

Jones, Andy. 2008a. "Catching the Malicious Insider." *Information Security Technical Report* 13 (4): 220-224.

Jones, Andy. 2008b. "The Evolution of Attack." *Infosecurity* 5 (3): 30-31.

Joseph, Kodjo. 2009. "The Influence of Organizational Culture on Organizational Learning, Worker Involvement and Worker Productivity." *International Journal of Business and Management* 4 (9): 243-250.

Kaiser, H. 1974. "An Index of Factorial Simplicity." *Psychometrika* 39: 6-31.

Karyda, Maria, Evangelos Kiountouzis, and Spyros Kokolakis. 2005. "Information Systems Security Policies: A Contextual Perspective." *Computers & Security* 24 (3): 246-260.

Keeney, Michelle , Dawn Cappelli, Eileen Kowalski, Andrew Moore, Timothy Shimeall, and Stephanie Rogers. 2005a. *Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors*.

Keeney, Michelle , Eileen Kowalski, Dawn Cappelli, Andrew Moore, Timothy Shimeall, and Stephanie Rogers. 2005b. *Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors*. Washington, DC.

Kemp, Mike. 2005. "Barbarians inside the Gates: Addressing Internal Security Threats." *Network Security* 2005 (6): 11-13.

Khanna, Poonam. 2005. The inside Job Is the Real Threat. *Computing Canada*, 16-17.

King, Chris 2012. *Spotlight On: Malicious Insiders and Organized Crime Activity*. CERT.

Kirkpatrick, Shelley A. 2008. Refining Insider Threat Profiles. *Security: Solutions for Enterprise Security Leaders*, 56-63.

Kowalski, Eileen, Tara Conway, Susan Keverline, Megan Williams, Dawn Cappelli, Bradford Willke, and Andrew Moore. 2008. *Insider Threat Study: Illicit Cyber Activity in the Government Sector*.

Levy , Yair , and Timothy J Ellis. 2006. "A Systems Approach to Conduct an Effective Literature Review in Support of Information Systems Research." *Informing Science Journal* 9: 181-211.

Lewellen, Todd , Andrew P Moore, Dawn M Cappelli, Randall F Trzeciak, Derrick Spooner, and Robert M Weiland. 2012. *Spotlight On: Insider Threat from Trusted Business Partners Version 2*. CERT.

Lincoln, Y.S., and E.G. Guba. 1985. *Naturalistic Inquiry*. Vol. 75. California: Sage Publications.

Liu, Debin, XiaoFeng Wang, and Jean Camp. 2008. "Game-Theoretic Modeling and Analysis of Insider Threats." *International Journal of Critical Infrastructure Protection* 1: 75-80.

Liu, Debin, XiaoFeng Wang, and L. Camp. 2009. "Mitigating Inadvertent Insider Threats with Incentives." In *Financial Cryptography and Data Security*, eds Roger Dingledine and Philippe Golle, 1-16. Springer Berlin / Heidelberg.

Longhurst, R. 2009. "Interviews: In-Depth, Semi-Structured." In *International Encyclopedia of Human Geography*, eds Kitchin Editors-in-Chief: Rob and Thrift Nigel, 580-584. Oxford: Elsevier.

Luo, Yadong, and Oded Shenkar. 2011. "Toward a Perspective of Cultural Friction in International Business." *Journal of International Management* 17 (1): 1-14.

Lynch, David M. 2006. Securing against Insider Attacks. *Information Systems Security*, 39-47.

Mack, Natasha, Cynthia Woodsong, Kathleen M MacQueen, Greg Guest, and Emily Namey. 2005. *Qualitative Research Methods: A Data Collector's Field Guide*. Triangle Park, Carolina: Family Health International.

Magklaras, G. B., and S. M. Furnell. 2002. "Insider Threat Prediction Tool: Evaluating the Probability of It Misuse." *Computers & Security* 21 (1): 62-73.

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.

Malhotra, Naresh K, Sung S Kim, and Ashutosh Patil. 2006. "Common Method Variance in Is Research: A Comparison of Alternative Approaches and a Reanalysis of Past Research." *Management Science* 52 (12): 1865-1883.

Martinez-Moyano, Ignacio , Eliot Rich, Stephen Conrad, and David Andersen. 2006 "Modeling the Emergence of Insider Threat Vulnerabilities." In *Proceedings of the 2006 Winter Simulation Conference, Monterey, California, USA*, 526- 568.

Martinez-Moyano, Ignacio, Eliot Rich, Stephen Conrad, David Andersen, and Thomas Stewart. 2008a. "A Behavioral Theory of Insider Threat Risks: A System Dynamics Approach." *ACM Transactions on Modeling and Computer Simulation* 18 (2): 1-27.

Martinez-Moyano, Ignacio, M Samsa, J Burke, and B Akcam. 2008b. "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*, 267-267. IEEE Xplore.

Mathur, Sanjeev Kumar, and Sunil Kumar Gupta. 2012. "Outside Factors Influencing Behavior of Employees in Organizations." *International Journal of Information and Education Technology* 2 (1): 48-50.

Maykut, P., and R Morehouse. 1994. *Beginning Qualitative Research: A Philosophical and a Practical Guide*. Vol. 6. Washington: Falmer Press.

Mayring, Ph. 2000a. *Qualitative Inhaltsanalyse. Grundlagen Und Techniken*. 7th ed. Weinheim: Deutscher Studien Verlag.

Mayring, Philipp. 2000b. "Qualitative Content Analysis." *Forum Qualitative Sozialforschung / Forum: Qualitative Social Research* 1 (2): 1-10.

McCoyd, Judith LM, and Toba Schwaber Kerson. 2006. "Conducting Intensive Interviews Using Email a Serendipitous Comparative Opportunity." *Qualitative Social Work* 5 (3): 389-406.

McNamara, Roy. 1998. "Networks -- Where Does the Real Threat Lie?" *Information Security Technical Report* 3 (4): 65-74.

Md Zabid Abdul, Rashid, Murali Sambasivan, and Juliana Johari. 2003. "The Influence of Corporate Culture and Organisational Commitment on Performance." *The Journal of Management Development* 22 (7/8): 708-728.

Mengshoel, Anne Marit. 2012. "Mixed Methods Research – So Far Easier Said Than Done?" *Manual Therapy* 17 (4): 373-375.

Messmer, Ellen. 2008. Insider Threat Looms Large in Sf. *Network World*, 8.

Messmer, Ellen. 2010. Sys Admin Gone Rogue Is Biggest Insider Threat. *Network World*, 11-13.

Miles, M, and A.M Huberman. 1994. *Qualitative Data Analysis*. Thousand Oaks, CA: Sage Publications.

Mingers, John. 2001. "Combining Is Research Methods: Towards a Pluralist Methodology." *Information Systems Research* 12 (3): 240.

Möller, Sebastian, Noam Ben-Asher, Klaus-Peter Engelbrecht, Roman Englert, and Joachim Meyer. 2011. "Modeling the Behavior of Users Who Are Confronted with Security Mechanisms." *Computers & Security* 30 (4): 242-256.

Monette, Duane R , Thomas J Sullivan, and Cornell R DeJong 2007. *Applied Social Research; Tool for the Human Services*. 6th ed. Vol. 22. Portland: Book News, Inc.

Moore, Andrew, Dawn Cappelli, Thomas Caron, Eric Shaw, and Randall Trzeciak. 2009. *Insider Theft of Intellectual Property for Business Advantage: A Preliminary Model*.

Moore, Andrew, Dawn Cappelli, and Randall Trzeciak. 2008. "The "Big Picture" of Insider It Sabotage across U.S. Critical Infrastructures." In *Insider Attack and Cyber Security*, eds Salvatore J. Stolfo, Steven M. Bellovin, Angelos D. Keromytis, Shlomo Hershkop, Sean W. Smith and Sara Sinclair, 17-52. Springer US.

Morse, J. & Richards, L. 2002. *Readme First of a User's Guide to Qualitative Methods*. Thousand Oaks: SAGE Publications.

Mubarak, Sameera, and Jill Slay. 2010. "Protecting Clients from Insider Attacks on Trust Accounts." *Information Security Technical Report* In Press, Corrected Proof.

Munshi, Asmaa, Peter Dell, and Helen Armstrong. 2012. "Insider Threat Behavior Factors: A Comparison of Theory with Reported Incidents." In *45th Hawaii International Conference on System Science (HICSS), Maui, HI* 2402-2411. IEEE.

Myers, Michael D. 1997. "Qualitative Research in Information Systems." *Management Information Systems Quarterly* 21 (1): 241-242.

Neumann, Peter G. 1999. Inside Risks: Risks of Insiders. *Communications of the ACM* 160.

Neumann, PeterG. 2010. "Combatting Insider Threats." In *Insider Threats in Cyber Security*, eds Christian W. Probst, Jeffrey Hunker, Dieter Gollmann and Matt Bishop, 17-44. Springer US.

Nouman, Muhammad, Imran Khan, and Faisal Khan. 2011. "Conflicts and Strategies for Their Resolution: A Case of Organizations Operating in Khyber Pakhtunkhwa, Pakistan." *Interdisciplinary Journal of Contemporary Research In Business* 3 (5): 618-633.

Nykodym, Nick, Robert Taylor, and Julia Vilela. 2005. "Criminal Profiling and Insider Cyber Crime." *Digital Investigation* 2 (4): 261-267.

Ofori-Dankwa, Joseph, and David A. Ricks. 2000. "Research Emphases on Cultural Differences and/or Similarities: Are We Asking the Right Questions?" *Journal of International Management* 6 (2): 173-186.

Okolica, James, Gilbert Peterson, and Robert Mills. 2006. "Using Plsi-U to Detect Insider Threats from Email Traffic." In *Advances in Digital Forensics Ii*, eds Martin Olivier and Sujeet Shenoi, 91-103. Springer Boston.

Oppenheim, A. N. 1992. *Questionnaire Design, Interviewing and Attitude Measurement.* . London: Pinter.

Ortega, Ross. 2006. The Insider Threat: When Trusted Assets Go Bad. *Electric Light & Power*, 22-24.

Padayachee, Keshnee. 2012. "Taxonomy of Compliant Information Security Behavior." *Computers & Security* 31 (5): 673-680.

Pallant, Julie 2011. *Spss Survival Manual*. Edited by 4th. Crows Nest, NSW: Allen & Unwin.

Parker, D.B. 1998. *Fighting Computer Crime: A New Framework for Protecting Information*. New York: John Wiley and Sons.

Patton, Michael Quinn. 2002. *Qualitative Research & Evaluation Methods*. 3rd ed. Thousand Oaks, CA Sage Publications.

Patzakis, J. 2003. *New Incident Response Best Practices: Patch and Proceed Is No Longer Acceptable Incident Response*. Pasadena.

Pfleeger, Charles P. 2008. "Reflections on the Insider Threat." In *Insider Attack and Cyber Security*, eds Salvatore J. Stolfo, Steven M. Bellovin, Angelos D. Keromytis, Shlomo Hershkop, Sean W. Smith and Sara Sinclair, 5-16. Springer US.

Pfleeger, S. L., J. B. Predd, J. Hunker, and C. Bulford. 2010. "Insiders Behaving Badly: Addressing Bad Actors and Their Actions." *Information Forensics and Security, IEEE Transactions on* 5 (1): 169-179.

Podsakoff, Philip M, Scott B MacKenzie, Jeong-Yeon Lee, and Nathan P Podsakoff. 2003. "Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies." *Journal of applied psychology* 88 (5): 879.

Pramanik, Suranjan, Vidyaraman Sankaranarayanan, and Shambhu 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*, 304 - 313 IEEE Computer Society

Predd, Joel, Shari Pfleeger, Jeffrey Hunker, and Carla Bulford. 2008. "Insider Behaving Badly." *IEEE Security and Privacy* 6 (4): 66-70.

Probst, Christian, René Hansen, and Flemming Nielson. 2007. "Where Can an Insider Attack?" In *Formal Aspects in Security and Trust*, eds Theo Dimitrakos, Fabio Martinelli, Peter Ryan and Steve Schneider, 127-142. Springer Berlin / Heidelberg.

Randazzo, Marisa, Michelle Keeney, Eileen Kowalski, Dawn Cappelli, and Andrew Moore. 2004. *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector*. CERT.

Reid, Anna , Peter Petocz, and Sue Gordon. 2008. "Research Interviews in Cyberspace." *Qualitative Research Journal* 8 (1): 47-67.

Rhee, Hyeun-Suk, Cheongtag Kim, and Young U. Ryu. 2009. "Self-Efficacy in Information Security: Its Influence on End Users' Information Security Practice Behavior." *Computers & Security* 28 (8): 816-826.

Richardson, Robert 2008. *Csi Computer Crime & Security Survey*

Robert, Willison, and Backhouse James. 2006. "Opportunities for Computer Crime: Considering Systems Risk from a Criminological Perspective." *European Journal of Information Systems* 15 (4): 403.

Roberts, Paul F. 2007. Secure Your Data. *InfoWorld*, 24-26.

Royds, J. 2009. Virtual Battlefield. *CIR Magazine*.

Ryan, A.B. (Eds.). 2006. " Methodology: Analysing Qualitative Data and Writing up

Your Findings." In *Researching and Writing Your Thesis: A Guide for Post Graduate Students* NUI Maynooth: MACE.

Sarala, Riikka M. 2010. "The Impact of Cultural Differences and Acculturation Factors on Post-Acquisition Conflict." *Scandinavian Journal of Management* 26 (1): 38-56.

Sarkar, Kuheli Roy 2010. "Assessing Insider Threats to Information Security Using Technical, Behavioural and Organisational Measures." *Information Security Technical Report* 15 (3): 112-133.

Sasaki, Takayuki 2011. "A Framework for Detecting Insider Threats Using Psychological Triggers." *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications* 3 (1/2): 99-119.

Schrag, Brian. 2001. "The Moral Significance of Employee Loyalty." *Business ethics quarterly* 11 (1): 41-66.

Schultz, E. Eugene. 2002. "A Framework for Understanding and Predicting Insider Attacks." *Computers & Security* 21 (6): 526-531.

Schultz, Eugene E, and Russell Shumway. 2001. *Incident Response: A Strategic Guide for System and Network Security Breaches*. Indianapolis: New Riders.

Schwartz, Ruth Bolotin, and Michele Russo, C 2004. "How to Quickly Find Articles in the Top Is Journals." *Commun. ACM* 47 (2): 98-101.

Secret Service, Cert Analyze Insider Computer Sabotage. 2005. *Claims*, 12-12.

Serdiouk, Victor. 2007. "Technologies for Protection against Insider Attacks on Computer Systems." In *Computer Network Security*, eds Vladimir Gorodetsky, Igor Kotenko and Victor A. Skormin, 75-84. Springer Berlin Heidelberg.

Shaw, Eric , Keven G. Ruby, and Jerrold M. Post. 1998. *The Insider Threat to Information Systems.Security Awareness Bulletin, No 2/98*.

Shaw, Eric , Keven G. Ruby, and Jerrold M. Post. 2005. *The Insider Threat to Information Systems1. The Psychology of the Dangerous Insider*.

Shaw, Eric D. 2006. "The Role of Behavioral Research and Profiling in Malicious Cyber Insider Investigations." *Digital Investigation* 3 (1): 20-31.

Siemsen, Enno, Aleda Roth, and Pedro Oliveira. 2010. "Common Method Bias in Regression Models with Linear, Quadratic, and Interaction Effects." *Organizational Research Methods* 13 (3): 456-476.

Siponen, M, and R Willison. 2007. "A Critical Assessment of Is Security Research between 1990- 004." In *In proceedings of 15th European Conference on Information Systems, Switzerland, St. Gallen*, 1-10.

Spooner, Derrick , Dawn Cappelli, Andrew Moore, and Randall Trzeciak. 2009. *Spotlight On: Insider Theft of Intellectual Property inside the U.S. Involving Foreign Governments or Organizations*. CyLab.

Stanton, Jeffrey M., Kathryn R. Stam, Paul Mastrangelo, and Jeffrey Jolton. 2005. "Analysis of End User Security Behaviors." *Computers & Security* 24 (2): 124-133.

Steele, Sean, and Chris Wargo. 2007. An Introduction to Insider Threat Management. *Information Systems Security*, 23-33.

Swartz, Nikki. 2007. "Protecting Information from Insiders." *Information Management Journal* 41 (3): 20-24.

Syauta, Jack Henry, Eka Afnan Troena, Margono Setiawan, and Solimun. 2012. "The Influence of Organizational Culture, Organizational Commitment to Job Satisfaction and Employee Performance (Study at Municipal Waterworks of Jayapura, Papua Indonesia)." *International Journal of Business and Management Invention* 1 (1): 69-76.

Tashakkori, Abbas, and Charles Teddlie. 2003. "Major Issues and Controversies in the Use of Mixed Methods in the Social and Behavioral Sciences." In *Handbook of Mixed Methods in Social and Behavioral Research*, eds A Tashakkori and C Teddlie, 3-50. Thousand Oaks, California: SAGE Publications, Incorporated.

Teo, Hock-Hai, Kwok-Kee Wei, and Izak Benbasat. 2003. "Predicting Intention to Adopt Interorganizational Linkages: An Institutional Perspective." *MIS Quarterly* 27 (1): 19-49.

Tesch, R. 1990. "Qualitative Research: Analysis Types & Software Tools." Bristol, PA: Falmer Press.

Theoharidou, Marianthi, Spyros Kokolakis, Maria Karyda, and Evangelos Kiountouzis. 2005. "The Insider Threat to Information Systems and the Effectiveness of Iso17799." *Computers & Security* 24 (6): 472-484.

Thompson, Herbert H, and Richard Ford. 2004. Perfect Storm: The Insider, Naivety, and Hostility. *Queue*, 58-65.

Thompson, Herbert H., James A. Whittaker, and Mike Andrews. 2004. "Intrusion Detection: Perspectives on the Insider Threat." *Computer Fraud & Security* 2004 (1): 13-15.

Thomson, Kerry-Lynn, and Rossouw von Solms. 2006. "Towards an Information Security Competence Maturity Model." *Computer Fraud & Security* 2006 (5): 11-15.

Vosloban, Raluca Ioana. 2012. "The Influence of the Employee's Performance on the Company's Growth - a Managerial Perspective." *Procedia Economics and Finance* 3 (0): 660-665.

Walker, Terrence. 2008. "Practical Management of Malicious Insider Threat - an Enterprise Csirt Perspective." *Information Security Technical Report* 13 (4): 225-234.

Walton, Richard, and Walton-Mackenzie Limited. 2006. "Balancing the Insider and Outsider Threat." *Computer Fraud & Security* 2006 (11): 8-11.

Warren, C. . 2001. "Qualitative Interviewing." In *Handbook of Interview Research Context and Method*, ed. Gubrium J. & J. Holstein, 83-102. Thousand Oaks: SAGE Publication.

Wehrum, Kasey. 2009. When It Workers Attack. *Inc.*, 132-133.

Weinhold, Barry K., and Janae B. Weinhold. 2004. "How Can I Apply the Partnership Way in the Workplace?" *Counseling and Human Development* 36 (7): 1-12.

Westerman, Michael A. 2006. "What Counts as “Good” Quantitative Research and What Can We Say About When to Use Quantitative and/or Qualitative Methods?" *New Ideas in Psychology* 24 (3): 263-274.

White, Jonathan, and Brajendra Panda. 2009. "Automatic Identification of Critical Data Items in a Database to Mitigate the Effects of Malicious Insiders." In *Information Systems Security*, eds Atul Prakash and Indranil Sen Gupta, 208-221. Springer Berlin / Heidelberg.

Whiteley, A. 2002. "Rigour in Qualitative Research " *Working Papers Series Curtin University of Tecnology Graduate School of Business* no. working paper series 02.01.

Whitworth, Martin. 2005. "Outsourced Security – the Benefits and Risks." *Network Security* 2005 (10): 16-19.

Williams, Brett , Ted Brown, and Andrys Onsman. 2010. "Exploratory Factor Analysis: A Five-Step Guide for Novices." *Journal of Emergency Primary Health Care* 8 (3): 1-13.

Willison, R, and M Warkentin. 2013. "Beyond Deterrence: An Expanded View of Employee Computer Abuse." *MIS Quarterly* 37 (1): 1-20.

Willison, Robert, and Mikko Siponen. 2009. Overcoming the Insider: Reducing Employee Computer Crime through Situational Crime Prevention. *Commun. ACM*, 133-137.

Wood, Bradley J. . 2000. "An Insider Threat Model for Adversary Simulation." *SRI International, Research on Mitigating the Insider Threat to Information Systems* 2: 1-3.

Yin, Robert K. 2006. "Mixed Methods Research: Are the Methods Genuinely Integrated or Merely Parallel." *Research in the Schools* 13 (1): 41-47.

Zafar, Humayun. 2013. "Human Resource Information Systems: Information Security Concerns for Organizations." *Human Resource Management Review* 23 (1): 105-113.

Zhang, Yan, and Barbara M Wildemuth. 2009. "Qualitative Analysis of Content." *Applications of social research methods to questions in information and library science*: 308-319.

Zou, Qiong. 2011. "Analysis and Intervention on the Influencing Factors of Employee's Job Insecurity." In *Computing and Intelligent Systems*, ed. Yanwen Wu, 129-135. Springer Berlin Heidelberg.

APPENDICES

Appendix 1: Survey Questions

Insider Threat Behavior Factors

I am a PhD student at Curtin University and I am conducting research into insider threat behavior. Any security system relies upon its operators, even if it is designed and implemented in a perfect manner. Organizations face ongoing threats and attacks from external and internal sources. Insider attacks are associated with legitimate users who abuse their privileges and can easily cause significant damage or loss to an organization.

Previous research in this area focused on narrow and specific areas and all of the frameworks developed so far specialize in either people-to-people relationships, segmentation of tasks, access to information or network architectures. There has been no research published so far that gives a 'big picture' view of insider threat behavior.
My research aims to develop a conceptual insider threat model that can frame such a 'big-picture' view of insider threat behavior and inform the development of a management framework to help organizations manage the insider threat

Please note:

- **The survey process will take approximately 15 minutes.**
- **Your privacy is greatly respected and any information that could identify you will not be published at any time.**
- **All information will be stored in a secure location at Curtin University for five years.**
- **Taking part is voluntary and you can withdrawal at any time.**

This study has been approved under Curtin University's process for lower-risk Studies (IS_12_14). This process complies with the National Statement on Ethical Conduct in Human Research (Chapter 5.1.7 and Chapters 5.1.18-5.1.21).For further information on this study contact the researchers: Asmaa Munshi on a.munshi@postgrad.curtin.edu.au or the Curtin University Human Research Ethics Committee. c/- Office of Research and Development, Curtin University, GPO Box U1987, Perth 6845 or by telephoning 9266 9223 or by emailing hrec@curtin.edu.au.

Page 1/3

What is your gender?

- Male
- Female

Please select your job title from the list below:

- IT Security Manager
- Principal Cyber Security Manager
- Security Systems Administrator
- Senior IT Security Consultant
- Other:

Do you have experience in dealing with insider threat behavior?

- Yes
- No

In which industries does your employer primarily operate?

Administrative and Support and Waste Management and Remediation Services
Agriculture, Forestry, Fishing, and Hunting
Arts, Entertainment, and Recreation
Construction
Educational Services
Finance and Insurance
Health Care and Social Assistance
Information
Manufacturing
Management of Companies and Enterprises

Page 2/3

Please indicate your level of agreement to each statement:

The risk of insider threat behavior is increased by...

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Unable to judge
... psychological factors such as social frustrations or computer dependency.						
... outsourced employees being given the same logical and/or physical access as the organization's regular employees.						
... the implementation of inappropriate information security policy.						
... organizational culture that tolerates unethical behavior.						
... insiders being motivated to harm their organization.						
... outdated information security procedures or policies.						
... a poor level of health and fitness among employees.						
... employees working from home.						
... personal factors such as alcohol and drug addiction or violent behavior.						
... high levels of access to IT systems given to employees.						
... allowing authorized mobile device to access organizational information from outside the organization physical boundary.						
... the organization engaging a relatively high number of outsourcing agreements.						
... employees from backgrounds where acceptable practices differ.						
... insiders being vulnerable to coercion by outsider.						
... insiders' knowledge of the methods used to detect insider threat behavior.						
... technically skilled insiders who violates the security for personal gain.						
... not promptly canceling access of ex-employees.						
... lack of customer and/or client participation in product development.						
... high levels of trust given to employees.						
... employees having formal training in computer science, IT or similar.						
... insiders' knowledge of methods to grant access to the organization's information.						
... inappropriate or concerning behavior prior to the incident such as delays, absences and poor job performance.						
... organization ownership being limited by shares.						
... employees' level of technical sophistication.						
... insufficient information security policy training and awareness.						
... cultural clash between employees and the organization.						
... insiders' knowledge of the potential value of the organization's information to outsiders.						
... insiders being unduly motivated by financial gain.						
... granting access to third- parties contracted to conduct work within the organization.						
... giving employees remote access to organizational information.						

Do you have any comments regarding insider threat behavior?

Appendix 2: Correlations Matrix

		psychological factors such as social frustrations or computer dependency.	personal factors such as alcohol and drug addiction or violent behavior.	inappropriate or concerning behavior prior to the incident such as delays, absences and poor job performance.
psychological factors such as social frustrations or computer dependency.	Pearson Correlation	1	.234*	.207*
	Sig. (2-tailed)		.019	.039
	N	100	100	100
personal factors such as alcohol and drug addiction or violent behavior.	Pearson Correlation	.234*	1	.261**
	Sig. (2-tailed)	.019		.009
	N	100	100	100
inappropriate or concerning behavior prior to the incident such as delays, absences and poor job performance.	Pearson Correlation	.207*	.261**	1
	Sig. (2-tailed)	.039	.009	
	N	100	100	100
outsourced employees being given the same logical and/or physical access as the organization's regular employees.	Pearson Correlation	.350**	.255*	.224*
	Sig. (2-tailed)	.000	.011	.025
	N	100	100	100
the organization engaging a relatively high number of outsourcing agreements.	Pearson Correlation	.142	.130	.175
	Sig. (2-tailed)	.158	.198	.081
	N	100	100	100
granting access to third-parties contracted to conduct work within the organization.	Pearson Correlation	.187	.300**	.076
	Sig. (2-tailed)	.063	.002	.454
	N	100	100	100
the implementation of inappropriate information	Pearson Correlation	.202*	.202*	.037
	Sig. (2-tailed)	.043	.043	.712

security policy.	N	100	100	100
outdated information security procedures or policies.	Pearson Correlation	.244*	.298**	.144
	Sig. (2-tailed)	.014	.003	.152
	N	100	100	100

Correlations

		outsourced employees being given the same logical and/or physical access as the organization's regular employees.	the organization engaging a relatively high number of outsourcing agreements.	granting access to third- parties contracted to conduct work within the organization.
psychological factors such as social frustrations or computer dependency.	Pearson Correlation	.350	.142*	.187*
	Sig. (2-tailed)	.000	.158	.063
	N	100	100	100
personal factors such as alcohol and drug addiction or violent behavior.	Pearson Correlation	.255*	.130	.300**
	Sig. (2-tailed)	.011	.198	.002
	N	100	100	100
inappropriate or concerning behavior prior to the incident such as delays, absences and poor job performance.	Pearson Correlation	.224*	.175**	.076
	Sig. (2-tailed)	.025	.081	.454
	N	100	100	100
outsourced employees being given the same logical and/or physical access as the organization's regular employees.	Pearson Correlation	1**	.210*	.246*
	Sig. (2-tailed)		.036	.014
	N	100	100	100
the organization engaging a relatively high number of outsourcing agreements.	Pearson Correlation	.210	1	.427
	Sig. (2-tailed)	.036		.000
	N	100	100	100
granting access to third- parties contracted to conduct work within the organization.	Pearson Correlation	.246	.427**	1
	Sig. (2-tailed)	.014	.000	
	N	100	100	100
the implementation of inappropriate information security policy.	Pearson Correlation	.504*	.158*	.243
	Sig. (2-tailed)	.000	.116	.015
	N	100	100	100
outdated information security	Pearson Correlation	.274*	.401**	.384

procedures or policies.	Sig. (2-tailed)	.006	.000	.000
	N	100	100	100

		the implementation of inappropriate information security policy.	outdated information security procedures or policies.	insufficient information security policy training and awareness.
psychological factors such as social frustrations or computer dependency.	Pearson Correlation	.202	.244*	.054*
	Sig. (2-tailed)	.043	.014	.596
	N	100	100	100
personal factors such as alcohol and drug addiction or violent behavior.	Pearson Correlation	.202*	.298	.176**
	Sig. (2-tailed)	.043	.003	.079
	N	100	100	100
inappropriate or concerning behavior prior to the incident such as delays, absences and poor job performance.	Pearson Correlation	.037*	.144**	.182
	Sig. (2-tailed)	.712	.152	.070
	N	100	100	100
outsourced employees being given the same logical and/or physical access as the organization's regular employees.	Pearson Correlation	.504**	.274*	.296*
	Sig. (2-tailed)	.000	.006	.003
	N	100	100	100
the organization engaging a relatively high number of outsourcing agreements.	Pearson Correlation	.158	.401	.370
	Sig. (2-tailed)	.116	.000	.000
	N	100	100	100
granting access to third- parties contracted to conduct work within the organization.	Pearson Correlation	.243	.384**	.321
	Sig. (2-tailed)	.015	.000	.001
	N	100	100	100
the implementation of inappropriate information security policy.	Pearson Correlation	1*	.460*	.326
	Sig. (2-tailed)		.000	.001
	N	100	100	100
outdated information security procedures or policies.	Pearson Correlation	.460*	1**	.429
	Sig. (2-tailed)	.000		.000
	N	100	100	100

Correlations

		organizational culture that tolerates unethical behavior.	employees from backgrounds where acceptable practices differ.	cultural clash between employees and the organization.
psychological factors such as social frustrations or computer dependency.	Pearson Correlation	.407**	.170*	.289*
	Sig. (2-tailed)	.000	.092	.004
	N	100	100	100
personal factors such as alcohol and drug addiction or violent behavior.	Pearson Correlation	.407*	.145	.337**
	Sig. (2-tailed)	.000	.150	.001
	N	100	100	100
inappropriate or concerning behavior prior to the incident such as delays, absences and poor job performance.	Pearson Correlation	.256*	.342**	.300
	Sig. (2-tailed)	.010	.000	.002
	N	100	100	100
outsourced employees being given the same logical and/or physical access as the organization's regular employees.	Pearson Correlation	.217**	.135*	.167*
	Sig. (2-tailed)	.030	.180	.096
	N	100	100	100
the organization engaging a relatively high number of outsourcing agreements.	Pearson Correlation	.167	.433	.390
	Sig. (2-tailed)	.096	.000	.000
	N	100	100	100
granting access to third- parties contracted to conduct work within the organization.	Pearson Correlation	.053	.296**	.411
	Sig. (2-tailed)	.601	.003	.000
	N	100	100	100
the implementation of inappropriate information security policy.	Pearson Correlation	.182*	-.046*	.142
	Sig. (2-tailed)	.070	.649	.158
	N	100	100	100
outdated information security procedures or policies.	Pearson Correlation	.264*	.216**	.352
	Sig. (2-tailed)	.008	.031	.000
	N	100	100	100

Correlations

		insiders being motivated to harm their organization.	insiders being vulnerable to coercion by outsider.	insiders being unduly motivated by financial gain.
psychological factors such as social frustrations or computer dependency.	Pearson Correlation	.349	.274*	.226*
	Sig. (2-tailed)	.000	.006	.023
	N	100	100	100
personal factors such as alcohol and drug addiction or violent behavior.	Pearson Correlation	.393*	.345	.344**
	Sig. (2-tailed)	.000	.000	.000
	N	100	100	100
inappropriate or concerning behavior prior to the incident such as delays, absences and poor job performance.	Pearson Correlation	.169*	.279**	.266
	Sig. (2-tailed)	.092	.005	.008
	N	100	100	100
outsourced employees being given the same logical and/or physical access as the organization's regular employees.	Pearson Correlation	.333**	.355*	.336*
	Sig. (2-tailed)	.001	.000	.001
	N	100	100	100
the organization engaging a relatively high number of outsourcing agreements.	Pearson Correlation	.146	.474	.361
	Sig. (2-tailed)	.146	.000	.000
	N	100	100	100
granting access to third- parties contracted to conduct work within the organization.	Pearson Correlation	.123	.360**	.392
	Sig. (2-tailed)	.222	.000	.000
	N	100	100	100
the implementation of inappropriate information security policy.	Pearson Correlation	.381*	.265*	.350
	Sig. (2-tailed)	.000	.008	.000
	N	100	100	100
outdated information security procedures or policies.	Pearson Correlation	.469*	.487**	.391
	Sig. (2-tailed)	.000	.000	.000
	N	100	100	100

Correlations

		employees working from home.	giving employees remote access to organizational information.	allowing authorized mobile device to access organizational information from outside the organization physical boundary.
psychological factors such as social frustrations or computer dependency.	Pearson Correlation	.374	.184*	-.031*
	Sig. (2-tailed)	.000	.066	.756
	N	100	100	100
personal factors such as alcohol and drug addiction or violent behavior.	Pearson Correlation	.361*	.124	.163**
	Sig. (2-tailed)	.000	.220	.105
	N	100	100	100
inappropriate or concerning behavior prior to the incident such as delays, absences and poor job performance.	Pearson Correlation	.194*	.187**	.103
	Sig. (2-tailed)	.053	.063	.306
	N	100	100	100
outsourced employees being given the same logical and/or physical access as the organization's regular employees.	Pearson Correlation	.336**	.216*	.062*
	Sig. (2-tailed)	.001	.031	.537
	N	100	100	100
the organization engaging a relatively high number of outsourcing agreements.	Pearson Correlation	.147	.280	.379
	Sig. (2-tailed)	.145	.005	.000
	N	100	100	100
granting access to third- parties contracted to conduct work within the organization.	Pearson Correlation	.320	.499**	.382
	Sig. (2-tailed)	.001	.000	.000
	N	100	100	100
the implementation of inappropriate information security policy.	Pearson Correlation	.214*	.015*	.136
	Sig. (2-tailed)	.032	.882	.177
	N	100	100	100
outdated information security procedures or policies.	Pearson Correlation	.195*	.121**	.193
	Sig. (2-tailed)	.052	.230	.054
	N	100	100	100

Correlations

		insiders' knowledge of the methods used to detect insider threat behavior.	insiders' knowledge of methods to grant access to the organization's information.	insiders' knowledge of the potential value of the organization's information to outsiders.
psychological factors such as social frustrations or computer dependency.	Pearson Correlation	.234	.331*	.227*
	Sig. (2-tailed)	.019	.001	.023
	N	100	100	100
personal factors such as alcohol and drug addiction or violent behavior.	Pearson Correlation	.094*	.336	.280**
	Sig. (2-tailed)	.353	.001	.005
	N	100	100	100
inappropriate or concerning behavior prior to the incident such as delays, absences and poor job performance.	Pearson Correlation	.206*	.238**	.139
	Sig. (2-tailed)	.040	.017	.169
	N	100	100	100
outsourced employees being given the same logical and/or physical access as the organization's regular employees.	Pearson Correlation	.126**	.246*	.293*
	Sig. (2-tailed)	.210	.014	.003
	N	100	100	100
the organization engaging a relatively high number of outsourcing agreements.	Pearson Correlation	.286	.337	.429
	Sig. (2-tailed)	.004	.001	.000
	N	100	100	100
granting access to third- parties contracted to conduct work within the organization.	Pearson Correlation	.369	.461**	.401
	Sig. (2-tailed)	.000	.000	.000
	N	100	100	100
the implementation of inappropriate information security policy.	Pearson Correlation	.221*	.363*	.308
	Sig. (2-tailed)	.027	.000	.002
	N	100	100	100
outdated information security procedures or policies.	Pearson Correlation	.263*	.496**	.289
	Sig. (2-tailed)	.008	.000	.004
	N	100	100	100

Correlations

		technically skilled insiders who violates the security for personal gain.	employees' level of technical sophistication.	employees having formal training in computer science, IT or similar.
psychological factors such as social frustrations or computer dependency.	Pearson Correlation	.338	.325*	.267*
	Sig. (2-tailed)	.001	.001	.007
	N	100	100	100
personal factors such as alcohol and drug addiction or violent behavior.	Pearson Correlation	.421*	.089	.140**
	Sig. (2-tailed)	.000	.379	.165
	N	100	100	100
inappropriate or concerning behavior prior to the incident such as delays, absences and poor job performance.	Pearson Correlation	.097*	.175**	.312
	Sig. (2-tailed)	.336	.081	.002
	N	100	100	100
outsourced employees being given the same logical and/or physical access as the organization's regular employees.	Pearson Correlation	.305**	.200*	.396*
	Sig. (2-tailed)	.002	.047	.000
	N	100	100	100
the organization engaging a relatively high number of outsourcing agreements.	Pearson Correlation	.311	.262	.109
	Sig. (2-tailed)	.002	.009	.281
	N	100	100	100
granting access to third- parties contracted to conduct work within the organization.	Pearson Correlation	.389	.320**	.268
	Sig. (2-tailed)	.000	.001	.007
	N	100	100	100
the implementation of inappropriate information security policy.	Pearson Correlation	.468*	.224*	.254
	Sig. (2-tailed)	.000	.025	.011
	N	100	100	100
outdated information security procedures or policies.	Pearson Correlation	.536*	.387**	.125
	Sig. (2-tailed)	.000	.000	.216
	N	100	100	100

Correlations

		high levels of access to IT systems given to employees.	not promptly canceling access of ex-employees.	high levels of trust given to employees.
psychological factors such as social frustrations or computer dependency.	Pearson Correlation	.200	.242*	.317*
	Sig. (2-tailed)	.046	.015	.001
	N	100	100	100
personal factors such as alcohol and drug addiction or violent behavior.	Pearson Correlation	.232*	.260	.207**
	Sig. (2-tailed)	.020	.009	.039
	N	100	100	100
inappropriate or concerning behavior prior to the incident such as delays, absences and poor job performance.	Pearson Correlation	.219*	.221**	.210
	Sig. (2-tailed)	.029	.027	.036
	N	100	100	100
outsourced employees being given the same logical and/or physical access as the organization's regular employees.	Pearson Correlation	.168**	.178*	.383*
	Sig. (2-tailed)	.094	.077	.000
	N	100	100	100
the organization engaging a relatively high number of outsourcing agreements.	Pearson Correlation	.380	.131	.283
	Sig. (2-tailed)	.000	.193	.004
	N	100	100	100
granting access to third- parties contracted to conduct work within the organization.	Pearson Correlation	.370	.294**	.255
	Sig. (2-tailed)	.000	.003	.010
	N	100	100	100
the implementation of inappropriate information security policy.	Pearson Correlation	.237*	.296*	.295
	Sig. (2-tailed)	.017	.003	.003
	N	100	100	100
outdated information security procedures or policies.	Pearson Correlation	.296*	.456**	.266
	Sig. (2-tailed)	.003	.000	.007
	N	100	100	100

Correlations

		organization ownership being limited by shares.	lack of customer and/or client participation in product development.	a poor level of health and fitness among employees.
psychological factors such as social frustrations or computer dependency.	Pearson Correlation	.118	-.054*	.056*
	Sig. (2-tailed)	.241	.592	.579
	N	100	100	100
personal factors such as alcohol and drug addiction or violent behavior.	Pearson Correlation	-.016*	-.007	.019**
	Sig. (2-tailed)	.876	.942	.854
	N	100	100	100
inappropriate or concerning behavior prior to the incident such as delays, absences and poor job performance.	Pearson Correlation	.094*	-.038**	.160
	Sig. (2-tailed)	.354	.706	.111
	N	100	100	100
outsourced employees being given the same logical and/or physical access as the organization's regular employees.	Pearson Correlation	-.120**	-.125*	.064*
	Sig. (2-tailed)	.235	.214	.527
	N	100	100	100
the organization engaging a relatively high number of outsourcing agreements.	Pearson Correlation	-.177	-.172	.099
	Sig. (2-tailed)	.079	.087	.327
	N	100	100	100
granting access to third- parties contracted to conduct work within the organization.	Pearson Correlation	-.033	.028**	.018
	Sig. (2-tailed)	.745	.784	.857
	N	100	100	100
the implementation of inappropriate information security policy.	Pearson Correlation	-.271*	-.116*	-.077
	Sig. (2-tailed)	.006	.251	.449
	N	100	100	100
outdated information security procedures or policies.	Pearson Correlation	-.195*	-.080**	-.107
	Sig. (2-tailed)	.052	.427	.290
	N	100	100	100

Correlations

		psychological factors such as social frustrations or computer dependency.	personal factors such as alcohol and drug addiction or violent behavior.	inappropriate or concerning behavior prior to the incident such as delays, absences and poor job performance.
insufficient information security policy training and awareness.	Pearson Correlation	.054	.176*	.182*
	Sig. (2-tailed)	.596	.079	.070
	N	100	100	100
organizational culture that tolerates unethical behavior.	Pearson Correlation	.407*	.407	.256**
	Sig. (2-tailed)	.000	.000	.010
	N	100	100	100
employees from backgrounds where acceptable practices differ.	Pearson Correlation	.170*	.145**	.342
	Sig. (2-tailed)	.092	.150	.000
	N	100	100	100
cultural clash between employees and the organization.	Pearson Correlation	.289**	.337*	.300*
	Sig. (2-tailed)	.004	.001	.002
	N	100	100	100
insiders being motivated to harm their organization.	Pearson Correlation	.349	.393	.169
	Sig. (2-tailed)	.000	.000	.092
	N	100	100	100
insiders being vulnerable to coercion by outsider.	Pearson Correlation	.274	.345**	.279
	Sig. (2-tailed)	.006	.000	.005
	N	100	100	100
insiders being unduly motivated by financial gain.	Pearson Correlation	.226*	.344*	.266
	Sig. (2-tailed)	.023	.000	.008
	N	100	100	100
employees working from home.	Pearson Correlation	.374*	.361**	.194
	Sig. (2-tailed)	.000	.000	.053
	N	100	100	100
giving employees remote access to organizational information.	Pearson Correlation	.184	.124	.187
	Sig. (2-tailed)	.066	.220	.063
	N	100	100	100

Correlations

		outsourced employees being given the same logical and/or physical access as the organization's regular employees.	the organization engaging a relatively high number of outsourcing agreements.	granting access to third- parties contracted to conduct work within the organization.
insufficient information security policy training and awareness.	Pearson Correlation	.296	.370*	.321*
	Sig. (2-tailed)	.003	.000	.001
	N	100	100	100
organizational culture that tolerates unethical behavior.	Pearson Correlation	.217*	.167	.053**
	Sig. (2-tailed)	.030	.096	.601
	N	100	100	100
employees from backgrounds where acceptable practices differ.	Pearson Correlation	.135*	.433**	.296
	Sig. (2-tailed)	.180	.000	.003
	N	100	100	100
cultural clash between employees and the organization.	Pearson Correlation	.167**	.390*	.411*
	Sig. (2-tailed)	.096	.000	.000
	N	100	100	100
insiders being motivated to harm their organization.	Pearson Correlation	.333	.146	.123
	Sig. (2-tailed)	.001	.146	.222
	N	100	100	100
insiders being vulnerable to coercion by outsider.	Pearson Correlation	.355	.474**	.360
	Sig. (2-tailed)	.000	.000	.000
	N	100	100	100
insiders being unduly motivated by financial gain.	Pearson Correlation	.336*	.361*	.392
	Sig. (2-tailed)	.001	.000	.000
	N	100	100	100
employees working from home.	Pearson Correlation	.336*	.147**	.320
	Sig. (2-tailed)	.001	.145	.001
	N	100	100	100
giving employees remote access to organizational information.	Pearson Correlation	.216	.280	.499
	Sig. (2-tailed)	.031	.005	.000
	N	100	100	100

Correlations

		the implementation of inappropriate information security policy.	outdated information security procedures or policies.	insufficient information security policy training and awareness.
insufficient information security policy training and awareness.	Pearson Correlation	.326	.429*	1*
	Sig. (2-tailed)	.001	.000	
	N	100	100	100
organizational culture that tolerates unethical behavior.	Pearson Correlation	.182*	.264	.153**
	Sig. (2-tailed)	.070	.008	.129
	N	100	100	100
employees from backgrounds where acceptable practices differ.	Pearson Correlation	-.046*	.216**	.307
	Sig. (2-tailed)	.649	.031	.002
	N	100	100	100
cultural clash between employees and the organization.	Pearson Correlation	.142**	.352*	.354*
	Sig. (2-tailed)	.158	.000	.000
	N	100	100	100
insiders being motivated to harm their organization.	Pearson Correlation	.381	.469	.222
	Sig. (2-tailed)	.000	.000	.027
	N	100	100	100
insiders being vulnerable to coercion by outsider.	Pearson Correlation	.265	.487**	.302
	Sig. (2-tailed)	.008	.000	.002
	N	100	100	100
insiders being unduly motivated by financial gain.	Pearson Correlation	.350*	.391*	.325
	Sig. (2-tailed)	.000	.000	.001
	N	100	100	100
employees working from home.	Pearson Correlation	.214*	.195**	.066
	Sig. (2-tailed)	.032	.052	.512
	N	100	100	100
giving employees remote access to organizational information.	Pearson Correlation	.015	.121	.316
	Sig. (2-tailed)	.882	.230	.001
	N	100	100	100

Correlations

		organizational culture that tolerates unethical behavior.	employees from backgrounds where acceptable practices differ.	cultural clash between employees and the organization.
insufficient information security policy training and awareness.	Pearson Correlation	.153	.307*	.354*
	Sig. (2-tailed)	.129	.002	.000
	N	100	100	100
organizational culture that tolerates unethical behavior.	Pearson Correlation	1*	.169	.456**
	Sig. (2-tailed)		.093	.000
	N	100	100	100
employees from backgrounds where acceptable practices differ.	Pearson Correlation	.169*	1**	.358
	Sig. (2-tailed)	.093		.000
	N	100	100	100
cultural clash between employees and the organization.	Pearson Correlation	.456**	.358*	1*
	Sig. (2-tailed)	.000	.000	
	N	100	100	100
insiders being motivated to harm their organization.	Pearson Correlation	.489	.136	.290
	Sig. (2-tailed)	.000	.177	.003
	N	100	100	100
insiders being vulnerable to coercion by outsider.	Pearson Correlation	.358	.451**	.434
	Sig. (2-tailed)	.000	.000	.000
	N	100	100	100
insiders being unduly motivated by financial gain.	Pearson Correlation	.445*	.150*	.438
	Sig. (2-tailed)	.000	.136	.000
	N	100	100	100
employees working from home.	Pearson Correlation	.184*	.167**	.206
	Sig. (2-tailed)	.066	.097	.040
	N	100	100	100
giving employees remote access to organizational information.	Pearson Correlation	-.002	.196	.222
	Sig. (2-tailed)	.985	.050	.026
	N	100	100	100

Correlations

		insiders being motivated to harm their organization.	insiders being vulnerable to coercion by outsider.	insiders being unduly motivated by financial gain.
insufficient information security policy training and awareness.	Pearson Correlation	.222	.302*	.325*
	Sig. (2-tailed)	.027	.002	.001
	N	100	100	100
organizational culture that tolerates unethical behavior.	Pearson Correlation	.489*	.358	.445**
	Sig. (2-tailed)	.000	.000	.000
	N	100	100	100
employees from backgrounds where acceptable practices differ.	Pearson Correlation	.136*	.451**	.150
	Sig. (2-tailed)	.177	.000	.136
	N	100	100	100
cultural clash between employees and the organization.	Pearson Correlation	.290**	.434*	.438*
	Sig. (2-tailed)	.003	.000	.000
	N	100	100	100
insiders being motivated to harm their organization.	Pearson Correlation	1	.511	.314
	Sig. (2-tailed)		.000	.001
	N	100	100	100
insiders being vulnerable to coercion by outsider.	Pearson Correlation	.511	1**	.409
	Sig. (2-tailed)	.000		.000
	N	100	100	100
insiders being unduly motivated by financial gain.	Pearson Correlation	.314*	.409*	1
	Sig. (2-tailed)	.001	.000	
	N	100	100	100
employees working from home.	Pearson Correlation	.226*	.306**	.132
	Sig. (2-tailed)	.024	.002	.191
	N	100	100	100
giving employees remote access to organizational information.	Pearson Correlation	-.013	.204	.225
	Sig. (2-tailed)	.900	.042	.024
	N	100	100	100

Correlations

		employees working from home.	giving employees remote access to organizational information.	allowing authorized mobile device to access organizational information from outside the organization physical boundary.
insufficient information security policy training and awareness.	Pearson Correlation	.066	.316*	.279*
	Sig. (2-tailed)	.512	.001	.005
	N	100	100	100
organizational culture that tolerates unethical behavior.	Pearson Correlation	.184*	-.002	.182**
	Sig. (2-tailed)	.066	.985	.069
	N	100	100	100
employees from backgrounds where acceptable practices differ.	Pearson Correlation	.167*	.196**	.156
	Sig. (2-tailed)	.097	.050	.122
	N	100	100	100
cultural clash between employees and the organization.	Pearson Correlation	.206**	.222*	.256*
	Sig. (2-tailed)	.040	.026	.010
	N	100	100	100
insiders being motivated to harm their organization.	Pearson Correlation	.226	-.013	.033
	Sig. (2-tailed)	.024	.900	.747
	N	100	100	100
insiders being vulnerable to coercion by outsider.	Pearson Correlation	.306	.204**	.193
	Sig. (2-tailed)	.002	.042	.054
	N	100	100	100
insiders being unduly motivated by financial gain.	Pearson Correlation	.132*	.225*	.172
	Sig. (2-tailed)	.191	.024	.087
	N	100	100	100
employees working from home.	Pearson Correlation	1*	.432**	.227
	Sig. (2-tailed)		.000	.023
	N	100	100	100
giving employees remote access to organizational information.	Pearson Correlation	.432	1	.372
	Sig. (2-tailed)	.000		.000
	N	100	100	100

Correlations

		insiders' knowledge of the methods used to detect insider threat behavior.	insiders' knowledge of methods to grant access to the organization's information.	insiders' knowledge of the potential value of the organization's information to outsiders.
insufficient information security policy training and awareness.	Pearson Correlation	.288	.364*	.297*
	Sig. (2-tailed)	.004	.000	.003
	N	100	100	100
organizational culture that tolerates unethical behavior.	Pearson Correlation	.414*	.275	.415**
	Sig. (2-tailed)	.000	.006	.000
	N	100	100	100
employees from backgrounds where acceptable practices differ.	Pearson Correlation	.326*	.123**	.211
	Sig. (2-tailed)	.001	.221	.035
	N	100	100	100
cultural clash between employees and the organization.	Pearson Correlation	.400**	.424*	.492*
	Sig. (2-tailed)	.000	.000	.000
	N	100	100	100
insiders being motivated to harm their organization.	Pearson Correlation	.322	.296	.151
	Sig. (2-tailed)	.001	.003	.133
	N	100	100	100
insiders being vulnerable to coercion by outsider.	Pearson Correlation	.324	.374**	.441
	Sig. (2-tailed)	.001	.000	.000
	N	100	100	100
insiders being unduly motivated by financial gain.	Pearson Correlation	.225*	.525*	.525
	Sig. (2-tailed)	.024	.000	.000
	N	100	100	100
employees working from home.	Pearson Correlation	.123*	.365**	.098
	Sig. (2-tailed)	.222	.000	.333
	N	100	100	100
giving employees remote access to organizational information.	Pearson Correlation	.164	.349	.232
	Sig. (2-tailed)	.103	.000	.020
	N	100	100	100

Correlations

		technically skilled insiders who violates the security for personal gain.	employees' level of technical sophistication.	employees having formal training in computer science, IT or similar.
insufficient information security policy training and awareness.	Pearson Correlation	.314	.386*	.240*
	Sig. (2-tailed)	.001	.000	.016
	N	100	100	100
organizational culture that tolerates unethical behavior.	Pearson Correlation	.494*	.207	.104**
	Sig. (2-tailed)	.000	.039	.305
	N	100	100	100
employees from backgrounds where acceptable practices differ.	Pearson Correlation	.101*	.270**	.177
	Sig. (2-tailed)	.317	.007	.078
	N	100	100	100
cultural clash between employees and the organization.	Pearson Correlation	.416**	.398*	.168*
	Sig. (2-tailed)	.000	.000	.095
	N	100	100	100
insiders being motivated to harm their organization.	Pearson Correlation	.471	.355	.080
	Sig. (2-tailed)	.000	.000	.426
	N	100	100	100
insiders being vulnerable to coercion by outsider.	Pearson Correlation	.393	.276**	.110
	Sig. (2-tailed)	.000	.005	.276
	N	100	100	100
insiders being unduly motivated by financial gain.	Pearson Correlation	.482*	.288*	.131
	Sig. (2-tailed)	.000	.004	.193
	N	100	100	100
employees working from home.	Pearson Correlation	.241*	.225**	.290
	Sig. (2-tailed)	.016	.024	.003
	N	100	100	100
giving employees remote access to organizational information.	Pearson Correlation	.169	.420	.372
	Sig. (2-tailed)	.094	.000	.000
	N	100	100	100

Correlations

		high levels of access to IT systems given to employees.	not promptly canceling access of ex-employees.	high levels of trust given to employees.
insufficient information security policy training and awareness.	Pearson Correlation	.180	.242*	.190*
	Sig. (2-tailed)	.073	.015	.059
	N	100	100	100
organizational culture that tolerates unethical behavior.	Pearson Correlation	.235*	.366	.243**
	Sig. (2-tailed)	.018	.000	.015
	N	100	100	100
employees from backgrounds where acceptable practices differ.	Pearson Correlation	.134*	-.016**	.149
	Sig. (2-tailed)	.185	.878	.140
	N	100	100	100
cultural clash between employees and the organization.	Pearson Correlation	.362**	.289*	.097*
	Sig. (2-tailed)	.000	.004	.337
	N	100	100	100
insiders being motivated to harm their organization.	Pearson Correlation	.148	.257	.164
	Sig. (2-tailed)	.141	.010	.102
	N	100	100	100
insiders being vulnerable to coercion by outsider.	Pearson Correlation	.211	.371**	.279
	Sig. (2-tailed)	.036	.000	.005
	N	100	100	100
insiders being unduly motivated by financial gain.	Pearson Correlation	.248*	.361*	.315
	Sig. (2-tailed)	.013	.000	.001
	N	100	100	100
employees working from home.	Pearson Correlation	.420*	.176**	.419
	Sig. (2-tailed)	.000	.081	.000
	N	100	100	100
giving employees remote access to organizational information.	Pearson Correlation	.280	.164	.327
	Sig. (2-tailed)	.005	.104	.001
	N	100	100	100

Correlations

		organization ownership being limited by shares.	lack of customer and/or client participation in product development.	a poor level of health and fitness among employees.
insufficient information security policy training and awareness.	Pearson Correlation	-.142	.031*	.004*
	Sig. (2-tailed)	.158	.759	.967
	N	100	100	100
organizational culture that tolerates unethical behavior.	Pearson Correlation	-.041*	-.153	-.126**
	Sig. (2-tailed)	.687	.128	.212
	N	100	100	100
employees from backgrounds where acceptable practices differ.	Pearson Correlation	.126*	-.031**	.067
	Sig. (2-tailed)	.213	.760	.510
	N	100	100	100
cultural clash between employees and the organization.	Pearson Correlation	.054**	.005*	.105*
	Sig. (2-tailed)	.592	.958	.296
	N	100	100	100
insiders being motivated to harm their organization.	Pearson Correlation	-.139	-.198	-.131
	Sig. (2-tailed)	.167	.049	.193
	N	100	100	100
insiders being vulnerable to coercion by outsider.	Pearson Correlation	-.072	-.130**	-.015
	Sig. (2-tailed)	.476	.197	.884
	N	100	100	100
insiders being unduly motivated by financial gain.	Pearson Correlation	-.179*	-.351*	-.105
	Sig. (2-tailed)	.075	.000	.296
	N	100	100	100
employees working from home.	Pearson Correlation	.067*	.104**	.247
	Sig. (2-tailed)	.508	.303	.013
	N	100	100	100
giving employees remote access to organizational information.	Pearson Correlation	.003	.085	.125
	Sig. (2-tailed)	.977	.399	.215
	N	100	100	100

Correlations

		psychological factors such as social frustrations or computer dependency.	personal factors such as alcohol and drug addiction or violent behavior.	inappropriate or concerning behavior prior to the incident such as delays, absences and poor job performance.
allowing authorized mobile device to access organizational information from outside the organization physical boundary.	Pearson Correlation	-.031	.163*	.103*
	Sig. (2-tailed)	.756	.105	.306
	N	100	100	100
insiders' knowledge of the methods used to detect insider threat behavior.	Pearson Correlation	.234*	.094	.206**
	Sig. (2-tailed)	.019	.353	.040
	N	100	100	100
insiders' knowledge of methods to grant access to the organization's information.	Pearson Correlation	.331*	.336**	.238
	Sig. (2-tailed)	.001	.001	.017
	N	100	100	100
insiders' knowledge of the potential value of the organization's information to outsiders.	Pearson Correlation	.227**	.280*	.139*
	Sig. (2-tailed)	.023	.005	.169
	N	100	100	100
technically skilled insiders who violates the security for personal gain.	Pearson Correlation	.338	.421	.097
	Sig. (2-tailed)	.001	.000	.336
	N	100	100	100
employees' level of technical sophistication.	Pearson Correlation	.325	.089**	.175
	Sig. (2-tailed)	.001	.379	.081
	N	100	100	100
employees having formal training in computer science, IT or similar.	Pearson Correlation	.267*	.140*	.312
	Sig. (2-tailed)	.007	.165	.002
	N	100	100	100
high levels of access to IT systems given to employees.	Pearson Correlation	.200*	.232**	.219
	Sig. (2-tailed)	.046	.020	.029
	N	100	100	100
not promptly canceling access of ex-employees.	Pearson Correlation	.242	.260	.221
	Sig. (2-tailed)	.015	.009	.027

Correlations

		outsourced employees being given the same logical and/or physical access as the organization's regular employees.	the organization engaging a relatively high number of outsourcing agreements.	granting access to third- parties contracted to conduct work within the organization.
allowing authorized mobile device to access organizational information from outside the organization physical boundary.	Pearson Correlation	.062	.379*	.382*
	Sig. (2-tailed)	.537	.000	.000
	N	100	100	100
insiders' knowledge of the methods used to detect insider threat behavior.	Pearson Correlation	.126*	.286	.369**
	Sig. (2-tailed)	.210	.004	.000
	N	100	100	100
insiders' knowledge of methods to grant access to the organization's information.	Pearson Correlation	.246*	.337**	.461
	Sig. (2-tailed)	.014	.001	.000
	N	100	100	100
insiders' knowledge of the potential value of the organization's information to outsiders.	Pearson Correlation	.293**	.429*	.401*
	Sig. (2-tailed)	.003	.000	.000
	N	100	100	100
technically skilled insiders who violates the security for personal gain.	Pearson Correlation	.305	.311	.389
	Sig. (2-tailed)	.002	.002	.000
	N	100	100	100
employees' level of technical sophistication.	Pearson Correlation	.200	.262**	.320
	Sig. (2-tailed)	.047	.009	.001
	N	100	100	100
employees having formal training in computer science, IT or similar.	Pearson Correlation	.396*	.109*	.268
	Sig. (2-tailed)	.000	.281	.007
	N	100	100	100
high levels of access to IT systems given to employees.	Pearson Correlation	.168*	.380**	.370
	Sig. (2-tailed)	.094	.000	.000
	N	100	100	100
not promptly canceling access of ex-employees.	Pearson Correlation	.178	.131	.294
	Sig. (2-tailed)	.077	.193	.003

Correlations

		the implementation of inappropriate information security policy.	outdated information security procedures or policies.	insufficient information security policy training and awareness.
allowing authorized mobile device to access organizational information from outside the organization physical boundary.	Pearson Correlation	.136	.193*	.279*
	Sig. (2-tailed)	.177	.054	.005
	N	100	100	100
insiders' knowledge of the methods used to detect insider threat behavior.	Pearson Correlation	.221*	.263	.288**
	Sig. (2-tailed)	.027	.008	.004
	N	100	100	100
insiders' knowledge of methods to grant access to the organization's information.	Pearson Correlation	.363*	.496**	.364
	Sig. (2-tailed)	.000	.000	.000
	N	100	100	100
insiders' knowledge of the potential value of the organization's information to outsiders.	Pearson Correlation	.308**	.289*	.297*
	Sig. (2-tailed)	.002	.004	.003
	N	100	100	100
technically skilled insiders who violates the security for personal gain.	Pearson Correlation	.468	.536	.314
	Sig. (2-tailed)	.000	.000	.001
	N	100	100	100
employees' level of technical sophistication.	Pearson Correlation	.224	.387**	.386
	Sig. (2-tailed)	.025	.000	.000
	N	100	100	100
employees having formal training in computer science, IT or similar.	Pearson Correlation	.254*	.125*	.240
	Sig. (2-tailed)	.011	.216	.016
	N	100	100	100
high levels of access to IT systems given to employees.	Pearson Correlation	.237*	.296**	.180
	Sig. (2-tailed)	.017	.003	.073
	N	100	100	100
not promptly canceling access of ex-employees.	Pearson Correlation	.296	.456	.242
	Sig. (2-tailed)	.003	.000	.015

Correlations

		organizational culture that tolerates unethical behavior.	employees from backgrounds where acceptable practices differ.	cultural clash between employees and the organization.
allowing authorized mobile device to access organizational information from outside the organization physical boundary.	Pearson Correlation	.182	.156*	.256*
	Sig. (2-tailed)	.069	.122	.010
	N	100	100	100
insiders' knowledge of the methods used to detect insider threat behavior.	Pearson Correlation	.414**	.326	.400**
	Sig. (2-tailed)	.000	.001	.000
	N	100	100	100
insiders' knowledge of methods to grant access to the organization's information.	Pearson Correlation	.275**	.123**	.424
	Sig. (2-tailed)	.006	.221	.000
	N	100	100	100
insiders' knowledge of the potential value of the organization's information to outsiders.	Pearson Correlation	.415**	.211*	.492*
	Sig. (2-tailed)	.000	.035	.000
	N	100	100	100
technically skilled insiders who violates the security for personal gain.	Pearson Correlation	.494	.101	.416
	Sig. (2-tailed)	.000	.317	.000
	N	100	100	100
employees' level of technical sophistication.	Pearson Correlation	.207	.270**	.398
	Sig. (2-tailed)	.039	.007	.000
	N	100	100	100
employees having formal training in computer science, IT or similar.	Pearson Correlation	.104*	.177*	.168
	Sig. (2-tailed)	.305	.078	.095
	N	100	100	100
high levels of access to IT systems given to employees.	Pearson Correlation	.235**	.134**	.362
	Sig. (2-tailed)	.018	.185	.000
	N	100	100	100
not promptly canceling access of ex-employees.	Pearson Correlation	.366	-.016	.289
	Sig. (2-tailed)	.000	.878	.004

Correlations

		insiders being motivated to harm their organization.	insiders being vulnerable to coercion by outsider.	insiders being unduly motivated by financial gain.
allowing authorized mobile device to access organizational information from outside the organization physical boundary.	Pearson Correlation	.033	.193*	.172*
	Sig. (2-tailed)	.747	.054	.087
	N	100	100	100
insiders' knowledge of the methods used to detect insider threat behavior.	Pearson Correlation	.322*	.324	.225**
	Sig. (2-tailed)	.001	.001	.024
	N	100	100	100
insiders' knowledge of methods to grant access to the organization's information.	Pearson Correlation	.296*	.374**	.525
	Sig. (2-tailed)	.003	.000	.000
	N	100	100	100
insiders' knowledge of the potential value of the organization's information to outsiders.	Pearson Correlation	.151**	.441*	.525*
	Sig. (2-tailed)	.133	.000	.000
	N	100	100	100
technically skilled insiders who violates the security for personal gain.	Pearson Correlation	.471	.393	.482
	Sig. (2-tailed)	.000	.000	.000
	N	100	100	100
employees' level of technical sophistication.	Pearson Correlation	.355	.276**	.288
	Sig. (2-tailed)	.000	.005	.004
	N	100	100	100
employees having formal training in computer science, IT or similar.	Pearson Correlation	.080*	.110*	.131
	Sig. (2-tailed)	.426	.276	.193
	N	100	100	100
high levels of access to IT systems given to employees.	Pearson Correlation	.148*	.211**	.248
	Sig. (2-tailed)	.141	.036	.013
	N	100	100	100
not promptly canceling access of ex-employees.	Pearson Correlation	.257	.371	.361
	Sig. (2-tailed)	.010	.000	.000

Correlations

		employees working from home.	giving employees remote access to organizational information.	allowing authorized mobile device to access organizational information from outside the organization physical boundary.
allowing authorized mobile device to access organizational information from outside the organization physical boundary.	Pearson Correlation	.227	.372*	1*
	Sig. (2-tailed)	.023	.000	
	N	100	100	100
insiders' knowledge of the methods used to detect insider threat behavior.	Pearson Correlation	.123*	.164	.182**
	Sig. (2-tailed)	.222	.103	.071
	N	100	100	100
insiders' knowledge of methods to grant access to the organization's information.	Pearson Correlation	.365*	.349**	.390
	Sig. (2-tailed)	.000	.000	.000
	N	100	100	100
insiders' knowledge of the potential value of the organization's information to outsiders.	Pearson Correlation	.098**	.232*	.353*
	Sig. (2-tailed)	.333	.020	.000
	N	100	100	100
technically skilled insiders who violates the security for personal gain.	Pearson Correlation	.241	.169	.207
	Sig. (2-tailed)	.016	.094	.039
	N	100	100	100
employees' level of technical sophistication.	Pearson Correlation	.225	.420**	.180
	Sig. (2-tailed)	.024	.000	.074
	N	100	100	100
employees having formal training in computer science, IT or similar.	Pearson Correlation	.290*	.372*	.137
	Sig. (2-tailed)	.003	.000	.175
	N	100	100	100
high levels of access to IT systems given to employees.	Pearson Correlation	.420*	.280**	.401
	Sig. (2-tailed)	.000	.005	.000
	N	100	100	100
not promptly canceling access of ex-employees.	Pearson Correlation	.176	.164	.027
	Sig. (2-tailed)	.081	.104	.793

Correlations

		insiders' knowledge of the methods used to detect insider threat behavior.	insiders' knowledge of methods to grant access to the organization's information.	insiders' knowledge of the potential value of the organization's information to outsiders.
allowing authorized mobile device to access organizational information from outside the organization physical boundary.	Pearson Correlation	.182	.390*	.353*
	Sig. (2-tailed)	.071	.000	.000
	N	100	100	100
insiders' knowledge of the methods used to detect insider threat behavior.	Pearson Correlation	1*	.294	.324**
	Sig. (2-tailed)		.003	.001
	N	100	100	100
insiders' knowledge of methods to grant access to the organization's information.	Pearson Correlation	.294*	1**	.460
	Sig. (2-tailed)	.003		.000
	N	100	100	100
insiders' knowledge of the potential value of the organization's information to outsiders.	Pearson Correlation	.324**	.460*	1*
	Sig. (2-tailed)	.001	.000	
	N	100	100	100
technically skilled insiders who violates the security for personal gain.	Pearson Correlation	.395	.425	.449
	Sig. (2-tailed)	.000	.000	.000
	N	100	100	100
employees' level of technical sophistication.	Pearson Correlation	.332	.485**	.330
	Sig. (2-tailed)	.001	.000	.001
	N	100	100	100
employees having formal training in computer science, IT or similar.	Pearson Correlation	.170*	.376*	.049
	Sig. (2-tailed)	.091	.000	.627
	N	100	100	100
high levels of access to IT systems given to employees.	Pearson Correlation	.461*	.455**	.312
	Sig. (2-tailed)	.000	.000	.002
	N	100	100	100
not promptly canceling access of ex-employees.	Pearson Correlation	.268	.388	.289
	Sig. (2-tailed)	.007	.000	.004

Correlations

		technically skilled insiders who violates the security for personal gain.	employees' level of technical sophistication.	employees having formal training in computer science, IT or similar.
allowing authorized mobile device to access organizational information from outside the organization physical boundary.	Pearson Correlation	.207	.180*	.137*
	Sig. (2-tailed)	.039	.074	.175
	N	100	100	100
insiders' knowledge of the methods used to detect insider threat behavior.	Pearson Correlation	.395*	.332	.170**
	Sig. (2-tailed)	.000	.001	.091
	N	100	100	100
insiders' knowledge of methods to grant access to the organization's information.	Pearson Correlation	.425*	.485**	.376
	Sig. (2-tailed)	.000	.000	.000
	N	100	100	100
insiders' knowledge of the potential value of the organization's information to outsiders.	Pearson Correlation	.449**	.330*	.049*
	Sig. (2-tailed)	.000	.001	.627
	N	100	100	100
technically skilled insiders who violates the security for personal gain.	Pearson Correlation	1	.320	.121
	Sig. (2-tailed)		.001	.231
	N	100	100	100
employees' level of technical sophistication.	Pearson Correlation	.320	1**	.347
	Sig. (2-tailed)	.001		.000
	N	100	100	100
employees having formal training in computer science, IT or similar.	Pearson Correlation	.121*	.347*	1
	Sig. (2-tailed)	.231	.000	
	N	100	100	100
high levels of access to IT systems given to employees.	Pearson Correlation	.257*	.321**	.305
	Sig. (2-tailed)	.010	.001	.002
	N	100	100	100
not promptly canceling access of ex-employees.	Pearson Correlation	.547	.221	.104
	Sig. (2-tailed)	.000	.027	.301

Correlations

		high levels of access to IT systems given to employees.	not promptly canceling access of ex-employees.	high levels of trust given to employees.
allowing authorized mobile device to access organizational information from outside the organization physical boundary.	Pearson Correlation	.401	.027*	.354*
	Sig. (2-tailed)	.000	.793	.000
	N	100	100	100
insiders' knowledge of the methods used to detect insider threat behavior.	Pearson Correlation	.461*	.268	.133**
	Sig. (2-tailed)	.000	.007	.188
	N	100	100	100
insiders' knowledge of methods to grant access to the organization's information.	Pearson Correlation	.455*	.388**	.555
	Sig. (2-tailed)	.000	.000	.000
	N	100	100	100
insiders' knowledge of the potential value of the organization's information to outsiders.	Pearson Correlation	.312**	.289*	.274*
	Sig. (2-tailed)	.002	.004	.006
	N	100	100	100
technically skilled insiders who violates the security for personal gain.	Pearson Correlation	.257	.547	.235
	Sig. (2-tailed)	.010	.000	.018
	N	100	100	100
employees' level of technical sophistication.	Pearson Correlation	.321	.221**	.278
	Sig. (2-tailed)	.001	.027	.005
	N	100	100	100
employees having formal training in computer science, IT or similar.	Pearson Correlation	.305*	.104*	.589
	Sig. (2-tailed)	.002	.301	.000
	N	100	100	100
high levels of access to IT systems given to employees.	Pearson Correlation	1*	.163**	.385
	Sig. (2-tailed)		.104	.000
	N	100	100	100
not promptly canceling access of ex-employees.	Pearson Correlation	.163	1	.232
	Sig. (2-tailed)	.104		.020

Correlations

		organization ownership being limited by shares.	lack of customer and/or client participation in product development.	a poor level of health and fitness among employees.
allowing authorized mobile device to access organizational information from outside the organization physical boundary.	Pearson Correlation	.014	.158*	.030*
	Sig. (2-tailed)	.893	.117	.770
	N	100	100	100
insiders' knowledge of the methods used to detect insider threat behavior.	Pearson Correlation	-.123*	-.101	-.093**
	Sig. (2-tailed)	.222	.318	.356
	N	100	100	100
insiders' knowledge of methods to grant access to the organization's information.	Pearson Correlation	-.074*	-.034**	.013
	Sig. (2-tailed)	.462	.736	.900
	N	100	100	100
insiders' knowledge of the potential value of the organization's information to outsiders.	Pearson Correlation	-.076**	-.142*	-.033*
	Sig. (2-tailed)	.450	.159	.742
	N	100	100	100
technically skilled insiders who violates the security for personal gain.	Pearson Correlation	-.209	-.021	-.075
	Sig. (2-tailed)	.037	.833	.460
	N	100	100	100
employees' level of technical sophistication.	Pearson Correlation	-.145	-.090**	.076
	Sig. (2-tailed)	.149	.373	.451
	N	100	100	100
employees having formal training in computer science, IT or similar.	Pearson Correlation	.063*	.197*	.128
	Sig. (2-tailed)	.532	.049	.204
	N	100	100	100
high levels of access to IT systems given to employees.	Pearson Correlation	-.189*	.071**	.093
	Sig. (2-tailed)	.060	.483	.358
	N	100	100	100
not promptly canceling access of ex-employees.	Pearson Correlation	.016	-.072	-.177
	Sig. (2-tailed)	.873	.474	.079

		psychological factors such as social frustrations or computer dependency.	personal factors such as alcohol and drug addiction or violent behavior.	inappropriate or concerning behavior prior to the incident such as delays, absences and poor job performance.
not promptly canceling access of ex-employees.	N	100	100*	100*
high levels of trust given to employees.	Pearson Correlation	.317	.207	.210
	Sig. (2-tailed)	.001	.039	.036
	N	100*	100	100**
organization ownership being limited by shares.	Pearson Correlation	.118	-.016	.094
	Sig. (2-tailed)	.241	.876	.354
	N	100*	100**	100
lack of customer and/or client participation in product development.	Pearson Correlation	-.054	-.007	-.038
	Sig. (2-tailed)	.592	.942	.706
	N	100**	100*	100*
a poor level of health and fitness among employees.	Pearson Correlation	.056	.019	.160
	Sig. (2-tailed)	.579	.854	.111
	N	100	100	100

		outsourced employees being given the same logical and/or physical access as the organization's regular employees.	the organization engaging a relatively high number of outsourcing agreements.	granting access to third- parties contracted to conduct work within the organization.
not promptly canceling access of ex-employees.	N	100	100*	100*
high levels of trust given to employees.	Pearson Correlation	.383	.283	.255
	Sig. (2-tailed)	.000	.004	.010
	N	100*	100	100**
organization ownership being	Pearson Correlation	-.120	-.177	-.033

limited by shares.	Sig. (2-tailed)	.235	.079	.745
	N	100*	100**	100
lack of customer and/or client participation in product development.	Pearson Correlation	-.125	-.172	.028
	Sig. (2-tailed)	.214	.087	.784
	N	100**	100*	100*
a poor level of health and fitness among employees.	Pearson Correlation	.064	.099	.018
	Sig. (2-tailed)	.527	.327	.857
	N	100	100	100

Correlations

		the implementation of inappropriate information security policy.	outdated information security procedures or policies.	insufficient information security policy training and awareness.
not promptly canceling access of ex-employees.	N	100	100*	100*
high levels of trust given to employees.	Pearson Correlation	.295	.266	.190
	Sig. (2-tailed)	.003	.007	.059
	N	100*	100	100**
organization ownership being limited by shares.	Pearson Correlation	-.271	-.195	-.142
	Sig. (2-tailed)	.006	.052	.158
	N	100*	100**	100
lack of customer and/or client participation in product development.	Pearson Correlation	-.116	-.080	.031
	Sig. (2-tailed)	.251	.427	.759
	N	100**	100*	100*
a poor level of health and fitness among employees.	Pearson Correlation	-.077	-.107	.004
	Sig. (2-tailed)	.449	.290	.967
	N	100	100	100

Correlations

		organizational culture that tolerates unethical behavior.	employees from backgrounds where acceptable practices differ.	cultural clash between employees and the organization.
not promptly canceling access of ex-employees.	N	100	100*	100*
high levels of trust given to	Pearson Correlation	.243	.149	.097

employees.	Sig. (2-tailed)	.015	.140	.337
	N	100*	100	100**
organization ownership being limited by shares.	Pearson Correlation	-.041	.126	.054
	Sig. (2-tailed)	.687	.213	.592
	N	100*	100**	100
lack of customer and/or client participation in product development.	Pearson Correlation	-.153	-.031	.005
	Sig. (2-tailed)	.128	.760	.958
	N	100**	100*	100*
a poor level of health and fitness among employees.	Pearson Correlation	-.126	.067	.105
	Sig. (2-tailed)	.212	.510	.296
	N	100	100	100

Correlations

		insiders being motivated to harm their organization.	insiders being vulnerable to coercion by outsider.	insiders being unduly motivated by financial gain.
not promptly cancelling access of ex-employees.	N	100	100*	100*
high levels of trust given to employees.	Pearson Correlation	.164	.279	.315
	Sig. (2-tailed)	.102	.005	.001
	N	100*	100	100**
organization ownership being limited by shares.	Pearson Correlation	-.139	-.072	-.179
	Sig. (2-tailed)	.167	.476	.075
	N	100*	100**	100
lack of customer and/or client participation in product development.	Pearson Correlation	-.198	-.130	-.351
	Sig. (2-tailed)	.049	.197	.000
	N	100**	100*	100*
a poor level of health and fitness among employees.	Pearson Correlation	-.131	-.015	-.105
	Sig. (2-tailed)	.193	.884	.296
	N	100	100	100

Correlations

		employees working from home.	giving employees remote access to organizational information.	allowing authorized mobile device to access organizational information from outside the organization physical boundary.
not promptly canceling access of ex-employees.	N	100	100*	100*
high levels of trust given to employees.	Pearson Correlation	.419	.327	.354
	Sig. (2-tailed)	.000	.001	.000
	N	100*	100	100**
organization ownership being limited by shares.	Pearson Correlation	.067	.003	.014
	Sig. (2-tailed)	.508	.977	.893
	N	100*	100**	100
lack of customer and/or client participation in product development.	Pearson Correlation	.104	.085	.158
	Sig. (2-tailed)	.303	.399	.117
	N	100**	100*	100*
a poor level of health and fitness among employees.	Pearson Correlation	.247	.125	.030
	Sig. (2-tailed)	.013	.215	.770
	N	100	100	100

Correlations

		insiders' knowledge of the methods used to detect insider threat behavior.	insiders' knowledge of methods to grant access to the organization's information.	insiders' knowledge of the potential value of the organization's information to outsiders.
not promptly canceling access of ex-employees.	N	100	100*	100*
high levels of trust given to employees.	Pearson Correlation	.133	.555	.274
	Sig. (2-tailed)	.188	.000	.006
	N	100*	100	100**
organization ownership being limited by shares.	Pearson Correlation	-.123	-.074	-.076
	Sig. (2-tailed)	.222	.462	.450

	N	100*	100**	100
lack of customer and/or client participation in product development.	Pearson Correlation	-.101	-.034	-.142
	Sig. (2-tailed)	.318	.736	.159
	N	100**	100*	100*
a poor level of health and fitness among employees.	Pearson Correlation	-.093	.013	-.033
	Sig. (2-tailed)	.356	.900	.742
	N	100	100	100

Correlations

		technically skilled insiders who violates the security for personal gain.	employees' level of technical sophistication.	employees having formal training in computer science, IT or similar.
not promptly canceling access of ex-employees.	N	100	100*	100*
high levels of trust given to employees.	Pearson Correlation	.235	.278	.589
	Sig. (2-tailed)	.018	.005	.000
	N	100*	100	100**
organization ownership being limited by shares.	Pearson Correlation	-.209	-.145	.063
	Sig. (2-tailed)	.037	.149	.532
	N	100*	100**	100
lack of customer and/or client participation in product development.	Pearson Correlation	-.021	-.090	.197
	Sig. (2-tailed)	.833	.373	.049
	N	100**	100*	100*
a poor level of health and fitness among employees.	Pearson Correlation	-.075	.076	.128
	Sig. (2-tailed)	.460	.451	.204
	N	100	100	100

Correlations

		high levels of access to IT systems given to employees.	not promptly canceling access of ex-employees.	high levels of trust given to employees.
not promptly canceling access of ex-employees.	N	100	100*	100*
high levels of trust given to	Pearson Correlation	.385	.232	1

employees.	Sig. (2-tailed)	.000	.020	
	N	100*	100	100**
organization ownership being limited by shares.	Pearson Correlation	-.189	.016	.006
	Sig. (2-tailed)	.060	.873	.950
	N	100*	100**	100
lack of customer and/or client participation in product development.	Pearson Correlation	.071	-.072	.131
	Sig. (2-tailed)	.483	.474	.195
	N	100**	100*	100*
a poor level of health and fitness among employees.	Pearson Correlation	.093	-.177	.186
	Sig. (2-tailed)	.358	.079	.065
	N	100	100	100

Correlations

		organization ownership being limited by shares.	lack of customer and/or client participation in product development.	a poor level of health and fitness among employees.
not promptly canceling access of ex-employees.	N	100	100*	100*
high levels of trust given to employees.	Pearson Correlation	.006	.131	.186
	Sig. (2-tailed)	.950	.195	.065
	N	100*	100	100**
organization ownership being limited by shares.	Pearson Correlation	1	.400	.241
	Sig. (2-tailed)		.000	.016
	N	100*	100**	100
lack of customer and/or client participation in product development.	Pearson Correlation	.400	1	.449
	Sig. (2-tailed)	.000		.000
	N	100**	100*	100*
a poor level of health and fitness among employees.	Pearson Correlation	.241	.449	1
	Sig. (2-tailed)	.016	.000	
	N	100	100	100

*. Correlation is significant at the 0.05 level (2-tailed).

**. Correlation is significant at the 0.01 level (2-tailed).

Appendix 3: Invitation Letter

Curtin University
School of Information Systems

A study of insider threat behaviour: Developing a holistic framework

My name is Asmaa Munshi. I am a doctoral candidate in the school of information systems at Curtin University in Western Australia. I am conducting research into insider threat behaviour. My research aims to identify factors that are correlated with the insider threat behaviour.

This email is seeking your permission to participate in an email interview to evaluate my draft insider threat model. This process will take more than one email between me and you to discuss this issue. If you decide to participate, you will be asked to complete a couple of questions about insider threat contributing factors from your perspective and experience. The interview will start with general questions regarding the insider threat cases that you have experienced and then asking you to evaluate my model about insider threat factors. Your participation is anonymous and your identity will not be published or disclosed.

This research aims to minimize the problems of the insider threat by providing a management framework how to manage insider behaviour and increase the users' awareness. The contributions of this research are applicable to businesses and users' needs, especially in security and IT departments.

I will keep you updated on my results of this study and at the end of my degree I will share with you my management framework.

If you would like to participate, please contact me at the email or number listed below to discuss your participation and email you the "participant information sheet" to understand more about my study, and later we can start off the interview.

Your help and cooperation is highly appreciated

With kind regards,
Asmaa Munshi
Perth, Western Australia

Phone number: +61423507092
E-mail: a.munshi@postgrad.curtin.edu.au

Appendix 4: Participant Information Sheet

Curtin University
School of Information System

A study of insider threat behaviour: Developing a holistic framework

My name is Asmaa Munshi; I am a PhD student at Curtin University, and I am conducting research into insider threat behaviour, in particular my research aim to identify factors that are correlated with this issue.

Introduction

Any security system relies upon its operators, even if it is designed and implemented in a perfect manner. Organisations face ongoing threats and attacks from external and internal sources. Insider attacks are associated with legitimate users who abuse their privileges and can easily cause significant damage or loss to an organisation. The overall aim of this research is to develop a conceptual insider threat model that can frame a holistic view of insider threat behaviour and inform the deviloping of a framework to manage the insider threat. Previous research in this area focused on quite narrow and specific areas and most of the models and frameworks developed so far specialise in either people to people relationships, segmentation of tasks, access to information or network architectures. Little research published so far gives a bigger picture in regard to insider threat behaviour. Therefore, this research amis to gain a holistic view of the insider threat through understanding the factors that influence insider threat behaviour, both by individuals and organisations, and then develop a framework which centres on security measures to manage insider threat behaviour.

Purpose of Research

This research will minimize the problem of the insider threat by providing a management framework to manage insider behaviour and increase the awareness of users. The contributions of this research are applicable to business and user needs especially in security and IT departments.

Purpose of interview

- To gather information about factors that influences the insider to behave inappropriately with to manage these factors.
- The primary point of these interviews is to evaluate my insider threat model.

- The results and recommendations obtain from the interviews will helps me to enhance and improve my model.

Please note:

- The interview process will take approximately 45 minutes.
- The interview will be recorded to help with deciphering and analysing.
- Your privacy is greatly respected and any information that could identify you will not be published at any time.
- All information will be stored in a secure location at Curtin University for five years.
- Taking part is voluntary and you can withdrawal at any time.
- Your withdrawal would not affect you in any way.

Thank you very much for you time. Please keep this letter for your information.

This study has been approved under Curtin University's process for lower-risk Studies (Approval Number IS_12_31). This process complies with the National Statement on Ethical Conduct in Human Research (Chapter 5.1.7 and Chapters 5.1.18-5.1.21).For further information on this study contact the researchers named above on 0423507092 or the Curtin University Human Research Ethics Committee. c/- Office of Research and Development, Curtin University, GPO Box U1987, Perth 6845 or by telephoning 9266 9223 or by emailing hrec@curtin.edu.au.

Appendix 5: Consent Form

Curtin University
School of Information Systems

A study of insider threat behaviour: Developing a holistic framework

- I understand the purpose and procedures of the study.
- I have been provided with the participant information sheet.
- I understand that the procedure itself may not benefit me.
- I understand that my involvement is voluntary and I can withdraw at any time without problem.
- I understand that no personal identifying information like my name and address will be used and that all information will be securely stored for 5 years before being destroyed.
- I have been given the opportunity to ask questions.
- I agree to participate in the study outlined to me.

Name: ———————— Signature: ————————

Date: ————————

Investigator: **Asmaa Munshi**

Research supervisor: **Peter Dell**

Appendix 6: Semi-structured Interview Questions

1- I would like to start with your experience how long you have been work and what is your job title?

2- As security specialists, what does *"insider threat"* mean to you?

3- Have you experienced any cases of insider threat in your organisation?
   a. Share with us this experience.

4- Are there any risk factors that we should look out for? Are there any evidences that someone might be an insider?

5- "Conflict between the organisation and an individual who is willing and able to seek personal gain at the organisation's expense".
   a. Share with us your perspective behind the risk of insider threat and effect on the organisation?
   b. From your perspective how to minimize this problem?
   c. Do you have any suggestion strategies to address this issue?

6- Out of your experience, do you agree that giving high trust to underachieving employee may affect the insider threat behaviour?
   a. If yes Why, if no Why not?
   b. What are your thoughts to minimize this problem?
   c. Do you have any suggestion strategies to address this issue?

7- Outside influence: employees' background, employees coercion by outsider or the use of outsourced employees.
   a. How outside influence increase the risk of insider threat behaviour?

b. What is your opinion to minimize this problem?

8- Do you agree that "knowledge of the insiders especially their awareness about the methods used to detect insider threat behaviour" can influence the insider to behave inappropriately?
   a. If yes Why, if no Why not?
   b. How this problem could be minimized in your estimation?

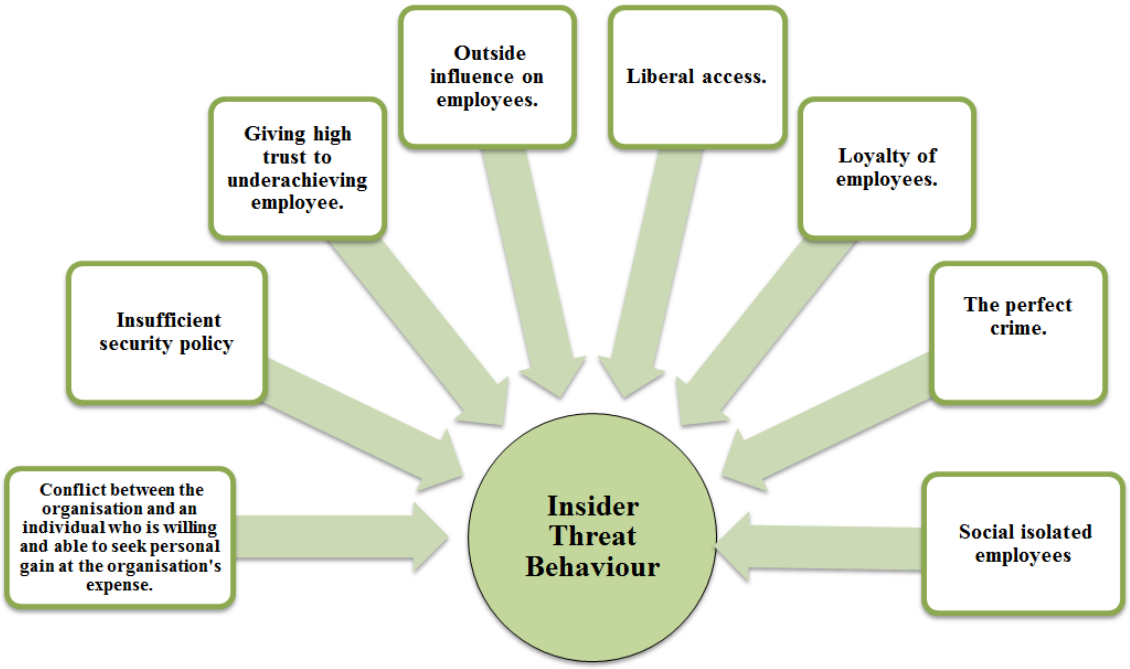
9- From your experience, do you think "Insufficient security policy" increase the insider threat behaviour?
   a. If yes Why, if no Why not?
   b. What are your thoughts to minimize this problem?
   c. Do you have any suggestion strategies to address this issue?

10- Out of your knowledge, can you please give any example how social isolated workers increase the risk of insider threat behaviour?
   a. What are your ideas to minimize this problem?
   b. Do you have any suggestion strategies to address this issue?

11- "Liberal access for the employees"
   a. From your experience, can you please define liberal access?
   b. How liberal access can influence the insider to behave wrongly?
   c. What are your thoughts to minimize this problem?
   d. Do you have any suggestion strategies to address this issue?

12- "Loyalty of workers"
   a. How loyalty may affect the insider threat behaviour?
   b. From your experience, how this problem can be minimized?

13- Do you have any documentation or guideline in your organisation about risk factors?



Factors Contributing to Insider Threat Behaviour

14- If you could add any factors to the model or delete any factors from the model, what would it be? Why these specific factors are essential?

15- Based on your experience, what are the factors you consider more common than others? Why these specific factors are essential?

Appendix 7: Interview Sample Script

1- I would like to start with your experience how long you have been work and what is your job title?

My job title is the Chief Information Security Officer. I've been involved in the security industry for over thirty years, and have attained certifications in both the traditional/physical and IT security environments (CPP and CISSP designations).

2- As security specialists, what does "insider threat" mean to you?
What does insider threat mean to me?

My definition of an insider threat is the possible avenues an employee/contractor/volunteer could use to compromise an organization's People, Property or Information. An insider threat is one of the most difficult to defend against because an employee/contractor/volunteer inherently has a pre-defined level of access to an organization's resources. It is this access, or the escalation of access, that leads to most insider threats being realized.

3- Have you experienced any cases of insider threat in your organisation?
Share with us this experience?

In the earlier phases of my career, I was exposed to insider threats and the consequences of these threats being realized. In one case, a previous organization I worked at was targeted by corporate espionage teams, seeking to gain greater market share. An employee was hired into one of my previous employer's workspace, this new employee got to know other employees and what they did, eventually stealing

marketing plans for an increasing market and then left the company after stealing company marketing plans. My organization suffered a direct loss from this event, but we could not criminally prove the charge.

The case I identified was attributed to corporate espionage. The actor was motivated by greed to steal the marketing plan and provide it to a competitor. We were unable to determine if the other corporation had compromised our employee (i.e. blackmail, veiled threat, etc.).

4- Are there any risk factors that we should look out for? Are there any evidences that someone might be an insider?

Again, my perspective of insider threats is from the corporate world. We categorized them into unplanned/opportunistic and planned threat vectors. As for clues, there- are a number of indicators that have consistently been uncovered during post-incident reviews. These include:

- an employee is identified to have poor credit or is in significant financial hardship
- an employee is displaying negative or neutral behaviour at work: either withdrawing from some social groups, or expressing anger/disappointment to the organization
- an employee is displaying a sudden interest in areas outside of their scope of control. The interest begins quietly enough, but becomes more persistent over time.
- an employee may be suffering marital problems, or problems with loved ones at home
- an employee begins to display aggressive behaviour in meetings, or with co-workers
- an employee begins to display odd or out of character work habits: showing up early or on weekends, staying late, working through lunch hours.
- an employee begins to make "justifying" statements, such as "they owe me".

- an employee is found to have made unflattering comments in social media posts, etc.

From a technical perspective, there are indicators as well:
- increased attempts to access confidential files/folders from outside the department
- increased use of remote access software, during off business hours
- increased file transfer activity during off business hours, either on premise or via remote connection.
- Attempts to increase privilege levels for "typical" business system users.
- Fumbled or aggressive calls to a help desk team to try and change someone's user ID/password that has higher privileges than other accounts.
- Increased traffic to social media sites, or to POP email accounts.
- increased file transfer traffic to upload sites, or to personal POP email accounts

5- "Conflict between the organisation and an individual who is willing and able to seek personal gain at the organisation's expense".

a- Can you please give any example from your experience how previous sentence increase the risk of insider threat and affect and organisation?

My personal experience, from previous positions, is that an insider with a real or perceived conflict with an organization is a greater threat than from an outside party. A motivated actor with inside access to assets, etc. has greater opportunity to impact an organization.

In previous organizations, I dealt with an inside threat stemming from an employee who took advantage of the organization while on sick leave. The

employee had justified the offense by stating they were upset at the organization not providing full benefits while on leave, and then took advantage of the corporation by working for a competitor. While we were unable to fully estimate the damage, we did identify that some information was missing and eventually attributed the loss to the employee.

b- From your perspective how to minimize this problem?

Keep the employees happy. Build with them an air of trust & rapport; keep listening from them through weekly casual social meetings if they are having any rough times or complaints against the organization. Moreover, an organization must have well-established control frameworks in place to manage, review and audit access to assets by employees. The assets could be the organization's people, property or information but each type of asset can have a series of controls in place to limit access and/or reduce threats by malicious forces.

c- Do you have any suggestion strategies to address this issue?

- Review the Recruitment policy in a way that personality screening is done through an expert who can foresee problems from a potential employee.
- Review HR policy in organization for bonuses, appreciations and rewards. No stone must be unturned to keep employees loyal &happy.
- Weekly social gathering (e.g. breakfast) to add some social spice to the team.
- Define and execute severe punitive actions for employees found doing breaching so that others would refrain from trying similar actions in future.
- <u>Improve Managers:</u> Train managers biyearly for:

- Team-building & Leadership skills (Leading is the best way to Manage)
- Internal threat analysis screening skills

6- Out of your experience, do you agree that giving high trust to underachieving employee may affect the insider threat behaviour?

a- If yes Why, if no Why not?

Yes it does. The probability of risks from employees with low performance and lack of core capabilities is very high. The problem becomes even greater if they had a high degree of trust and access.

b- What are your thoughts to minimize this problem?

- Review and provide adequate training to low performers lacking skills.
- Personality and Suitability check of other low performers (seeming to lack core capabilities) and assign them better suited responsibilities as per their capabilities.
- Downsize employees not needed.

c- Do you have any suggestion strategies to address this issue?

Apart from above mentioned:

- Periodic evaluation of employees for performance and root cause analysis to perform the above mentioned.
- Organization internal roles and responsibilities must be reviewed in such a way that criticality of available data (or propriety info) flows

down the stream i.e. the most critical data stays with the top order and the least important data/responsibilities stay with the bottom order.

7- *Outside influence: employees' background, employees' coercion by outsider or the use of outsourced employees*.

a- How outside influence increase the risk of insider threat behaviour?

Increased risks in all such cases

- Weak values and less moral personalities.
- People doing multiple and similar jobs
- Outsourcers may deploy staff to steal info. Also outsourced resources are less careful (why should they care?)
- What is your opinion to minimize this problem?
- Reduce outsourcing: Capitalize on own resources.
- Signatures on stringent NDA (Non-Disclosure Agreements) signed with all employees specially the outsourcer company.
- NDAs (Non-Disclosure Agreements) are important entities that secure organizations against vulnerabilities. In most simplified words, these are agreements that the invited parties will not steal, sell, misuse the information while working in or for that organization. If violations done, the organization can sue the violators in court.
- All organizations (wherever applicable) must get NDAs signed with:
    - its employees (as part of recruitment)
    - any outsourcing companies who'll send staff to this organization for work (even for janitor services).

Roles and responsibilities review as I stated above.

- Special provisions in all employee contracts barring them to do multiple similar jobs.
- Provisions in HR for severe punitive actions as stated above.

8- Do you agree that "knowledge of the insiders especially their awareness about the methods used to detect insider threat behaviour" can influence the insider to behave inappropriately?

a- If yes Why, if no Why not?

Obviously, if the insiders know how their posed threats or actions are detected, they'll find out ways to compromise the measures taken. As a matter of fact, any risks can be mitigated or minimized; they can never be eliminated to zero level. Our concern must always be to have least possible residual risk.

I believe an insider's knowledge about existing controls (or lack thereof) can influence behaviour. If an insider has the requisite motivation and opportunity, and if they learn that there is a limited chance of being detected, all three components of an event/theft/etc. triangle are present.

Reducing the likelihood of an insider threat being realized requires a detailed knowledge of internal processes and controls. In many cases, the lack of controls in place to monitor or enforce behaviour places an organization at risk. If an organization spends the time to identify where they are at risk from insider threats, appropriate controls can be put into place to: restrict access to sensitive information, enforce the "separation of duties" required for financial transactions, and create a "two man" rule for major research projects.

a- How this problem could be minimized in your estimation?

Here are some suggestions that hopefully illustrate my point:

- Limit access to sensitive files to only those employees with a business need to know, and ensure adequate automated logging/monitoring mechanisms are in place to audit access to information (what was seen, what was done, who did it, etc.).
- Ensure employees are restricted to what they can do in financial systems. You may even want to physically separate the Accounts Payable from the Accounts Receivable teams, to reduce the likelihood of collusion.
- Create a "two man" rule for major research projects or product launches. Don't simply rely on just one individual – ensure there are others involved in key projects, particularly sensitive projects with a direct impact to the organizations' well-being (i.e. new product launch).
- Layer auditing and control mechanisms into every automated system (i.e. file sharing systems, financial applications). If auditing and logging capabilities are present, enable them and regularly review them for suspicious behaviour.
- Inform your staff that monitoring and compliance programs are in place. In many cases, simply educating your staff that controls are in place, and consequences exist, will deter some of the more "opportunistic" behaviour.

9- From your experience, do you think "insufficient security policy" increases the insider threat behaviour?

a- If yes Why, if no Why not?

Absolutely! This has been one of the most telling indicators of potential insider threat – the lack of policy, training etc. and the lack of formal support from senior

management. The most effective ways to avoid leakages are sufficient policies and security procedures. These are pillars to avoid insider threats. Without them, no measures could be practical & effective.

b- What are your thoughts to minimize this problem?

There's really only one way to address this – ensure the senior management team endorses the requirement for policy, compliance and enforcement. Without senior management consent, any security program will be meaningless.

One suggestion that has worked for me in the past is to regularly engage senior management not only on the need for such a program, but the benefits to the organization if a program/policy/process/enforcement mechanism are in place. Employees that know what is expected of them, and understand there is a consequence for their actions, typically perform better than those who do not have a clear understanding of their role regarding security, etc.

- Development of efficient and sufficient policies & procedures
- Concentration of propriety information on the upper nodes of organization staff (as described in the previous question).
- Periodic management audit of procedures and policies for effectiveness and practice.
- Update of policies after regular intervals. Many things happen in passing years.
- Do you have any suggestion strategies to address this issue?
- Policy & Procedure development by people very much experienced in this area (technical and human sciences)
- Management buy-in for the ownership of policies.

10- Out of your knowledge, do you think that "social isolated workers" can increase the risk of insider threat behaviour?

a- If yes Why, if no Why not?

Yes. Socially isolated workers are greater threats. The reason behind in my view is the personal factors which is the major cause of leakages. Breathing in a friendly & social environment (psychologically) adds lots to get people stay human & ethical. This applies equally to night shift workers and other people who have to work in isolated work areas (like Finance, Programming or monitoring service departments).

b- Can you please give any example?

One of my client companies in my old organization was a top-notch Technology Retailer focusing on the big-shots. An employee there was working as the database administrator & programmer and was working in a somehow socially isolated environment (language and culture barriers). Someone noticed that at some point of time later, he was found offering elite class SMS advertising service to people (he offered on a social network). What he did in fact was to steal mobile numbers from the customers list in his company database and then use them as target audiences for his advertising. Based on my assessment, the factors to make him so were majorly social.

c- *What are your ideas to minimize this problem? And do you have any suggestion strategies to address this issue?*

- Weekly social gathering (e.g. breakfast) to add some social spice to the team.
- Engaging the workforce on multiple levels is one method of reducing the potential for this type of threat to be realized. Not every employee will engage in every activity, but if employees are valued and they perceive their value to the organization, the risk of an insider threat being realized will diminish.
- Improve Managers: Train managers (bi-yearly for example) for Team-building, Socialism & Leadership skills (Leading is the best way to Manage).

11- ***"Liberal access for the employees"***

a- From your experience, can you please define liberal access?

Unnecessary open-minded access to facilities allowed to employees. Sometimes given for convenience, and sometimes just for nothing.

b- How liberal access can influence the insider to behave wrongly?

With pure information security point of view, liberal access is sometimes simply wrong and sometimes it's very wrong. But the most immediate disadvantage of stopping it is killing the convenience. So we must control it, not stop it in full. For example I'm checking my mail 24/7 on my iPhone. If they stop my access, I'll have to stay in my office to check my mail. This is impractical for people like me who have to play versatile roles in my company.

Liberal Access for insiders in nothing more than a convenience to cheat. They can show their mails, other confidential info to anyone they like. Liberal access to systems will allow them program or tame policies applied on systems as they like.

Liberal Access poses external threats too. For example, what if an authorized smartphone is stolen. Or what if an employee with liberal access corrupts the IPS and IDS (Intrusion detection & prevention systems). Many external sources will be able to break into and steal whatever they like.

c- *What are your thoughts to minimize this problem? And do you have any suggestion strategies to address this issue?*

There are a number of controls an organization can put into place to minimize this type of risk. A solid control framework, focused on the "least access" privilege principle, is an excellent first step to securing access to resources. These resources may be your people, property or information.

User education and training is another key component for reducing the potential for employees to unintentionally misuse their level of access. Employees should be aware of their roles in keeping information secure, and know how to report potentially suspicious activity like someone gaining inappropriate access to resources.

Selecting the "right" employee during the hiring process is also a part of the overall control framework. If an organization can take the right steps to hire the "right" employee (i.e. using reference checks, financial/criminal checks, background investigation and behavior interviews/tests), the organization can minimize the risk of hiring the "wrong" person for the "right" position.

Separation of duties and responsibilities must also be in place to reduce this type of risk. Accurately defining a job role and responsibility and then ensuring any corresponding positions have different access will immediately reduce this level of risk.

12- "Loyalty of workers"

a- How loyalty may affect the insider threat behaviour?

Hugely! much more than any other factors. I know there are studies that have assessed employee loyalty, and tried to gauge their response to scenarios. I can't remember which study I read, but if an employee does feel some fealty to the organization, they are less likely to do something inappropriate. There must be a level of trust, reward and reciprocation between the employee and the organization beyond the simple employment contract.

b- From your experience, how this problem can be minimized? And do you have any suggestion strategies to address this issue?

Loyalty is not something we can impose onto someone. It has to come from inside the personality of the recruited and appointed person. And then it must be respected in three ways.

- Encourage motives to ascertain loyalty (bonuses, appreciations, social ingredients, job satisfaction with other colleagues)
- Discourage motives to disloyal anyone (injustice, ignorance, doubting someone in the wrong way)
- Prevention of external factors like distributed loyalty (working at 2 different but similar places simultaneously)

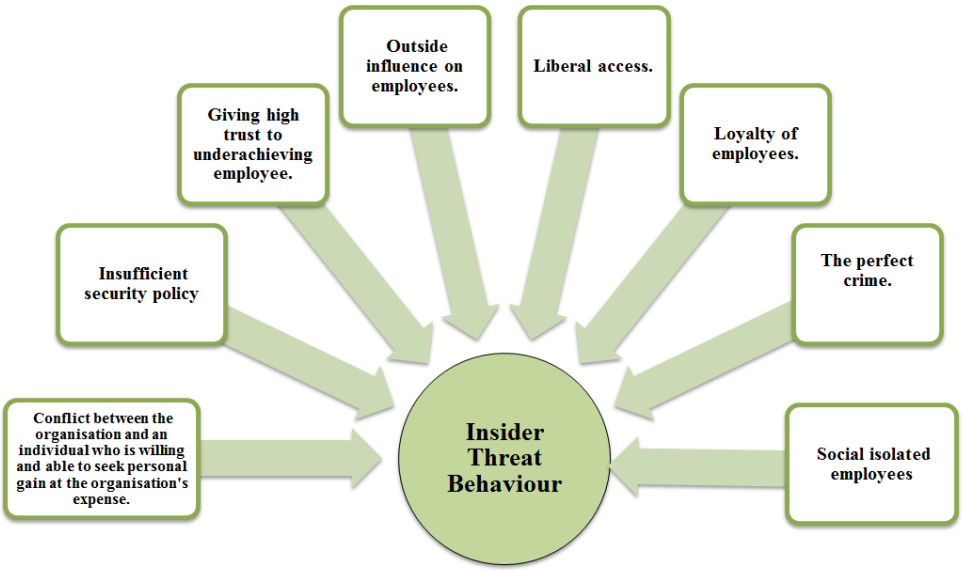
13- Do you have any documentation or guideline in your organisation about risk factors?

a- If yes, does it include some of the factors that we have discussed in this interview?

We do try to assess the risks to our organization from insiders, and have deployed most if not all of the controls I've talked about over these past few questions. In general, we have discussed almost everything (if not everything) in this interview. In previous organizations, I was successful in deploying all of these controls and a few more, to reduce the risks we were facing from individuals trying to leverage their access to resources for personal gain.

Unfortunately, it sometimes takes being victimized by insider threats to make these changes occur. Earlier in my career, I was with an organization that not only lost market share, but proprietary information to a competitor. It turned out an employee, with unrestricted access, was able to download and sell information on sales plans, etc. That was really an eye opener for me - and made me much more aware of what someone with unlimited access to a company's resources can really do if properly motivated.

INSIDER THREAT BEHAVIOURAL MODEL



Factors Contributing to Insider Threat Behaviour

14- If you could add any factors to the model or delete any factors from the model, what would it be? Why these specific factors are essential?

As for your model - I really like it. I don't think I'd add or subtract from the model or its definitions. I think it encompasses the components of insider threats, and identifies the most common aspects of how an organization is impacted by the insider.

15- Based on your experience, what are the factors you consider more common than others? Why these specific factors?

In the order of occurrence I noticed:

- Conflict between the organization and an individual who is willing and able to seek personal gain at the organisation's expense.
- Outside influence on workers.
- To support a cause
- Loyalty of workers.
- Personality Issues
- The perfect crime.
- Social isolated workers.

Appendix 8: Copyright Permission

Title:	Insider Threat Behavior Factors: A Comparison of Theory with Reported Incidents
Conference Proceedings:	System Science (HICSS), 2012 45th Hawaii International Conference on
Author:	Munshi, A.; Dell, P.; Armstrong, H.
Publisher:	IEEE
Date:	4-7 Jan. 2012

Logged in as:
Asmaa Munshi
LOGOUT

Thesis / Dissertation Reuse

The IEEE does not require individuals working on a thesis to obtain a formal reuse license, however, you may print out this statement to be used as a permission grant:

Requirements to be followed when using any portion (e.g., figure, graph, table, or textual material) of an IEEE copyrighted paper in a thesis:

1) In the case of textual material (e.g., using short quotes or referring to the work within these papers) users must give full credit to the original source (author, paper, publication) followed by the IEEE copyright line © 2011 IEEE.
2) In the case of illustrations or tabular material, we require that the copyright line © [Year of original publication] IEEE appear prominently with each reprinted figure and/or table.
3) If a substantial portion of the original paper is to be used, and if you are not the senior author, also obtain the senior author's approval.

Requirements to be followed when using an entire IEEE copyrighted paper in a thesis:

1) The following IEEE copyright/ credit notice should be placed prominently in the references: © [year of original publication] IEEE. Reprinted, with permission, from [author names, paper title, IEEE publication title, and month/year of publication]
2) Only the accepted version of an IEEE copyrighted paper can be used when posting the paper or your thesis on-line.
3) In placing the thesis on the author's university website, please display the following message in a prominent place on the website: In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of [university/educational entity's name goes here]'s products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink.

PERMISSION TO USE COPYRIGHT MATERIAL AS SPECIFIED BELOW:

Insider Threat Behavior Factors: A Comparison of Theory with Reported Incidents. In 45th Hawaii International Conference on System Science 2012 (HICSS), Maui, 2402-2411. IEEE.

I hereby give permission for Asmaa Munshi to include the abovementioned materials in her higher degree thesis for the Curtin University, and to communicate this material via the Australasian Digital Thesis Program. This permission is granted on a non-exclusive basis and for an indefinite period.

I confirm that I am the co-author of the specified material.

Signed:
Name: Peter Dell
Position: Head of School, School of Information Systems, Curtin University.
Date: 4/12/13.

PERMISSION TO USE COPYRIGHT MATERIAL AS SPECIFIED BELOW:

Insider Threat Behavior Factors: A Comparison of Theory with Reported Incidents. In 45th Hawaii International Conference on System Science 2012 (HICSS), Maui, 2402-2411. IEEE.

I hereby give permission for Asmaa Munshi to include the abovementioned materials in her higher degree thesis for the Curtin University, and to communicate this material via the Australasian Digital Thesis Program. This permission is granted on a non-exclusive basis and for an indefinite period.

I confirm that I am the co-author of the specified material.

Signed:
Name: HELEN ARMSTRONG
Position: COAUTHOR
Date: 4/12/2013

PERMISSION TO USE COPYRIGHT MATERIAL AS SPECIFIED BELOW:

1- Insider Threat: A Critical Review of the Literature. In *IADIS Internationa Conference - Internet Technologies and Society 2012, Perth, WA*: IADIS press.

2- A Study of Insider Threat Behaviour: Developing a Holistic Framework. In *IADI International Conference - Internet Technologies and Society 2010, Perth, WA* IADIS press.

I hereby give permission for Asmaa Munshi to include the abovementionec materials in his higher degree thesis for the Curtin University, and tc communicate this material via the Australasian Digital Thesis Program. Thi: permission is granted on a non-exclusive basis and for an indefinite period.

I confirm that I am the copyright owner of the specified material.

Signed: Ana Rodrigues
Name: Ana Rodrigues
Position: Conference Director
Date: 4th December 2013

PERMISSION TO USE COPYRIGHT MATERIAL AS SPECIFIED BELOW:

Insider Threat: A Critical Review of the Literature. In IADIS International Conference - Internet Technologies and Society 2012, Perth, WA: IADIS press.

I hereby give permission for Asmaa Munshi to include the abovementioned materials in her higher degree thesis for the Curtin University, and to communicate this material via the Australasian Digital Thesis Program. This permission is granted on a non-exclusive basis and for an indefinite period.

I confirm that I am the co-author of the specified material.

Signed: Tomayess Issa.
Name: Dr. Tomayess Issa.
Position: Senior Lecturer
Date: 5 Dec. 2013