ORGANISATIONAL VULNERABILITY TO INTENTIONAL INSIDER THREAT

A Thesis submitted by

Justine Bedford, MAppPsych

For the award of

Doctor of Professional Studies

2018

For Lorraine and Lisa.

ABSTRACT

In recent times there has been a spate of reporting on the counterproductive behaviour of individuals in both private and public organisations. As such, research into insider threat as a form of such behaviour is considered a timely contribution. The Australian Government now mandates that public sector organisations protect against insider threat through best practice recommendations and adopting a risk management approach. Whilst non-government organisations and private businesses are less accountable, these organisations can also benefit from the efficiencies, performance, resilience, and corporate value associated with an insider threat risk management approach.

Mitigating against Intentional Insider Threat (IIT) is an organisational priority which requires new ways of thinking about the problem, especially in terms of a multidisciplinary approach that holistically addresses the technical, individual, and organisational aspects of the problem. To date, there has been limited academic and practical contribution and a dearth of literature providing recommendations or practical tools as a means to mitigate IIT.

The purpose of this study is to develop a set of diagnostic inventories to assess for Organisational Vulnerability to Intentional Insider Threat (the OVIT). In order to achieve this overall purpose, the study sought to answer three research questions:

Research Question 1: *What are the main organisational influences on Intentional Insider Threat (IIT) based on available literature?*
Research Question 2: *What are the main organisational influences on IIT based on expert opinion?*
Research Question 3: *How is organisational vulnerability to IIT operationalised by the study?*

The methodology adopted by the study assumes a pragmatist paradigm and mixed methods design. There were three phases to this research:

- Phase One - a thorough review of the extant literature to determine the status of research and applied knowledge and identify factors and variables of IIT.

- Phase Two - conduct of a Delphi study to gather expert opinion on IIT and combine this professional knowledge with the literature review outcomes to enhance the factors and variables associated with IIT.
- Phase Three - operationalise IIT diagnostic instruments utilising multivariate statistical techniques to determine the validity of the inventories and develop a framework of organisational vulnerability to IIT.

Qualitative and quantitative analysis procedures were used throughout the research. The final survey data of phase three was analysed using multivariate statistics. The results from Exploratory Factor Analysis (EFA) demonstrate the underlying factors of each of the three dimensions (individual, technical, and organisational) which operationalise the construct of organisational vulnerability to IIT. The exploratory results indicate that diagnostic inventories of organisational vulnerability to IIT can validly and reliably measure each of the three dimensions. These were triangulated with the Delphi panel results and indicated alignment while further developing the IIT construct.

A reflection on additional contributions is an important aspect of pragmatic research. The literature available on insider threat highlights the emerging focus on the topic. Gaps in the literature indicate a number of limitations which were addressed in the current research beginning with the development of a conceptual framework illustrating the relationships of the construct, dimensions, and factors of organisational vulnerability to IIT. Whilst this work-based study had three very specific research questions to operationalise IIT, additional contributions from the research emerged as follows:

The research enhanced knowledge through: (1) study of IIT from an Australian perspective, utilising Australian expert opinion and Australian samples; (2) demonstration of the utility of the Delphi method in the study and further development of the insider threat construct; (3) an Australian definition of IIT; (4) integration of risk management standards with the available literature on insider threat; and, (5) contribution to the foresight and futures study of IIT.

While this research study has proved beneficial in addressing gaps in current literature, it is not without limitations. The generalisability of findings is hampered by the size and nature of an Australian sample and the study's exploratory approach. The ability to generalise findings and assert causality is restricted in this research, and this can be overcome by undertaking future longitudinal research or other future studies based on the findings of this study.

CERTIFICATION OF THESIS

This Thesis is entirely the work of Justine Bedford except where otherwise acknowledged. The work is original and has not previously been submitted for any other award, except where acknowledged.

Principal Supervisor: Luke van der Laan

Associate Supervisor: Janson Yap

Student and supervisors signatures of endorsement are held at the University.

Acknowledgements

I would firstly like to thank my Principal Supervisor, Dr. Luke van der Laan, for his unwavering support, guidance, and patience over the past four years. Through his mentoring and supervision, step by step, this final product was possible.

Dr. Janson Yap, my Associate Supervisor, for his valuable contributions and guidance, especially from the viewpoint of a practitioner.

My friend and supporter, Scott Ceely, who encouraged me initially to pursue this research topic and continued to motivate me to finish.

To my family and friends who supported me on this journey from beginning to end. Without your practical, emotional, and general support, this would not have been possible. I love you all dearly.

And:

The Delphi expert panel members, who provided valuable professional knowledge and insight, without which the final product would not be as comprehensive.

All those people who were able to participate in the survey and make this work-based research possible.

Also acknowledging:

Libby Black for her editing and proofreading skills.

The Australian Commonwealth Government contribution through the Research Training Scheme (RTS)/Research Training Program (RTP).

Publications arising from this Thesis

- Bedford, J & Van Der Laan, L 2016, 'Organizational Vulnerability to Insider Threat', *HCI International 2016*, 18th International Conference, July 17-22, 2016, Toronto, Canada, Proceedings Part I, Springer International Publishing, pp. 465-70.

Table of Contents

List of Figures

List of Tables

1 Introduction and Overview

1.1 Introduction

As an Organisational Psychologist, the study of insider threat has been of long-term interest to the researcher. An attraction to this field led the researcher to seek out a postgraduate program to further education and research on Intentional Insider Threat (IIT). The current thesis is the result of work based research undertaken as a practitioner researcher in the Doctor of Professional Studies (DPRS) program at the University of Southern Queensland (USQ).

In the researcher's professional practice, the scientist-practitioner model has been a strong influence through training and application. The ideology behind this research undertaking is that psychologists and their professional practice should be grounded in both research and scientific practice. The integration of research and practice is an important component allowing psychologists to gain knowledge and skills that facilitate effective psychological services and, in turn, develops a greater body of research literature that is relevant in the real world (Jones & Mehr 2007).

Being able to reduce organisational vulnerability to IIT is an important academic and applied contribution to knowledge. Research suggests that as much as 75 percent of corporate value can be tied to intangible assets (Shaw et al. 2009) including intellectual property, and so, protection of organisational assets is becoming increasingly important. IIT actions such as espionage, sabotage, theft and terrorism can cause significant damage to organisations.

The Australian Government now mandates, through its Protective Security Policy Framework (PSPF) that public sector organisations protect against insider threat by adopting a risk management approach to security management (Attorney General's Department 2016). No such mandate exists for the private sector, although a consistent approach to the management of insider threat would assist with benchmarking and developing a greater understanding of the micro (organisation

specific) and macro (the entire study of insider threat) position. Such benchmarking can demonstrate how and where organisations have reduced vulnerability to insider threat and, in a broader sense, contribute to insider threat knowledge.

There is a gap in the academic literature to aid organisations in their endeavours to protect and mitigate against IIT. In the applied sense, there is no current validated or reliable diagnostic measure to inform potential insider threat risks. As such, research is necessary to help further the field and guide practice through informed strategies and diagnostic tools that protect organisations against IIT.

1.2 Background

The study of IIT has gained increasing attention in recent years. The issue of espionage within and across Governments and private enterprises is encouraging researchers and practitioners to reassess potential insider threat detection and management. Furthermore, the significant advancements in technology are revealing new insider attack and threat vectors (for example social media, BYOD (Bring Your Own Device), Internet of Things).

Despite these advancements, our understanding of insider threat is hampered by a variety of factors: practice reveals a tendency to be reactive rather than forward thinking and protective, and understanding is hampered by organisational underreporting, ignorance, and fear. The literature available on insider threat is narrow in focus due to its complexity and difficulty to study; the predominant focus on IIT, both in practice and academic literature, is at the individual or technological (mainly ICT) level. Despite these hampering factors, a multidisciplinary approach to research and practice of IIT is increasing and showing promise. There is potential for Australian based researchers and practitioners to further contribute to the IIT narrative, which is on the rise but has, to date, been limited. There is potential to benefit from a broadening scope and inclusion of a greater focus on the organisational context and influence while further developing the field of risk management beyond its currently constrained scope related to IIT.

A work-based study which focuses on IIT is necessary due to gaps in the literature, especially around organisational factors of influence on IIT, but also to address the lack of available tools to aid practitioners in reducing organisational vulnerability to IIT. In response to the limitations in the current research and in the application of knowledge, especially in Australia, a rigorous research study can positively contribute to the field of IIT. Pursuing this work-based research through fully accredited Higher Degree Research Program provides the researcher the opportunity to engage in a well-balanced, rigorous, and methodologically sound approach to the investigation of IIT.

1.3 Work-based Research

Undertaking work-based research through the DPRS has several benefits. The more obvious academic contribution is the completion of a thesis that helps to contribute organisational knowledge and understanding of IIT. Another benefit is the advancement of professional practice through the operationalisation of IIT. Finally the work-based research encourages personal development consistent with the approach to lifelong learning and advances the scientist-practitioner model in the field of psychology.

The three phases of the research provide a consecutive and accumulative approach to the study of IIT. Phase one is a thorough review of the extant literature to determine the status of research and applied knowledge in IIT. The identification of factors and variables of IIT available in open source literature is then utilised in phase two. In the second phase a Delphi study is conducted to gather expert opinion on IIT that combines this professional knowledge with the literature review outcomes to develop an expanded diagnostic inventory. Finally, phase three operationalises the dimensions of IIT, utilising multivariate statistical techniques (exploratory factor analysis) to determine the validity of the inventory and determine a simple, yet comprehensive, working model of organisational vulnerability to IIT.

1.4 Scope

This study aims to develop a diagnostic inventory to assess for Organisational Vulnerability to Intentional Insider Threat (the OVIT). As discussed earlier there is a growing interest in the field of insider threat and an associated increase in literature on the topic. However, contemporary research is limited by a lack of Australian representation therein. There is need to broaden the scope of the research by thoroughly investigating the organisational influence of IIT in the Australian context. In order to reduce the scope of the work-based research, a number of delimitations are imposed. Limiting the current work-based research to *intentional* insider threat reduces the scope of the project by focusing on the trusted insider (a person with legitimate access to an organisations information and systems) causing damage to an organisation rather than on the broader definition of insider threat encompassing accidental and negligent behaviour or external agents gaining access and causing harm to an organisation. The researcher recognises the strong representation and influence of the United Kingdom and the United States of America in IIT research field and contributes to its scope by providing an Australian perspective.

The scope of this project includes:

- Conducting an extensive literature review to comprehensively understand the research problem and identify gaps in the available research
- Designing a sequential mixed methods research project which explores organisational vulnerability to IIT, resulting in a diagnostic inventory and conceptual model that operationalises and contextualises IIT
- Examining the operationalisation of IIT within a risk management framework (AS/NZ ISO 31000:2009)
- Analysing data from phase one and two of the study through exploratory factor analysis
- Presenting the data analysis and interpretation of results in a logical sequence
- Developing the diagnostic inventory and working model of IIT with evidence--based results obtained from all three phases of the research

- Evaluating the validity and reliability of the resulting diagnostic inventory
- Compiling and presenting the research findings.

1.5 Research Questions

There are two main aims of the current study. The first is to develop a diagnostic inventory to assess organisational vulnerability to IIT and, secondly, based on these findings of this work-based research, present a preliminary model of organisational vulnerability to IIT with both practical and academic utility.

In order to address these aims there are three research questions presented for the current research:

Research Question 1: *What are the main organisational influences on Intentional Insider Threat (IIT) based on available literature?*

Research Question 2: *What are the main organisational influences on IIT based on expert opinion?*

Research Question 3: *How is organisational vulnerability to IIT operationalised by the study?*

1.6 Methodology

In order to reach the aims of the work-based research the methodology of this project will be underpinned by a pragmatist paradigm. The pragmatic paradigm is chosen as it does not have a focus on antecedent conditions and it "is not committed to any one system of philosophy or reality" (Creswell 2009, p. 4). Instead, the pragmatic paradigm focuses on knowledge claims being a result of action orientation, and the consequences of action and change, in order to find solutions to current problems (Creswell 2009).

The pragmatic paradigm determines the *problem* as the most important factor and allows the introduction of a variety of approaches to understand the problem (or area of investigation). Given that insider threat risks are statistically rare (Shaw & Fischer 2005) quantitative methods alone are not considered sufficiently able to provide a

comprehensive picture. Therefore a mixed methods research design, consistent with the pragmatist paradigm, was employed to respond to the three research questions, thus including depth of meaning by utilising a qualitative approach.

This work-based research follows an exploratory sequential design. Phase one is a thematic analysis of the literature that is already available on insider threat and risk management (as it applies to insider threat). Phase two of the research employs the Delphi method to achieve both qualitative and quantitative outcomes. Phase three is the development and validation of a diagnostic inventory utilising multivariate statistics in order to operationalise organisational vulnerability to intentional insider threat. A full justification of the research approach and design can be found in Chapter 3.

As already explained the current research is exploratory in nature. In Phase one, a literature review was conducted to identify, organise, and distil concepts associated with intentional insider threat (Rowley & Slack 2004). The outcomes of the content analysis of the literature then formed the basis for further exploration and provides direction for the second phase of the research.

Phase two was a Delphi study, an iterative process to gather opinions from subject matter experts whilst attempting to discover new insight and gain consensus. Experts were chosen based on *a priori* criteria for inclusion. Participants were recruited through convenience sampling and snowball techniques. Predetermined questions and free-text responses allowed the panel members to provide feedback and important insights. Quantitative analysis in Phase Two used Frequencies and P-P plots to assess the responses from the Australian panel experts and to determine consensus. Classical content analysis of qualitative data was used to determine emerging themes from responses to open ended questions in all the Delphi rounds. The outcomes of the Delphi analysis, including the dimensions and variables associated with IIT, were then used to construct the items for the diagnostic inventory.

Phase Three included the development of an organisational diagnostic inventory from the information obtained during phases one and two and its statistical validation. This phase of the study employed a quantitative cross-sectional approach to the research and the use of a survey as a valid form of enquiry (Creswell 2009, 2014). Due to the nature of the construct of organisational vulnerability to intentional insider threat the inventory was constructed to examine the three dimensions (individual, organisational, and technical) as elucidated in the literature and Delphi process. A pilot study was conducted to improve the instrument and reduce the length of the inventory. Based on pilot feedback changes were made to the inventory.

Responses to the final inventory were collected online through Questionpro™. Again, the use of convenience, purposive, and snowball sampling techniques were employed. Descriptive and multivariate statistics was performed on the inventory data. Exploratory Factor Analysis (EFA) was used to aid the construction, refinement, and evaluation of the inventory (Williams et al. 2010). The multivariate analysis techniques for this research are described in greater detail in Chapter 3. Finally, this rigorous exploratory research culminated in the operationalisation of organisational vulnerability to intentional insider threat. A working model of organisational vulnerability to IIT was also presented.

1.7 Anticipated Contributions of the Study

If high-level competence is achieved by combining both research- and practice-based knowledge, then the integration can provide the most advantageous outcomes, especially in terms of adapting and forming new perspectives (Nilsen et al. 2012a). The DPRS provides the opportunity to undertake workplace research which values the broader contribution of a research study. The value in the chosen higher degree program was that it allows students the opportunity to contribute to theory, professional practice, and the self. It is anticipated that engagement in the DPRS will lead to the following academic, professional, and personal contributions.

1.7.1 Academic Contributions

- An Australian based study that expands the current knowledge base on IIT
- A thesis contributing to the academic environment
- Articles and conference presentations contributing to the growing knowledge base on IIT
- Enhanced understanding and knowledge of organisational vulnerability to intentional insider threat
- A model that operationalises organisational vulnerability to IIT

1.7.2 Professional Practice

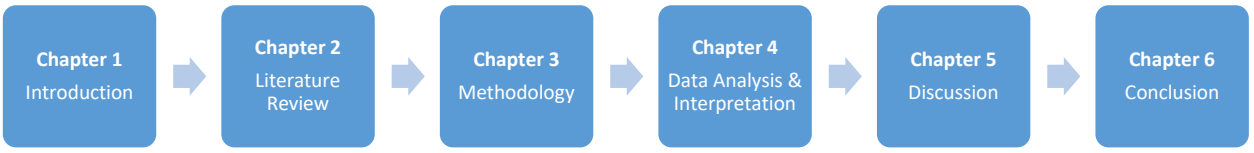
- A diagnostic inventory that provides organisations with information on their vulnerability to IIT
- Transform research outcomes into educational resources for businesses
- Through use of the diagnostic inventory provide a means of education and a way to demonstrate trends in organisations that can lead to IIT behaviour
- A simple and comprehensive model of organisational vulnerability to IIT

1.7.3 Personal Development

- Enhanced theoretical knowledge by developing greater understanding of risk management and insider threat
- Enhanced professional knowledge, tolerance for ambiguity and critical judgement by increasing understanding of insider threat through use of high level research skills
- Enhanced objective judgment, analytical skills, and research techniques, to develop and validate an inventory to help organisations assess vulnerability to IIT
- Enhanced collaboration and professional knowledge by developing greater networks in risk management and with experts in CWB/Insider threat

- Subject matter expertise through superior communication skills including in-house presentations and articles for publication
- Improved subject positioning, status and expertise in the field of insider threat.

1.8 Outline of the Research Thesis Structure



This thesis is presented with six content chapters, followed by references and appendices. Each chapter is set out according to the higher degree presentation schedule. Further, the chapters provide a brief introduction and conclusion to guide the reader. The chapters are presented in order of the work-based research process, beginning with the introduction to the research, followed by a comprehensive literature search and review, then the design of the mixed-methods study to address the aims of the research and research questions, next an examination and analysis of the data, culminating in the discussion and ending with the overall work-based research conclusion.

1.9 Summary

Chapter 1 provided an overview of the intention for study as well as an introduction to the specific topic area. Through completion of the work-based research it is intended that positive and significant contributions will be made to academia, professional practice, and the personal development of the research practitioner. The following chapter 2 provides a review of the relevant literature on insider threat and risk management, addresses limitations in the current research, and identifies gaps whereby the current work-based research can provide a valuable contribution to the existing body of knowledge.

2 Literature Review

2.1 Introduction

The previous chapter provided an introduction and overview to the thesis which included a summary of the significance of the research and the proposed original advancement to professional practice, the researcher's personal development, as well as important contribution to the organisational community of practice. The first chapter provided an overview and outline of the thesis which will now be explored in greater depth beginning with Chapter 2.

Chapter 2 is a comprehensive literature review which provides the foundational knowledge on insider threat and risk management (including security risk management) required to advance understanding of organisational vulnerability to intentional insider threat. This chapter will explore the state of knowledge, limitations to research and practice, and provide foundation for the progression of the research study.

2.2 Management and Organisational Studies

Management and organisational studies is a broad discipline which involves the "examination of how individuals construct organizational structures, processes, and practices, and how these, in turn, shape social relations and create institutions that ultimately influence people" (Clegg & Bailey 2008, p. xliii). The discipline of management and organisational studies therefore explores the challenges around employment and the workplace in a manner that addresses theory, strategy, and policy.

Mullins (2010, p. 1) expressed a "multiplicity of interrelated factors that influence the decisions and actions of people as members of a work organisation". As such, the study of management and organisations requires a multidisciplinary position and cannot be undertaken in isolation or in terms of a single discipline or approach to research (Clegg & Bailey 2008; Mullins 2010).

Insider threat fits neatly under the parent discipline of management and organisational studies. The ability to draw upon multiple related disciplines and concepts is essential in the study of this complex topic.

2.3 Insider Threat

2.3.1 Background

In 1999, a former Australian Defence Intelligence Organisation (DIO) officer, Jean-Phillipe Wispelaere, was arrested for attempting to sell highly classified material (Williams 2000). Whilst this is not the first, or only, case of espionage in Australia, it certainly highlighted that insider threat was not just something that other countries experienced. No longer could Australian Government ignore that they may be the target of internal sinister activity. A review (Blick Review) was instigated by Government, followed by an effort to try and reduce potential espionage in the future through psychological assessment, vetting of staff, improved physical and personnel security practices, and strengthened security programs (Williams 2000).

Outside of government there appears to be less emphasis on organisational protection against industrial espionage and other insider threats. Whilst organisations recognise the potential insider threat there has been more emphasis on combatting external and generally technological risks (Cyber Security Division 2009). This is a concern given the evidence for insider threat is significant and the cost of compromise is expensive (Australian Cyber Security Centre 2015). Surveys indicate that as much as 81% of fraud (Kroll 2015), 28% of electronic crime (CSO Magazine et al. 2014), and 58% of organisational security incidents (Clearswift 2013) are a result of insider actions. In an Australian survey of major Australian businesses (Cert Australia & Australian Cyber Security Centre 2015) sixty percent of respondents indicated that insiders are the most concerning cyber actors. Further, a Deloitte report (Deloitte 2015, p. 5) recognises the increasing sophistication and challenge of insider threats stating that “the combined power of an insider threat allied to organized crime is most dangerous”. Of course survey data has its limitations - including convenience sampling and lacking statistical rigour (Hunker & Probst 2011)

– and whilst it cannot be relied upon as absolute, the trends and opinions remain relevant and compelling.

Government and private sectors are all at risk (Greitzer & Hohimer 2011; Hewes 2016) and this includes Australian government, private enterprise and not-for-profit agencies. Those businesses most likely to be a target are those that control data and information that is useful to others. This may be highly classified Defence material, confidential product development details, trade secrets, or personal identity information. However, with the proliferation and growth of technology (including the Internet of things) and the growing interdependencies of businesses, even small and previously untargeted businesses are now at risk (Fenz et al. 2014).

Of concern is that our understanding of insider threat is hampered by a lack of reporting and preference for many organisations to handle insider incidents through internal mechanisms (Cyber Security Division 2009; Sarkar 2010; Shaw et al. 1998). Therefore prevalence may actually be higher and more widespread than we currently understand. Sarkar (2010) provides an overview of the reasons why insider threat information is not readily available and is even ignored. He explains that fear of negative publicity, difficulty in identifying culprits, ignorance of attacks, overlooking less damaging insider threat, and potential loss of reputation are contributing factors to a lack of reporting. Williams (2008) extends these to also include small organisations that may not have sufficient resources to investigate or monitor insider threat potential.

The reasons for participation in insider threat behaviour are vast and, because of this, the industry of corporate espionage is reportedly growing (Vashisth & Kumar 2013). The ability to gain strategic and competitive advantage is a strong corporate espionage influence (Vashisth & Kumar 2013). In some countries, for example India, research indicates the sectors most at risk include financial services, information communication and entertainment, telecommunications, real estate and industrial markets (KPMG 2012). In Australia, the ASCS threat report (2015) reveals that cyber risk incidents are reported more frequently by Energy, Banking and Financial Services,

Communications, Defence Industry, and Transport. Whilst this report is more broadly focused (i.e. not just insider threat reporting) it highlights the sectors most often the target of sinister cyber activity.

2.3.2 Definition

In order to define *insider threat* a definition of *insider* is necessary. There is debate in the literature around the definition of an *insider* with a number of definitions proffered (for a review of the definitions see Pfleeger et al. 2010). Neumann (2010) and Chinchani et al. (2005) also argue that the process of distinguishing between insiders and outsiders can be difficult given its multidimensionality. Even so, for some academics categorising insiders has been important. For example, Cole (2006) classifies insiders as either a Pure insider, an Insider associate, an Insider affiliate, or an Outside affiliate. Other definitions have been narrow in focus, for example Pfleeger et al. (2010, p. 170) defined an insider as "A person with legitimate access to an organization's computers and networks"; limiting the definition of an insider to be more technically-focused rather than more broadly relevant.

Probst et al. (2008) offer a cross-disciplinary definition that "an insider is a person that has been legitimately empowered with the right to access, represent, or decide about one or more assets of the organization's structure." Of course even the most comprehensive definition of insider threat will have its shortcomings (Crampton & Huth 2010). Additionally some researchers argue that there is no benefit in determining degrees of "insiderness" (Crampton & Huth 2010, p. 183) such as that offered by Cole (2006). Given it is generic and cross-disciplinary, the definition by Probst et al. (2008) underpins this study.

Armed with a common, albeit imperfect, understanding of the definition of an insider, the next stage is to define *insider threat*. Costa et al. (2014) suggest that defining insider threat is difficult due to variations in interpretation and scope. Whilst there are many definitions Hunker and Probst (2011, p. 4) express there to be "no uniform or widely accepted definition".

Insider threat is defined by Shaw et al. (2009, p. 1) as "…any activity by military, government, or industry employees whose actions or inactions, by intent or negligence, result (or could result) in the loss of critical information or valued assets". However, this definition is limited to persons considered *employees*. Catrantzos (2012, p. 4) defined insider threat "[as] an individual and, more broadly, the danger posed by an individual who possesses legitimate access and occupies a position of trust in or with the infrastructure or institution being targeted". The limitation of this definition is that it does not extrapolate on the types of danger or risks and how these might present.

Another commonly referenced definition is presented by the CERT program at Carnegie Mellon University (CMU). They define insider threat as a "current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organisation's information or information systems" (Cappelli et al. 2012, p. xx). This is a more complex and lengthy definition but it does extend beyond a single focus on employees and clearly articulates where the vulnerability exists and how the organisation may be negatively affected. As far as the researcher can ascertain, there exists no Australian based definition on insider threat. Whilst a specific definition for the Australian context may not be a necessity, a more precise definition for Australia may provide assistance to alleviate the fragmented conceptions which exist. Further, an Australian based definition can assist in operationalising insider threat in the Australian context. The current research will aim to determine a relevant and comprehensive definition of insider threat from Australian experts. However, in the absence of such, the definition proposed by Cappelli et al. (2012), for its comprehensive, and direct focus on intent, underpins this study.

2.3.3 Intentional versus unintentional insider threat

As indicated above there is a distinction in the literature, including definitions, between those who maliciously and intentionally cause harm to an organisation and

those who accidentally or inadvertently cause harm, perhaps due to naïvety, ignorance, or accidents (Sarkar 2010). The current thesis focuses on *intentional* insider threat, where a person is motivated and acts to deliberately cause harm to an organisation. Those insiders who represent an intentional insider threat have also been described in the literature as hostile insiders, malicious insiders or trust betrayers (Catrantzos 2012).

In some ways the distinction is arbitrary, as organisational protective measures and mitigation strategies are likely to be of benefit regardless of the insider's intent (Cappelli et al. 2012). As Pfleeger et al. (2010, p. 175) write "the set of preventative responses is likely to be the same whether or not intention is malicious". Still, the distinction helps to delimit the research and provide an operationalised focus. The attention on intentional insider threat remains important especially given reporting indicates that as much as 90% of breaches by insiders are the result of intentional actions and behaviour (Verizon and U.S. Secret Service 2010).

2.3.4 Past research

An exhaustive review of the published works available on insider threat, presented in this thesis with selective citation (Cooper 1988), reveal a growing body of literature on the topic, especially since 2000. According to Google Ngrams the term 'insider threat' has been gaining in popularity since the 1990s with a significant increase from 2000 to the present time. The discourse on insider threat has been promulgated in many ways. Whilst a thorough review of all publications has been pursued, the main focus of this thesis has been on publications that extend beyond a general commentary. Only those that have extended our knowledge of insider threat in some way - empirically, practically or theoretically - are presented in this thesis.

The Defense Personnel and Security Research Center (PERSEREC) has focused on the study of insider threat since its establishment in 1986 (Band et al. 2006). It was in 1999 that RAND conducted workshops to better understand the research required to address the insider threat problem (Brackney & Anderson 2004; Hunker & Probst 2011; Pfleeger et al. 2010). The U.S Department of Defense embarked on its own

search for policy and research to reduce the insider threat (Hunker & Probst 2011; Pfleeger et al. 2010). Since then large and long term projects on insider threat have been pursued (predominantly in the United States and the United Kingdom) by the Software Engineering Institute's Computer Emergency Response Team (CERT) and U.S. Secret Service and Centre for Protection of National Infrastructure (CPNI 2013). In addition, smaller academic research studies have emerged. The result is that there is a rich and diverse literature on insider threat, albeit lacking in full comprehensiveness and coverage including a limited contribution from Australia.

Reporting on insider threat covers theoretical understanding, practice, and application in the field. Consistent with previous reviews of the literature (for example, Festa (2012a) and Catrantzos (2012)), the current literature review has also determined that the focus of research has predominantly been on the individual (personality, characteristics, motivations), societal and environmental influences, and cyber security. There has been less emphasis on specific organisational factors associated with insider threat although there is a growing interest in perspectives including personality characteristics, organisational environments and the interaction between these (Kraemer et al. 2009; Vashisth & Kumar 2013).

Much of the reporting on insider threat agrees that the focus of historical research is narrow in perspective. There is a strong concentration on computer hackers, disgruntled employees, ex-employees and consultants (Brackney & Anderson 2004). Whilst it is acknowledged that the study of insider threat is complex (Sarkar 2010; Williams 2008), it has failed to provide significant recommendations or practical tools as a means of countermeasure (Catrantzos 2012). Furthermore, psychological approaches to the insider research have been embedded in personality and motivational theories (Catrantzos 2012). Whilst the focus of the growing body of literature and research on individualistic aspects of insider threat is useful, it has to a large extent ignored or undervalued broader organisational influences.

Given this gap in research on insider threat there is potential to expand our understanding of the insider threat phenomenon. It requires a more rigorous focus

on organisational predispositions and vulnerabilities (Band et al. 2006). In response to this gap in the current literature, the present study aims to distil organisational vulnerabilities and strengths and develop an inventory to assess the potential for intentional insider threat from a broader organisational perspective.

A brief overview of the main areas of insider threat research, including the individual, technical and organisational foci, is provided below. These approaches to the study of insider threat demonstrate potential biases in research and application. Whilst the study of insider threat is still in the formative stages, addressing potential bias and specificity in the research is important for increasing our understanding of intentional insider threat. It also helps to guide further research in a more balanced and considered way.

2.3.5 Individual Focus

2.3.5.1 Demographical

Demographic approaches to the study of insider threat look at historical cases in order to identify common characteristics or traits of the perpetrator (Festa 2012a). Earlier research into insider threat, mainly based in the United States of America, used this approach to draw statistical conclusions about the common demographical characteristics across espionage cases (one type of insider threat).

In the USA, the Defense Personnel and Security Research Center (PERSEREC) undertakes research to improve personnel suitability, security, and policy and practice (PERSEREC 2016). Based on statistical interrogation of the PERSEREC database information, researchers established that those who have committed espionage in America, since the Cold War, are more likely to be well-educated heterosexual males, who hold security clearances and are over the age of 30 years (Herbig 2008). These findings are consistent with outcomes of other studies on intellectual property theft. Research in this area indicates the majority of intellectual property theft in the USA is committed by males at approximately 37 years of age holding engineering, science, management, sales and programming positions (Shaw & Stock 2011).

Whilst a useful approach to develop greater understanding of the demographical influence on insider threat, there are limitations to this approach. The main drawback is a lack of predictive ability evidenced by the large number of people who are represented by the same demographical profile (e.g. educated males over 30 years of age) who have not participated in insider threat behaviour (Festa 2012a). So, whilst the above findings show some similarities in offender demographical information, other studies have found insiders to be demographically diverse (Keeney et al. 2005; Kowalski et al. 2008). Even those that have determined demographic characteristics to be significant have cautioned against focusing on demographics alone. For example, Cappelli et al. (2012) in discussing IT sabotage suggest that it is more important to attend to developing understanding of positions at risk for the crime, influential behavioural and organisational factors, as well as implementation of mitigation strategies.

2.3.5.2 Motivational

Motivation is defined in the online Oxford Dictionary (Oxford Unviersity Press 2016b) as 'a reason or reasons for acting or behaving in a particular way'. Shaw et al. (2009, p. 1) note that individuals participating in negative insider behaviours are 'frequently driven by the same motivations – greed, disgruntlement, conflicting loyalties, [and] ego-satisfaction'. Such motivations are consistently reported in other writings as well (Civiello 1999; Fischer 2000; Vashisth & Kumar 2013).

However, research elaborates that motivation differs based on the type of insider crime. For example, Cappelli et al. (2012) report, based on large scale research, that IT sabotage is usually motivated by revenge whilst insider fraud is motivated by financial need or greed. Further, Fischer (2000) demonstrates that money is a larger motivation in volunteer spies and those recruited by foreign intelligence, but ingratiation is more evident in those recruited by family or friends.

Interestingly data from PERSEREC shows a shift in individual motivations over time and that a number of spies have mixed motives for engagement (Fischer 2000); A finding that Randazzo et al. (2005) also report in their research in the finance sector.

Sokolowski et al. (2016), suggest that as a generalisation, motive is associated with some type of "*gain*"; financial gain, competitive advantage, and/or retaliation.
Research on insider threat focusing on individual motivations has included loyalty and allegiance (Herbig 2008; Shaw et al. 2009), response to boredom (Civiello 1999), professional setbacks or unmet expectations (Shaw & Stock 2011), as well as an interest in hacking (Civiello 1999). Research has indicated that individuals may not be motivated by their work environment or by the purpose of the organisations in which they work. Additionally, professional setbacks or unmet expectations are highlighted as having the potential to accelerate an individual from intent to action (Shaw & Stock 2011).

Even where employees are aligned with the values of their organisation, this may not supersede personal drivers and values. Certainly in research that focuses on loyalty it is cautioned that an employer may not be at the top of the loyalty chain; falling behind that of family, religion, and faith (Shaw et al. 2009). Reduced loyalty in the IT profession has also been challenged by the high demand for IT services and high rates of turnover in IT roles (Shaw et al. 1998). Loyalty and allegiance may also be affected by globalisation (Herbig 2008). Cappelli et al. (2012) caution that foreign allegiance is a necessary consideration where organisations are expanding outside their own country. Organisational commitment is not guaranteed and the research elucidates that there are many factors (including globalisation, mismatched values) which have an influential role (Safa et al. 2018).

As with the demographic approach there are limitations in the study of motivation and insider threat. Whilst motivation has been found to be a significant factor in insider threat based on case studies (Munshi et al. 2012) there is a challenge in robustly determining insider motivation (Pfleeger et al. 2010). This is especially relevant given it is difficult to verify self-reported motivation and historical data is from offenders whose reasons for providing motivational information may be questioned (Sokolowski et al. 2016). Further motivation is not static and can change over time (Sokolowski & Banks 2015).

Additionally, there is also no controlled research to understand why people with the same drivers respond differently with respect to action (Shaw & Stock 2011). For example, it is recognised that whilst many insiders may be predisposed to disgruntlement most do not participate in negative insider activity. The act requires that the insider moves beyond having intention (Shaw & Stock 2011) to acting or behaving on the intent. Hence, targeting motivation as a primary source of data to assess potential for insider threat may lead to false positive errors. In criminology the theory of planned behaviour suggests that both motive and opportunity must be present for a crime to be committed (Hunker & Probst 2011). Therefore, at least with respect to this theory, opportunity must also be included in data sources.

2.3.5.3 Psychological

A review of the published literature on insider threat shows that a large portion of research focuses on individual characteristics that may lead to insider threat behaviour. For some researchers the main aim is to identify psychological predispositions which can indicate higher potential to participate in insider threat activity. One of the earliest research projects on espionage, a form of insider threat, was an Intelligence Community sponsored project conducted in the United States of America. Known as Project Slammer (Director of Central Intelligence 1990), this research examined espionage through interviews and psychological assessment of convicted espionage subjects. Interviews of known associates (co-workers, supervisors and family members) were also undertaken to identify personal characteristics along with events that led to their actions (Shaw et al. 1998). Among other findings, outcomes suggest that those involved in espionage considered themselves as special and deserving and that security procedures did not apply to them.

Ongoing research continues to demonstrate similar findings and expands our understanding of psychological predispositions that are linked to insider threat. Personality vulnerabilities identified in the research includes psychopathy, malignant narcissism, and borderline personality organisation (Liang & Biros 2016; Shechter & Lang 2011), as well as personal predispositions such as medical or psychiatric

disorders that affect judgment and social skill problems (Shaw et al. 1998; Shaw & Sellers 2015). Greitzer and Hohimer (2011) identify that disgruntlement, anger management, disengagement and disregard for authority as important tendencies toward insider threat.

Further ethical flexibility, entitlement, and lack of empathy are also identified as personal predispositions that can trigger insider threat (Shaw et al. 1998). More recently in a proof of concept study, Liang and Biros (2016) presented more positive individual characteristics associated with insider threat. Acknowledging the limitations of a pilot study (including a small test set of cases and related low power) Liang and Biros (2016) discovered that cognitive ability, dedication, and being well-educated, were characteristics of their group of cases.

When it comes to insider threat, much of the research notes that psychological and personality predispositions are not enough on their own. It is the interaction of the vulnerability, with a current stressor, which can lead to poor judgment, especially where no social support is available for effective intervention. This is an important consideration given the prevalence of exposure to psychosocial risks by the workforce. Surveys and research indicate that as much as one third of the workforce is exposed to psychosocial risks and therefore "could conceivably pose a significant threat to the enterprise's prosperity" (Frangopoulos et al. 2013, p. 55).

As with the demographic and motivational approaches to the study of insider threat, the predictive potential of psychological characteristics is a limitation of this approach. Shaw (2006) cautions that data obtained from interviews of insiders (or their co-workers, supervisors, family) may be skewed due to bias in reporting. He further acknowledges the danger of 'false positives' in focusing on personal characteristics. Personal traits on their own are not considered predictors of insider threat (Shaw & Fischer 2005). In practice a sole focus on the individual may also be limiting and "screening for specific personal characteristics paint an imperfect picture" (Pfleeger et al. 2010, p. 174). As Catrantzos (2012) notes submitting individuals to further scrutiny may also be alienating for the average employee.

A review of practice following an espionage case in Australia recommended that greater attention and priority be given to heightening awareness of security arrangements in the public sector through a greater focus on the individual (Williams 2000). One of the main recommendations in the review was that "staff of intelligence agencies be subject to psychological testing and accept a more detailed inquiry into their personal affairs than is required for employment in other areas" (Williams 2000).

The improvement of personnel security practices as recommended was implemented but again the focus was more directed towards the individual level, rather than broader organisational level. Such an approach has received criticism due the expectation that vetting processes are able to establish an individual's character and from this make predictions of future actions (Young 2017). As Catrantzos (2012) notes focusing solely on an individual, without broader context, may be self-limiting and it is the multidisciplinary approach to research and countermeasure that is promising. Hence the importance of the current study which explores an understanding of the organisational context and influence to a greater level, extending the purview beyond the individual focus.

2.3.5.4 Organisational Focus

More recently a focus on organisational context and environmental influence has emerged within insider threat research. Whilst research on insider threat often considers the above foci (demographical, motivational, psychological), it provides guidance on how a positive and secure work environment can be achieved (Festa 2012a). The Organisation is important as Pfleeger et al. (2010, p. 173) report "[t]he organization plays several roles in enabling an inappropriate insider action". The organisation does this by deciding who can have legitimate access, determining organisational boundaries, setting security policy, and determining central goals and strategies.

Consistent with this, Theoharidou et al. (2005) determines that a sole focus on the individual without reference to their organisational environment is ineffective in

addressing insider threat. Shaw et al. (2009) acknowledge that organisational and situational factors can contribute to (and mitigate) insider threat. The way employers hire, train and manage staff are important considerations to overall organisational security (Shaw & Fischer 2005) especially given that effective management can reduce risk and strengthen competitive position (CPNI & PA Consulting Group 2012). Further, organisational culture (Shaw & Stock 2011; Tang et al. 2016), working conditions and pressures on organisations can also be relevant considerations when it comes to insider threat (Shaw & Stock 2011).

Research by the Centre for Protection of National Infrastructure (CPNI 2013, p. 5) in the UK note that organisational level factors are exploited in insider cases and that vulnerability to insider threat may be reduced by identifying organisational level factors and ensuring "a strong, on-going personnel security regime, establishing effective management practices and recognising that the insider threat can come from anyone with access to an organisation's assets".

Given the link between psychosocial risks and insider threat (as discussed earlier) it is important to recognise that organisations can place demands on their workers that can lead to greater stress, and therefore potentially result in negative workplace behaviour. Research in employee behaviour and occupational health has consistently shown that, among others, restructuring, temporary work conditions, job insecurity, high workloads and working hours, poor workplace relationships, poor working conditions, and lack of work-life balance can all contribute to greater stress in individuals.

Shaw et al. (2009) published an 'insider risk evaluation and audit' to help address specific vulnerabilities to insider threat. Based on previous studies of insider threat they define several areas that may mitigate (or magnify) insider threat potential. These include policies and practices, recruitment, pre-employment screening, training and education, continuing evaluation and policy implementation, and employee intervention (Shaw et al. 2009, pp. 10-1). These authors suggest that improvement to personnel security practices and effective management intervention

can help minimise damage to organisations posed by insider threat cases. Other findings indicate that insufficient and inappropriate management intervention can actually contribute to insider activity (Shaw & Sellers 2015).

It is established that organisation specific sources of risk can escalate insider threat behaviour. An organisations response to its staff may increase or decrease the likelihood of insider threat (Band et al. 2006) and make matters worse through some action or failure to act (Shaw & Stock 2011). In a 2005 review study, 92% of insider cases were found to follow employment related events such as termination, demotion, or conflict within the workplace (Keeney et al. 2005). Shaw et al. (2009, p. 9) report that the following can increase insider threat: competitive nature of the business; reputation; overseas locations; technological dependence; and difficulty monitoring employees.

Kraemer et al. (2009) discuss how a variety of studies have found that a high workload can affect security behaviour. In addition, according to Vashisth and Kumar (2013) globalisation (including inter-company collaboration) and the internet have contributed to an increase in insider threat.

Colwill (2010) suggests that outsourcing can fragment or dilute protection controls leading to an increase in third party access and privilege akin to the insider. Whilst these authors raise concern, empirical evidence does not appear to support outsourcing or the use of contractors as a significant factor in insider threat (Munshi et al. 2012).

Reports on unethical behaviour in organisations is increasing with informal norms contributing to negative employee behaviour (Vashisth & Kumar 2013). Research finds that organisational environments can influence employee expectations. For example, organisations which ignore stealing can set an expectation that this behaviour is socially acceptable (Sauser 2007). Vashisth and Kumar (2013) write in their article about the ‘Bad Barrel’ approach, which hypothesises that unethical behaviour (such as insider threat) is more a function of organisational and societal

factors. As such it is assumed organisational factors strongly influence insider threat behaviour (including leadership, policy and process and culture) and that some organisational environments will encourage insider threat activity (Vashisth & Kumar 2013). Further, the behaviour of leaders and their ability to model sound security practices may assist in developing a positive security culture (Theoharidou et al. 2005).

The employment of specific types of employees, such as hackers, may also have important implications for organisational culture (Civiello 1999). Whilst organisational factors are a strong consideration, creating opportunity, an individual's characteristics and social networks cannot be overlooked (Vashisth & Kumar 2013). Furthermore, creating a culture of ethical conduct is an important consideration for mitigation (Vashisth & Kumar 2013).

Whilst it is acknowledged that a critical pathway may exist and that personal predispositions, societal and technical factors play an important role in insider threat (Shaw & Sellers 2015), organisational factors may be easier to address with many organisations. A focus on organisation specific ad targeted solutions provides a rudimentary and initial engagement in addressing insider threat problems, especially for those that have been afraid, ignorant, or looking for cost-effective solutions.

2.3.5.5 Technical Focus

As previously discussed, the most significant amount of research available on insider threat is in the information technology and cyber fields. For example, it has previously been mentioned that cyber security research has dominated over other forms of insider threat research (Catrantzos 2012) despite being a technically hard problem (Cyber Security Division 2009). A library search on insider threat, using the University of Southern Queensland database, demonstrates a strong representation of journals focused on technology and computers. Whilst not a comprehensive list these publications include (in order of appearance), IET Information Security, International Journal of Computer Applications, Computational and Mathematical Organization Theory, IEEE Security & Privacy Magazine, International Journal on Artificial

Intelligence Tools, International Journal of Information Security, Network Security, European Journal of Information Systems, ACM Transactions on Internet Technology, Advanced Computing : an International Journal, and International Journal of Network Security & Its Applications.

Research focuses on how the insider threat problem can be addressed by implementing technological solutions. As Shaw et al. (1998, p. 1) explain “it is not surprising that overwhelming attention has been devoted by computer security experts to technological vulnerabilities and solutions”. Especially since these solutions are often preferred by business, emphasised by organisational uptake and acceptance (Kraemer et al. 2009).

Whilst preventing insider threat is the ultimate aim; detection, analysis, and identification of misuse has dominated the research (Neumann 2010). The study of insider threat from a technical perspective can be difficult as threats span an IT system’s life cycle; through design, development, operation, and decommissioning (Cyber Security Division 2009). As examples, publications on technological solutions cover denial of access, fraud detection technology (Flegel et al. 2010), access control (Crampton & Huth 2010; Cyber Security Division 2009), decoys (Bowen et al. 2010), anomalous pattern detection (Gelles 2016), automated detection (Magklaras & Furnell 2010), use of big data (Festa 2012a), and data mining, profiling, monitoring and multilevel security (Cyber Security Division 2009). As well, more specific programmatic and cyber tools outside the scope (and technological sophistication) of this thesis are ongoing avenues of study.

Whilst there is a heavy emphasis on technological solutions to insider threat, a shift in focus has occurred over the past ten years. For example there has been a move to cover the importance of information security management (Coles-Kemp & Theoharidou 2010) and policy (Colwill 2010; Hunker & Probst 2011; Kraemer et al. 2009; Pfleeger et al. 2010; Probst et al. 2010b). Recently there has been a visible shift to integrate human aspects along with technological considerations.

Our understanding of insider threat, especially the multifactorial influence which includes the individual and organisation, continues to grow. Computer technology on its own is not enough to combat insider threat and high level of computer sophistication is not necessarily a risk factor (Mouton et al. 2016; Sarkar 2010). Cappelli et al. (2012) discovered through their research on insider threat that IT sabotage requires a level of technical sophistication and was often carried out by those in IT roles (e.g. system administration, database administration, programmers).

However, other insider crimes did not necessarily require high level technology skills. For insider theft of intellectual property, scientists, engineers, and sales people are amongst the highest offenders. In the case of fraud, lower-level employees in a variety of roles (and presumably with a variety of IT skill) are the biggest offenders. Randazzo et al. (2005) provide further support from their review of case examples in the financial services sector, concluding that insider threats are not technically sophisticated and often exploit business processes and policies (organisational level factors) rather than technical vulnerabilities.

Catrantzos (2012) reflects that most cyber security attacks occur after termination of employment which suggests a fundamental difference between cyber security/IT sabotage and other insider threat cases. In fact, according to the CERT Guide to Insider Threats, IT sabotage occurs following termination or during suspension from duties in the majority of cases, a finding not repeated in other insider cases (Cappelli et al. 2012).

What is consistent, however, is the growing acknowledgement in cyber security research that personal predispositions contribute to an increase in risk and observable behaviours in the workplace can represent concern (Band et al. 2006).
Cappelli et al. (2012) identify in their research personal predispositions as: conflict with co-workers; bullying and intimidation; personality conflicts; unprofessional behaviour; inability to conform to rules; anger management concerns; and disgruntlement. Hence, combining psychosocial data along with the more traditional cyber security audit data may enhance the predictive capabilities of models of insider

threat (Greitzer et al. 2009). Whilst the emphasis beyond technological vulnerability and countermeasures is growing, limited research reflects a more holistic approach to insider threat with respect to psychosocial and organisational risks (Frangopoulos et al. 2013).

Colwill (2010) agrees that a focus on cyber security and information technology alone does not provide a balanced solution, overlooking important individual and organisational interventions. Whilst security can be improved by technological assistance and advancement (e.g. passwords, data analytics, and multi-factor authentication) it does not address the full spectrum of insider threat. Employers can become comfortable and perhaps overly reliant on technology, missing the opportunity to embrace other proactive forms of addressing the insider threat (e.g. security awareness programs and personality testing). This is probably why surveys across industry consistently find that insider threat programs often lack direct focus on the suspicious non-technical behaviours of insiders (Intelligence and National Security Alliance 2013).

Sarkar (2010) suggests that assessing insider threat requires a focus on technological, behavioural and organisational components. Randazzo et al. (2005) emphasise the importance of looking at the interplay between technology and overall business processes to ensure a comprehensive approach to insider threat. Gelles (2016) concurs that policy, processes, communications, and training are critically important aspects of evaluating an insider threat program. Human factors, education and awareness, and after care amongst the top priorities of consideration in the research effort (Colwill 2010). Further, Green (2014) discusses in his article that while research in insider threat has increased, it has largely ignored the existing body of literature available on workplace deviance, especially as it relates to information and communication technologies (that is, cyber deviance).

It is the combination of technical controls along with psychosocial considerations and organisational factors, that hold the most promise for understanding, detecting, and preventing insider threat (Borrett et al. 2013; Gelles & Mitchell 2015; Greitzer et al.

2009; Kraemer et al. 2009). A variety of disciplines contribute to the study of computer and information security (CIS). While individual and organisational factors have been a focus, further research is still an important consideration in extending knowledge and understanding of the interplay between individual, organisational, and information security (Safa et al. 2018). Kraemer et al. (2009) provide an overview and examination of human and organisational factors in CIS research. They conclude that streams of research have included usability and users' role, user perceptions and behaviours, organisational policies, security culture, management support, employee training and awareness. Their specific study also expands to include lack of funding, inadequate staffing, lack of CIS knowledge, and lack of CIS policies, among others, as contributing to security vulnerability, which is a precursor to insider threat.

The traditional and function based reporting of organisations creates an opportunity for insider threat and therefore, working more closely, collaboratively, and intentionally is seen as a proactive preventative measure against insider risk (Pace 2016; Safa et al. 2018). Hence, the recommendations from a number of authors, researchers, and the CERT team are that in order to detect and/or prevent insider threat a multidisciplinary effort and understanding of the psychological, organisational, and technical aspects of the problem is required (Moore et al. 2008). It is through this multidisciplinary approach that the current research progresses the narrative of insider threat. It develops an inventory that specifically addresses individual, organisational, and technical vulnerabilities, to reduce insider risks within organisations.

2.3.6 Models and Frameworks of insider threat

Schultz (2002) identifies that research into insider threat is in its infancy and, as such, the ability to detect or predict insider attacks is limited. He examines a number of insider threat models, however, these are mostly attack-focused, interested in an insider's capability, motive, and opportunity (Schultz 2002). Since then there has been a shift in focus to extend beyond the attention on individuals and an increase in the number of models and frameworks that attempt to explain insider threat with more dimensionality. Models to detect and prevent insider threat are heavily focused

on technical factors (see, Munshi et al. 2012). Importantly, there has been a shift to a broader and multidimensional focus. For example, Pfleeger et al. (2010) present a framework for insider action that describes the role of the individual, the environment, the system, and the organisation.

Legg et al. (2013) provide a summary of models and frameworks that are commonly referenced in insider threat literature. In their commentary Legg et al. (2013) acknowledge many models focusing on insider attributes and different types of insider actions. Other models focus on prediction and detection of insider threat. Additionally, many frameworks are limited as they do not focus on the complexity of interactions between individuals, behaviour, and environmental (including organisational) aspects of the problem.

More recently models have appeared in the literature that help explain how insider threat happens and what organisations can do to intervene at various risk points (Greitzer et al. 2009; Legg et al. 2013; Pfleeger et al. 2010; Sokolowski et al. 2016). One of the earliest and most published models is that of the Critical Pathway, which presents a more holistic approach to explain insider threat, (see section 4.5.1; Band et al. 2006; Cappelli & Moore 2010; Cappelli et al. 2012; Nurse et al. 2014a; Shaw & Fischer 2005).

2.3.6.1 The Critical Pathway Approach

Based on case studies, the critical pathway approach seeks to demonstrate that there are common factors, including individual and organisational behaviours, which increase the risk of counterproductive behaviours (e.g. rule violations, disgruntlement) and insider threat (Shaw & Sellers 2015). The critical pathway approach considers the complex nature of insider threat and moves away from the idea of fixed profiles of perpetrators (Shaw & Stock 2011). In the literature there are several researchers who employ the critical pathway approach to study insider threat, including sabotage, espionage, and/or theft of intellectual property (see Band et al. 2006; Cappelli & Moore 2010; Cappelli et al. 2012; Director of Central Intelligence 1990; Shaw & Fischer 2005).

The first research to discuss a critical pathway appears to be that of 'Project Slammer' which examined convicted espionage subjects (see Section 2.1.5.3) and demonstrated that insider activity results from predisposing personal traits, an acute stressor, an emotional fallout, problems with decision-making and judgement, and finally a failure of peers and supervisors to intervene effectively (Shaw et al. 1998). Band et al. (2006) demonstrate that an individual engaging in insider threat behaviour travels down a critical pathway which is influenced not only by individual factors but also the interaction with their environment. They identify six commonalities between IT sabotage and espionage cases including common individual predispositions, experience of stressful events, observable behaviours of concern, technical activity, organisations failing to detect (or just ignoring) rule violations, and lack of physical and/or electronic access controls that influence insider threat behaviour.

There are four elements of the critical pathway model (see Figure 1): (1) personal predispositions, (2) stressors, (3) concerning behaviours, and (4) organisational responses. Vulnerabilities across all of these critical points lead to an increased risk of an insider threat.

Figure 1: The progression of events along the critical pathway

Source: Shaw and Stock (2011, p. 8).

This model emphasises how personal predispositions can affect judgment and reliability, resulting in a greater propensity to travel along the critical pathway. Personal predispositions in this model include not only medical, personality, and psychiatric disorders but extend to social-skills problems, biases in interpersonal decision-making, social-network risks, a history of rule violations, and travel history as potential indicators of concern (Shaw & Sellers 2015; Shaw & Stock 2011).

Of course, these predispositions on their own are not the only factors to increase insider threat. Personal, professional and financial stressors also contribute to an individual's progression towards insider threat activity. Shaw and Stock (2011) explain personal problems to include financial problems, relationship difficulties, legal concerns, medical issues, and even relocation can create substantial stress for at-risk individuals. Further, professional stressors include conflict in the workplace, demotion, role changes due to mergers or acquisition, and disappointing performance reviews.

The model suggests that concerning behaviour follows stressful events and that these behaviours are often observed by others in the workplace or are known to other associates (Cappelli et al. 2006; Director of Central Intelligence 1990; Fischer 2000; Shaw & Sellers 2015). Such counterproductive behaviour can include, but is not limited to, professional misconduct, absenteeism, poor performance, policy violations, conflict with co-workers, and security breaches (Shaw & Stock 2011).
Finally, the last factor along the critical pathway that leads to a hostile act is the problematic organisational response. When "at-risk" insiders are exposed to problematic organisational responses such as inaction, inattention, and indifference, the likelihood of participating in a hostile act increases. Ineffective actions can also increase risk. Shaw and Sellers (2015) suggest that aggressive investigations, undertaking action without an appreciation of psychological vulnerability, and actions during termination can promote insider threat behaviour.

As can be seen by the graphic above, this model has a strong emphasis on the individual. This is consistent with the literature review presented above that suggests

a greater focus on individual factors (compared with organisational) in the insider threat domain. The critical pathway model does represent an organisational context, noting that problematic organisational responses (e.g. inattention, inadequate investigation, etc.) contribute to insider threat actions. However, the model does not extend beyond maladaptive organisational responses and therefore loses the potential for organisationally driven protective measures.

Stock (2008, cited in Shaw & Stock 2011) described an approach called the Pathological Organizational Affective Attachment (POAA), the critical pathway model. This conceptual framework suggests four variables which can influence an offender's trajectory down the critical-pathway. These include: employee/subject variables, extra-work variables, workplace variables, and target characteristics. According to Stock's framework, addressing these variables can decrease risk of insider threat action. Not all four components of the framework need to be addressed equally (Shaw & Stock 2011), however the framework is more robust than that of the critical pathway approach in acknowledging the importance of organisational factors.

An article by Shaw and Sellers (2015) suggests that the critical pathway model may be a useful empirical framework for insider threat. However, there is lack of controlled studies using the critical pathway model which is one of its limitations (Shaw & Stock 2011). Correspondingly, there is a lack of understanding on how mitigating factors may reduce or even prevent trajectory along the critical pathway. Finally, a lack of controlled research reveals the gap that exists in our understanding of persons who commit insider attacks and do not demonstrate the characteristics of the critical pathway (Shaw & Stock 2011).

2.3.6.2 CERT's MERIT Models of Insider Threats

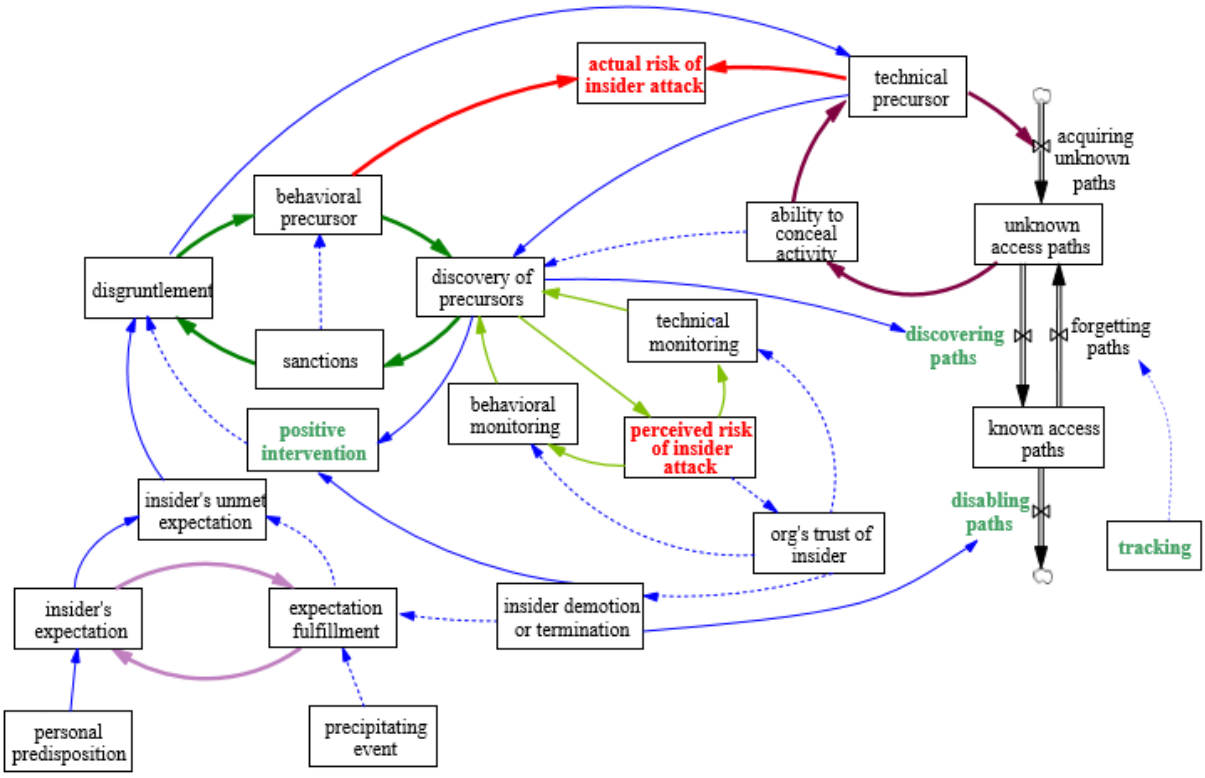
Since 2000 the CERT Insider Threat Center has been researching the insider threat problem (Cappelli et al. 2012; Legg et al. 2013) and is recognised as providing extensive and comprehensive contribution into insider threat (Nurse et al. 2014a). "The objective of the CERT Insider Threat Center is to assist organizations in preventing, detecting, and responding to insider compromises" (Cappelli et al. 2012,

p. 13). Using a system dynamics approach and their database of case studies, CERT researchers present models focusing on sabotage, theft and fraud. They term these as the Management and Education of the Risk of Insider Threat (MERIT) models.
The MERIT Models were developed to simulate the complex nature of insider threat (Cappelli et al. 2012). There was initially one main model (see Figure 2). Over time and through the course of research the CERT team recognised that not all insider threats were alike, hence they presented three main models; theft of intellectual property, IT sabotage, and fraud (see Cappelli et al. 2012).

The system dynamic method was chosen for its ability to capture the dynamic complexity of insider behaviour and allow for continuous feedback (Cappelli et al. 2012). It allows for the inclusion of soft factors (policies, procedure, culture) as well as hard factors (Cappelli et al. 2012). Graphically these models are represented as balancing and reinforcing feedback loops that underlie insider threat and demonstrate how the problem temporally unfolds (Cappelli et al. 2012).

The CERT team has modified the system dynamic presentation to some degree for practitioner ease. The all-encompassing model is presented below although publications since have presented models specific to each insider threat under research (sabotage, fraud, theft; see Band et al. (2006); Cappelli et al. (2012); Moore et al. (2011); Moore et al. (2008); Carnegie Mellon University (2016).

Figure 2: MERIT model Extreme Overview



Source: Cappelli et al. (2006).

Perhaps one potential weakness of the CERT's MERIT models is that they began from the identification of a specific insider-threat problem (sabotage, fraud, theft) and greater influences were incorporated potentially reducing its effectiveness with novel attack vectors (Legg et al. 2013). The MERIT models are essentially an organisation-centric viewpoint of the problem (Nurse et al. 2014a). The MERIT models were born out of an attempt to address individual, organisational, contextual and technical inputs (Band et al. 2006), however, the organisational focus is somewhat limited compared to the focus on technical and individual factors.

In the MERIT models, organisations are represented by perceived risk, trust of insider, and in their failure to recognise or detect problems (such as identifying technical precursors) and lack of controls. Band et al. (2006) state that future research can include factors such as management errors, organisational culture, and effectiveness of security awareness training to add breadth and depth to the organisational influences on insider threat.

A further limitation of this model is that system dynamics require accurate quantification of attributes and impacts that may not be available in the study of insider threat cases (Nurse et al. 2014a). Furthermore, from an applied perspective, the MERIT models can be seen as cumbersome and challenging for practitioners to use (Nurse et al. 2014a).

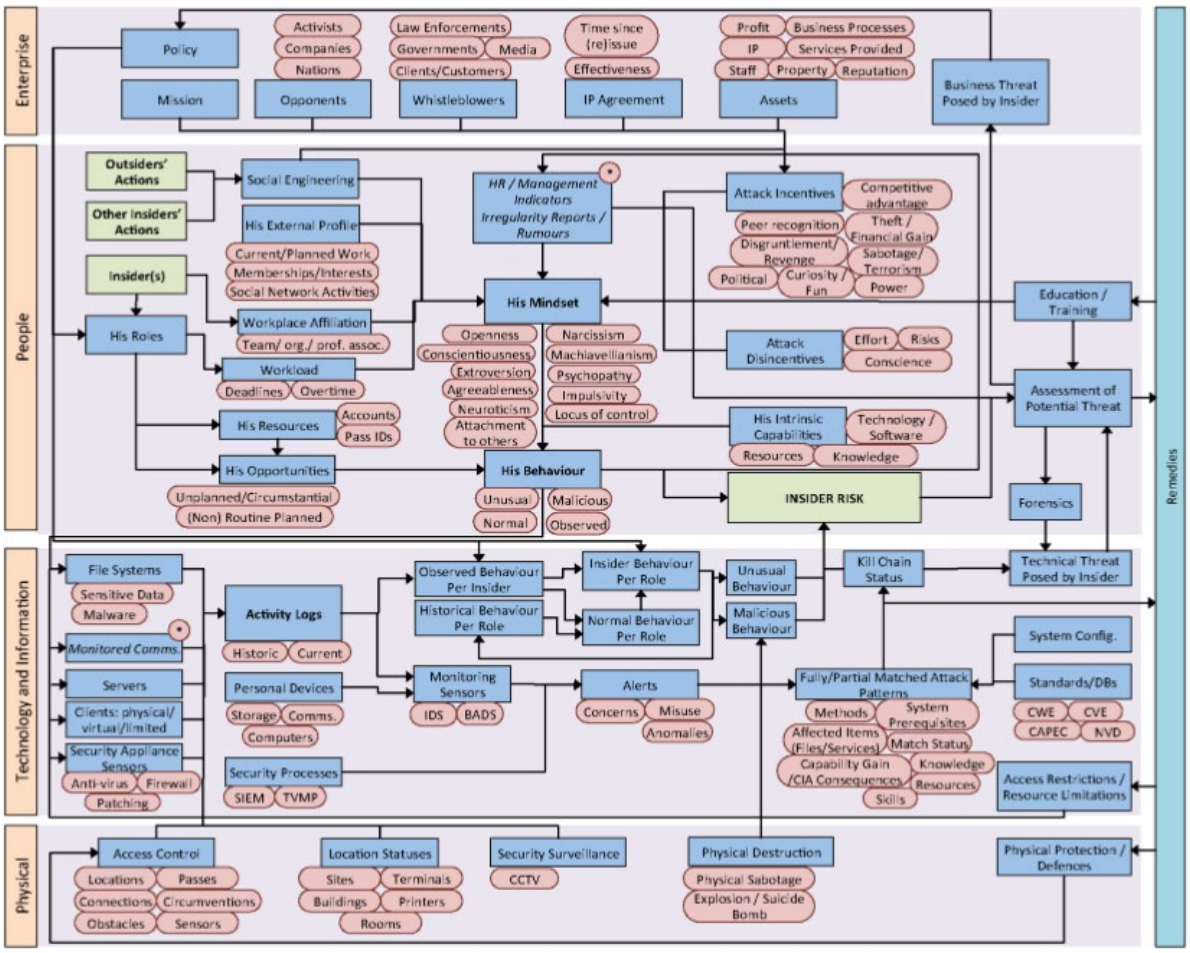
2.3.6.3 Cyber Security Centre, Department of Computer Science, University of Oxford

Legg et al. (2013) recognised the inadequacies of any model or reasoning structures to understand the entire picture of insider attacks. In response, they proposed a framework for modelling insider threat detection that they believe extends beyond previous models, including the MERIT models identified above. Legg et al. (2013) identified the opportunity to also extend beyond the technical to include behavioural and psychological characteristics leading to an "all-encompassing organisational view of the problem" (p. 21). It is commonly accepted that insider threat research has provided significant evidence on the importance of psychosocial factors and therefore any useful models must incorporate this focus (Greitzer et al. 2009).

The model (see Figure 3) proposed by Legg et al. (2013) consists of three tiers (Hypothesis, Measurement, and Real World) and draws on four 'lanes' to model the insider threat problem. They define each of these lanes as follows (Legg et al. 2013, p. 26):

(1) Enterprise – elements that constitute the enterprise on an operational level
(2) People – elements describing an insider, his motivations and his behaviour within the enterprise
(3) Technology and Information – elements relating to hardware and software in the enterprise and the digital activities that can be recorded
(4) Physical – elements that capture physical components (e.g. locations) that exist within the enterprise

Figure 3: Elements diagram that represents the Real World Level of the Legg et al. conceptual model



Source: Legg et al. (2013, p. 25).

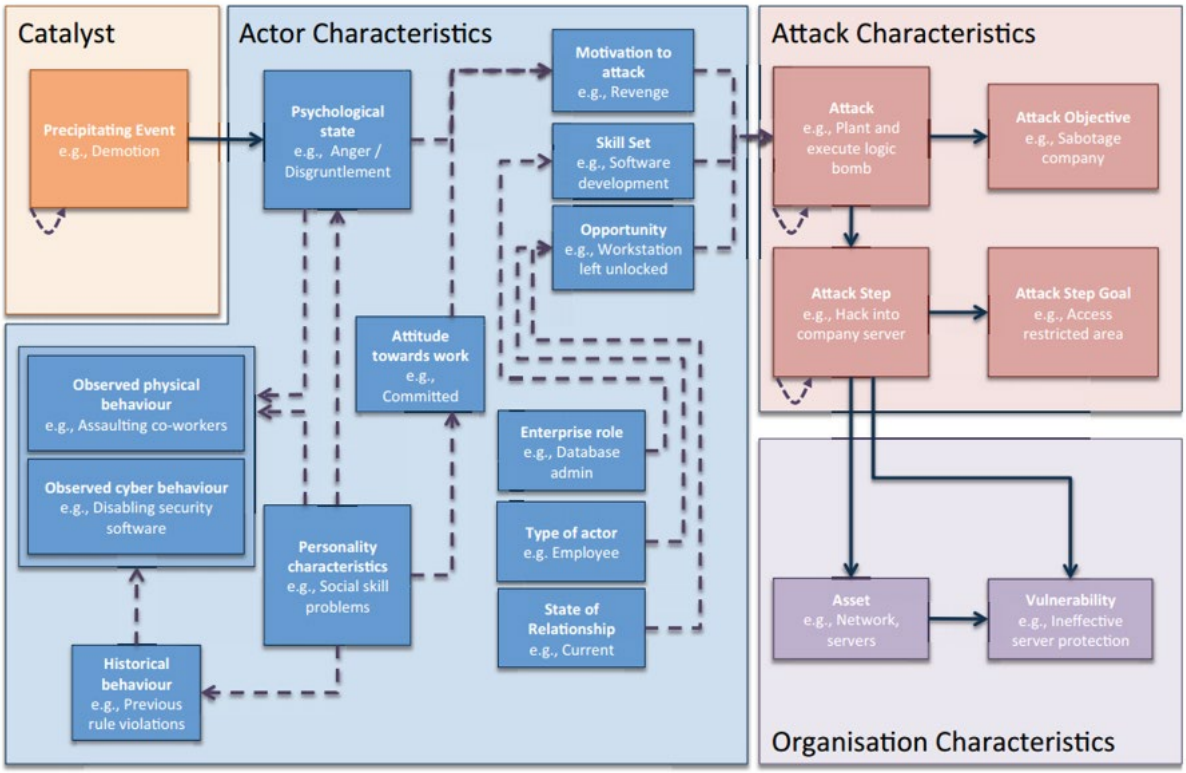
By focusing on four lanes in the model, Legg et al. (2013) have been able to extend over other models to consider additional aspects of insider threat. The model allows for inter- and intra-tier reasoning across psychological, social, and technological domains. It also allows for both a top-down and bottom-up reasoning process (Legg et al. 2013).

The benefit of this model is a direct representation of the *Organisation* and its capacity to influence insider threat (both positively and negatively). Organisational relationships, reputation, and culture for example are represented and allow for greater understanding of insider threat as a multifaceted problem. Further, Legg et al. (2013) propose that strategies or "remedies" can be implemented across the four

lanes demonstrating how an organisation can intervene to deter insider threat. Still, the model is not without criticism, for example, Sokolowski et al. (2016) suggest that the model's reliance on subjective conclusions rather than mathematical outputs is a limitation.

Extending on the Legg et al. (2013) model, Nurse et al. (2014a, p. 214) developed 'a grounded framework' for characterising and understanding insider attacks in a simple yet comprehensive way (see Figure 4). These researchers included; (1) technical and behavioural indicators (2) human factors and motivations, and (3) the range of attacks possible, in their framework that considers both intentional and unintentional insider threat (Agrafiotis et al. 2015; Nurse et al. 2014a).

Figure 4: Framework for characterising insider attacks



Source: Nurse et al. (2014b, p. 216).

As can be determined from Figure 4 the framework has several elements across four areas – Catalyst, Actor Characteristics, Attack Characteristics, and Organisation Characteristics. Dotted lines represent potential relationships whilst solid lines indicate a definite relationship between elements. Not only does the model account for individual factors (psychological state, personality, behaviour, motivation, etc.) and broader actor characteristics (e.g. role, skills, relationship status) but extends to consider the catalyst and the environment as well as the types of attacks possible.

Of most interest to the current thesis is the clear emphasis on organisation characteristics - Assets (items of value) and Vulnerabilities (weaknesses in assets or protections). The framework provides a means to incorporate the type of asset the organisation has but also the myriad of vulnerabilities that could be present, including lack of security awareness training, limited employee support, inadequate security and technological controls, and lack of staff training and supervision among others (Nurse et al. 2014a). There remains, however, a lack of emphasis on protective

measures within this model. It also places organisational characteristics at the back end of the model potentially de-emphasising the influence of organisational characteristics as a catalyst for insider threat action.

As with the other models presented above, the limitation of this framework is the lack of available research using the framework and looking at detection and prediction of insider threat actions. It also does not address practical concerns of implementation. As Nurse et al. (2014a) cautioned, a great challenge in using this framework (as well as others identified above) lies in ethical and legal considerations regarding the use of information, especially employee information. Greitzer et al. (2009) outlined that whilst personal information may be useful in the insider threat space it is unlikely to be legal or appropriate. However, use of organisational information and observational data provides a legal means of information gathering, including employee records and organisational feedback processes (Greitzer & Hohimer 2011; Greitzer et al. 2009). Despite the restraints outlined, this framework does provide a multidisciplinary view of the insider threat problem in a simplistic model that should be easy for practitioners to use.

2.3.7 Limitations of insider threat research

Whilst the limitations of insider threat research have been elucidated throughout this thesis, it is a worthwhile exercise to revisit the main concerns. Insider threat is a complex and difficult subject to study and because of this there are general flaws and limitations in the studies addressing insider threat. Festa (2012) describes the overall body of research on insider threat as biased, insufficient, and lacking. For example, in the USA the majority of research has been funded or directed by the Department of Defense. There has been a lack of attention to broader government, private enterprise and not-for-profit organisations have been insufficiently researched. In addition, applied research on insider threat in other parts of the world has been limited (Festa 2012), especially in Australia.

Many of the available studies have a high level of specificity and focus on one type of problem in a specific organisation. As such few empirical studies exist which are

publicly accessible (Schultz 2002). There is also a lack of controlled research (Shaw et al. 2009) with the majority of publications being descriptive and policy oriented rather than explanatory or predictive (Band et al. 2006).

Research is anecdotal, speculative (Greitzer et al. 2009; Hunker & Probst 2011), rich in case studies (Band et al. 2006; Liang & Biros 2016), and uses convenience samples (Randazzo et al. 2005) raising questions regarding the generalisability of the results. There is also a domination of demographic and psychological approaches showing correlation but not causation (Festa 2012a). This can prevent organisations from pursuing observed behaviour that may be suspicious given that the activity may be correlated but not causally linked with insider threat concerns (Hunker & Probst 2011). It can also lead to false positive results (Shaw 2006). As such further research is required to compare prevalence of predispositions with occurrence rates in employee population in order to validate the hypothesised relationships (Greitzer et al. 2009; Hunker & Probst 2011).

As Shaw and Stock (2011) discuss understanding the insider threat phenomenon is limited by access to insider threat information and the likely underreporting of insider threat cases. This results in data that is skewed and potentially biased. Hunker and Probst (2011) describe that the fundamental challenge in researching and gaining a greater holistic knowledge of insider threat is due to the lack of real data. Post hoc investigations are also speculative in predictive value (Hunker & Probst 2011). For example, as Shaw (2006) expresses information provided by convicted insiders (and known associates) is fraught with bias and questionable motivations.

From an applied perspective, the literature is growing and does provide insight into insider threat. However, current practice tends toward reactive and detection focus rather than predictive (Greitzer & Hohimer 2011; Greitzer et al. 2009) or protective outcomes. This is not a surprise given that detection is difficult and prediction is harder (Greitzer et al. 2013). Although one could argue that protective measures can be easily implemented and matched to organisational needs.

Whilst past research explores insider threat from a variety of perspectives there is more traction in recent times to explore insider threat through models that incorporate a multidimensional focus. A promising perspective that is limited due to its infancy and scarcity of controlled research and application of these models. As such, there is a limited amount of evidence that these models work. Some of these models also overemphasise the individual and/or technical aspects, and generally there is an absence of organisational protective measures within the frameworks. There is also argument that many models are statistically focused representing past activity and providing unsatisfactory representation of likelihood for future insider threat risk (Sokolowski & Banks 2015). Finally, several of the models are considered cumbersome and difficult to apply in practice.

It appears that legal and ethical considerations that were overlooked are gaining greater attention and will begin to filter through the study of insider threat. Legal, ethical and privacy related questions are being raised and some authors have begun to explore these topics further (Carpenter et al. 2018; Greitzer et al. 2009; Hunker & Probst 2011; Huth 2013; Nurse et al. 2014b; Reid 2018; Williams 2008; Young 2017). In a practical sense, at least in the United States of America, organisations have started implementing ethics and integrity hotlines (Gelles 2016). This may provide an avenue to capture suspicious behaviour but also help address the gap in research surrounding ethical and moral implications. Consideration of the legal ramifications of employing a formalised insider threat program will need greater review (Huth 2013). Also the implementation of such programs will be made more difficult by the variation in legal frameworks across countries.

Finally, the difficulty in researching and responding to intentional insider threat is that by its definition it is behaviour undertaken by an individual with the intention that it will not be discovered. The hidden nature of the offense makes it difficult to predict but also difficult to research in any way that is not retrospective in nature. In an applied and practical sense, organisations looking to protect themselves from potential insider threat activity will need to accept that pinpointing a specific insider actor is difficult and identifying all insider risk potential is virtually impossible.

However, reducing risk and mitigating efforts can be assisted by the implementation of a risk management approach to insider threat.

Thus far this thesis has provided a background to insider threat, an overview of past research and relevant models, as well as an exploration of limitations to insider threat research. Next, the thesis introduces the topic of risk management and how risk management can be applied to insider threat research and application.

2.4 Risk Management – Overview

2.4.1 Defining Risk

In his seminal book 'An Anatomy of Risk', Rowe (1977) discusses the complexity of the concept of risk. He defines risk as "the potential for realization of unwanted, negative consequences of an event" (Rowe 1977, p. 24). The online Oxford dictionary defines *risk* in a number of ways including a "situation involving exposure to danger" (Oxford Unviersity Press 2016a). Both of these definitions emphasise the negative consequences of risk and historically risk management has focused on ways of managing negative risk.

However, the definition of risk, and application of risk management, has evolved over time. Now, the term risk is associated with negative consequences, positive outcomes, and uncertainty of outcomes (Hopkin 2014a). Within risk management the definition of risk concentrates on risks as events. This is exemplified in the International Organization for Standardization (ISO) which defines risk as the "effect of uncertainty on objectives" where an effect can be both positive and/or negative (Standards Australia 2009, p. 1). Given that there is not a universally accepted definition of risk (Andretta 2014) the definition presented by the ISO underpins the current thesis.

2.4.2 Defining Risk Management

Risk management is an integrated approach to the assessment and evaluation of risk. The ISO defines risk management as the "coordinated activities to direct and control

an organization with regard to risk" (Standards Australia 2009, p. 2). Hopkin (2014a) states that organisations that take a proactive approach to risk and its management can expect improvement across strategy, tactics, operations, and compliance. The level of acceptable risk differs across organisations depending on their risk attitude and risk appetite. Personality and situational characteristics can also affect propensity to take risks (Rowe 1977). According to Dionne (2013) the absence of defining executive risk appetite was one of the underlying problems resulting in significant financial loss during the Financial Crisis of 2007-2008. As such, it is important that organisations define risk and implement risk management approaches tailored for purpose.

2.4.3 Development of Risk Management

Risk management has a long history with influence from a number of unrelated disciplines (Clarke & Varma 1999). The structured and organisationally driven approach to risk management reportedly began as an insurance management function in the United States in the 1950s (Dionne 2013; Hopkin 2014a). It continued to develop with the growing interest in business continuity planning during the 1960s. It was then applied to risk financing and risk control in Europe during the 1970s and simultaneously gathered momentum in the field of occupational health and safety (Hopkin 2014a). Risk management gained commercial and corporate status in the late 1990s with the application of risk management to project management, credit and financial risk, and eventually Enterprise Risk Management (ERM; Dionne 2013).

It is not surprising that the influence of various disciplines led to a fragmented approach to risk management and a number of different approaches and frameworks for operation (Clarke & Varma 1999). Traditional approaches to risk management therefore tend to address a specific risk, one at a time, in a silo technique (Grace et al. 2015).

However, with the growth of risk management the focus has shifted to a more holistic and integrated approach to risk management across the organisation (Clarke &

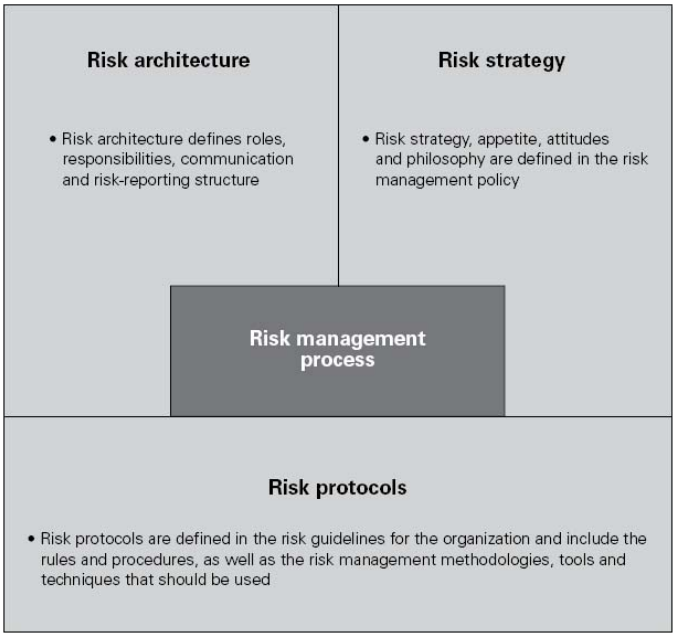
Varma 1999; Grace et al. 2015; Hopkin 2014a). The shift from a more fragmented approach to an integrated risk management approach has been important as the latter is linked with superior cost and revenue efficiency (Grace et al. 2015), better stock performance (Clarke & Varma 1999), greater organisational resilience (Hopkin 2014b), as well as greater protective function and maximisation of organisational value (Dionne 2013).

Risk management is now an established discipline that is applied across many professions and disciplines. It continues to develop, evolve and be applied to protect organisations in much broader scope. Whilst historically protection from hazards was the main focus, risk management in the 21st century has developed to include focus on control risks and opportunity risks (Hopkin 2014a). It has also sparked specialist areas of risk management such as health and safety, disaster recovery, business continuity planning, financial risk management, and IT risk management among others (Hopkin 2014a). It is not too far a stretch to consider that employee or HR risk management and more specifically insider threat may continue to grow as a specialist field of risk management.

2.4.4 Risk Management Frameworks and Standards

There are a number of risk management frameworks and standards that can be employed by organisations. A risk management framework is chosen based on specific organisational needs and alignment with concepts such as risk attitude and tolerance. According to Hopkin (2014a) a risk management standard contains both the risk management framework and risk management process. The framework is fundamental to the implementation and support of the risk management process. The framework has been represented in a multitude of ways, although Hopkin (2014a) offers a simplified version that demonstrates how components of the risk management framework (including risk architecture, risk strategy, and risk protocols) can support and enhance the risk management process (see Figure 5).

Figure 5: Components of a risk management framework



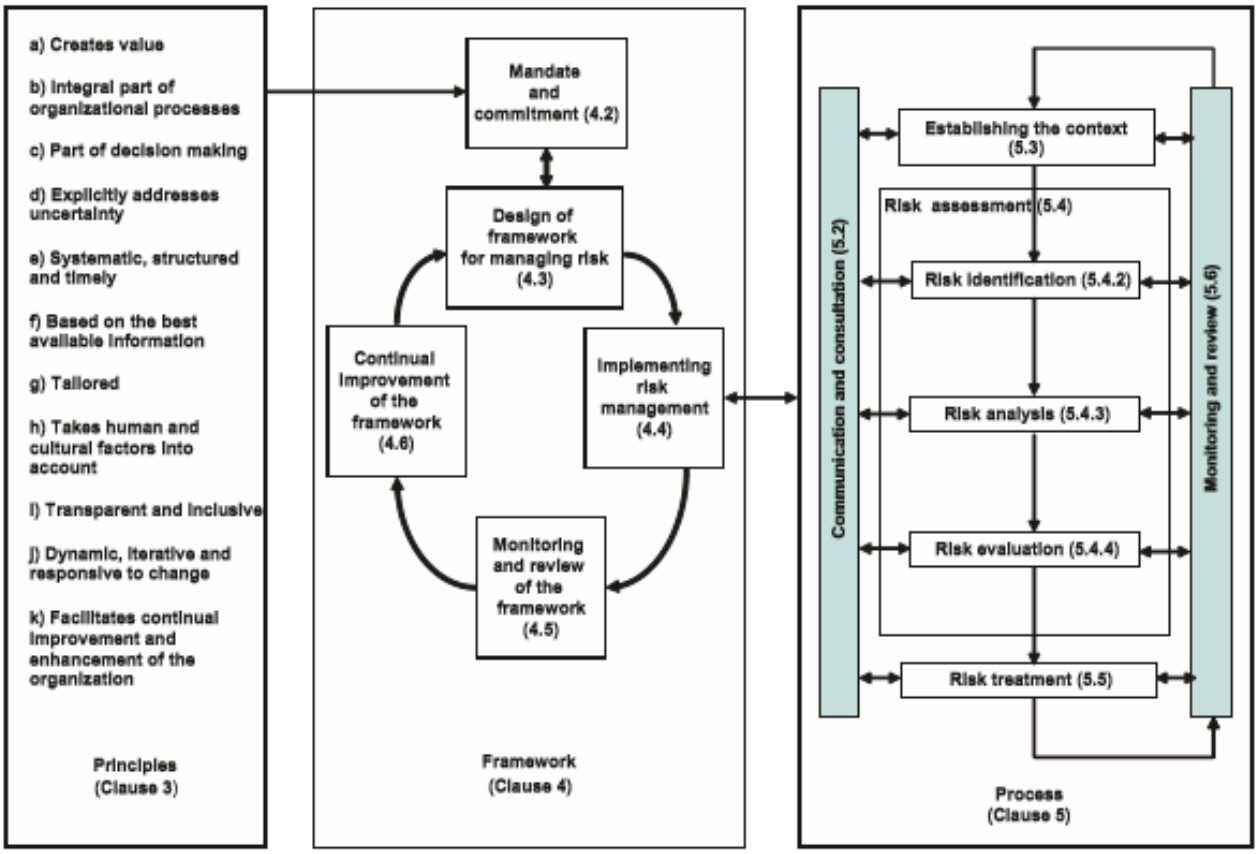
Source: Hopkin (2014a).

2.4.4.1 AS/NZS ISO 31000:2009

From an historical perspective the first risk management standards were developed in Australia in 1995 (Hopkin 2014a). Other countries, national standards bodies, and government agencies around the world followed (Hopkin 2014a). However, Australian standards have been long respected and widely recognised. It was the AS/NZS 4360:2004 that acted as the first draft of the international risk management standard and resulted in the ISO 31000:2009 (Standards Australia 2009).

The AS/NZ ISO 31000:2009 is a generic guide for managing risk which can be utilised by both public and private enterprise. It is an international standard that is not specific to any industry or sector (Leitch 2010). The AS/NZ ISO 31000:2009 (Standards Australia 2009, p. iv) provides a systematic and logical process and describes the "relationship between the principles of managing risk, the framework in which it occurs and the risk management process" (see Figure 6).

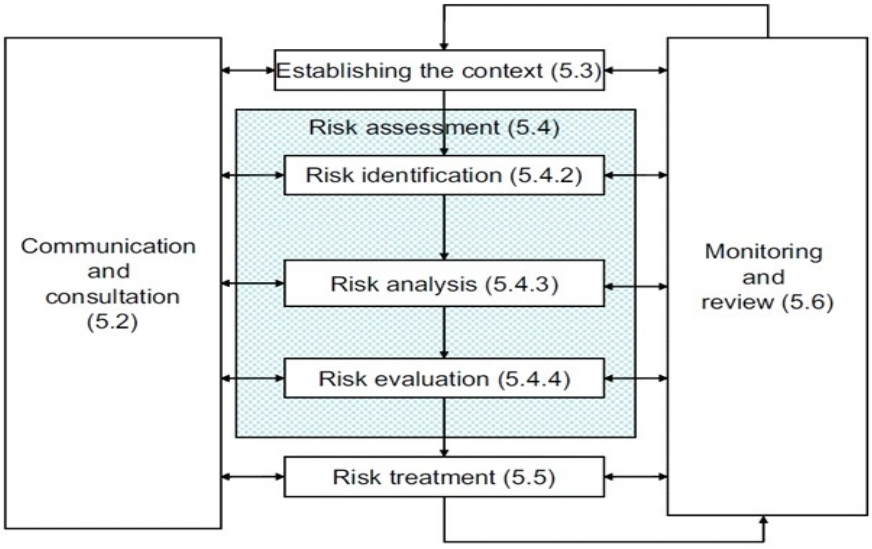
Figure 6: Relationships between risk management principles, framework and process



Source: Standards Australia (2009).

The AS/NZ ISO 31000:2009 is a risk management framework that can provide the foundation for designing, implementing, monitoring, reviewing and continually improving insider threat management throughout an organisation. Within the framework, risk management is covered by (1) implementing the framework for managing risk, and (2) implementing the risk management process (Standards Australia 2009). Of particular interest in this thesis is the risk management process and specifically the risk assessment component (that is, identification, assessment, and evaluation of insider threat). The risk management process as defined in the AS/NZ ISO 31000:2009 is a seven step process (see Figure 7 below).

Figure 7: Risk Management Process



Source: Standards Australia (2009).

The AS/NZS ISO 31000:2009 (Standards Australia 2009, p. 3) defines the risk management process as a "systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk". Risk assessment is defined as the overall process of risk identification, risk analysis and risk evaluation (Standards Australia 2009, p. 4). The risk assessment component has not changed significantly to that presented over 40 years ago where the elements of risk assessment included risk identification, risk estimation, and risk evaluation (Rowe 1977). Hopkin (2014a) suggests that it can be argued that the risk management process of the AS/NZ ISO 31000:2009 contains elements of the risk management framework along with the key stages of the risk management process.

2.4.5 Risk Management and Insider Threat

As has already been described in the previous chapter there are limitations to the study of insider threat. Catrantzos (2012) explains that insider threat is heavily represented by cyber research and technological approaches. The representation of other disciplines is growing with influence from information management, organisational behaviour, and risk management. The diversity in approach to the

study of insider threat has resulted in multiple and distinct perspectives with a lack of an underlying systematic framework (Liang & Biros 2016). There appears to be a fundamental lack of an underpinning multidisciplinary framework to guide insider threat research, application, and delivery. As described in the previous chapter, there are models and frameworks to guide research in specific disciplines, with those that have a specific emphasis on organisational factors described in more detail, there is no commonly accepted risk management framework or policy to manage the risk of insider threat (Hunker & Probst 2011).

It is understood that insider threat is a complex issue and as such should sit within a multidisciplinary context rather than depend on a single discipline of study. In finding a multidisciplinary approach it was discovered that the risk field is "strongly multidisciplinary, thus involving many communities of scientists and practitioners" (Aven & Zio 2014, p. 1170). A full and comprehensive risk process which promotes best practice fits within the broader risk management framework. This is consistent with conclusions by Theoharidou et al. (2005) that insider threat mitigation can benefit from a multiparadigm and multidisciplinary approach. And Shaw and Stock (2011) that risk assessment (a component of risk management methodology) is best made by a multidisciplinary team.

In September 2016 a search for "insider threat and risk management" on the USQ library search function revealed fewer than 11,500 peer-reviewed journal articles. Not surprisingly many of these were related to technical solutions and cyber security. There was a distinct lack of integration of risk management principles in the study of insider threat; rather the two terms appeared in the literature often separately in an unrelated sense. At the same time, a more specific search on "insider threat" and "risk management" produced only 136 journal articles. Consistently many of these publications failed to discuss in any great detail the relationship between insider threat and the risk management process or the importance of the nexus between the two. In fact in the library database there were a very limited number of publications that directly focused on risk management as an underlying framework or

multidisciplinary approach to better understand insider threat and apply mitigation strategies.

Perhaps the limited focus on an integrated study of insider threat relates to the greater investment that organisations make in protecting themselves from external, rather than internal, attacks. Gelles (2016) indicates that it is common for organisations to deprioritise investment in an insider threat mitigation program reasoning that insider attacks are less common than external attacks. Even though it has been argued that the insider can, through exploiting their knowledge and abilities, cause more damage than an external adversary (Bishop et al. 2010). In addition, the ability of an organisation to manage risk in the workplace is related to insider threat behaviour (Gelles 2016).

Positioning insider threat within a risk management framework, though not a unique contribution, is not well explored in the literature. As expressed by Cho and Lee (2016, p. 405) although there are few studies integrating risk measurement and insider threat, "[t]he insider problem can be approached in terms of risk management". In the limited publications positioning insider threat within a risk management framework, the majority are from overseas hardly any specific to Australia. Two relevant and widely referenced overseas publications which specifically focus on insider threat and risk management methodology provides direction for organisations to assess, protect, respond and recover from employee risk (CPNI & PA Consulting Group 2012) and focus on how to prevent, detect, and respond to various information technology crimes (Cappelli et al. 2012).

Within Australia there appears to be only one publication that specifically addresses insider threat in the risk management context. The Protective Security Policy Framework (PSPF, Protective Security Policy Section Attorney-General's Department 2010, p. 12) mandates Australian Government to "adopt a risk management approach to cover all areas of protective security activity across their organisation, in accordance with the Australian Standard for Risk Management AS/NZS ISO 31000:2009 and the Australian Standards HB 167:2006 Security Risk Management".

However, there is no such guidance or mandate for private and Not-for-Profit enterprises. Gelles (2016, p. 1) suggests that this lack of mandating makes it difficult for non-government agencies "to assess where they stand relative to peers and to make decisions regarding their insider threat mitigation capabilities". The PSPF focuses on protecting people, information, and assets. It provides coverage for managing the insider threat and people of security concern (Attorney General's Department 2016).

Applying risk management standards to the study of insider threat allows for a consistent approach which can help to systematically dissect insider threat. It may also work to provide organisations with a consistent language in addressing insider threat. Risk management standards provide organisations the ability to meaningfully determine what can happen, how often it is likely to happen, and with what consequences (Luko 2013). Gelles (2016) explains that whilst many organisations have an enterprise risk management strategy, few address insider threat. The Intelligence and National Security Alliance (2013) reports that 25-50% of the surveyed organisations have formal insider threat programs. This low rate of insider threat program uptake is a concern given that successful prevention and/or mitigation of insider threat relies on organisations addressing their vulnerabilities as part of their enterprise risk management strategy (Gelles 2016; Intelligence and National Security Alliance 2013; Stafford et al. 2018).

2.4.6 Risk Management Standards and Insider Threat

Colwill (2010) reports that a proactive approach to insider threat, that includes assessment, prioritisation, and action, is required. He notes that while organisations are coming to accept the risk of insider attack they are not in a position to effectively identify, measure, monitor, assess or quantify their risk level. The argument of this thesis is that in order to prevent, detect, deter, and mitigate insider threat, a holistic framework is relevant. It is not the intention that the risk management framework should replace all existing models, but that it complements other models and provides the relevant multidisciplinary focus.

The Risk Management Standard – AS/NZS ISO 31000:2009 - can be applied to the study and practice of insider threat. The Australian Government requires an approach to manage insider threat that is consistent with the AS/NZS ISO 31000:2009 guidelines, however, as previously mentioned this is not enforced by non-government entities. Despite some objections and concerns regarding the AS/NZ ISO 31000:2009 (see Leitch 2010) an insider threat risk management approach that is based on the Australian Standard is considered, by the Australian Government, as integral to organisational processes and may be enhanced by the additional focus on security risk management.

2.4.7 Security Risk Management and Insider Threat

When applying risk management to insider threat the Handbook of Security Risk Management (HB 167:2006; Standards Australia 2006, p. 3) provides additional support through guidance on "fundamental assessment, control and treatment processes". The HB 167:2006 is a broad approach that covers the critical elements to be covered in a security risk management process as provided in Figure 7. The structure of the security risk management process is further elaborated in Table 1.

Table 1: The structure of security risk management.

Communicate and consult	communicating and consulting with internal and external stakeholders within each of the security risk management stages
Establish the context	the external context, the internal context, the security risk management context, structuring the security risk management activities, developing evaluation criteria
Identify risks	determining the threats, identifying critical organisational and community elements under threat determining the vulnerability of those elements to the threats identified, identifying specific events and scenarios that might affect individuals, organisations, or communities, and their possible consequence
Analyse risks	evaluating existing controls (security and emergency systems), determining the consequence should the risk eventuate, determining the likelihood of such a risk with that consequence occurring, defining a level of risk based on a combination of consequence and likelihood
Evaluate risks	determining the tolerance to individual risks, evaluating the need for any further treatment of those risks
Treat risks	developing recommendations and strategies for the treatment of priority risks, assigning accountabilities, responsibilities and budget for risk treatment activities
Monitor and review	monitoring of the external and internal security environments to detect change, review of the risks and their treatment strategies, monitoring and reviewing progress and outcomes of each of the steps of the process.

Source: Standards Australia (2006).

2.4.8 Applying Risk Management Process to Insider Threat

Colwill (2010) reports that organisations have started accepting the risk of insider attack but are not in a position to effectively identify, measure, monitor, assess or quantify their risk level. The risk management process (see 2.2.4, and Figure 7), along with guidance from the security risk management process (see 2.2.7 and Table 1), can be applied to insider threat and help to address this limitation. By systematically and logically applying the risk management methodology discussed above, organisations can effectively and efficiently identify and begin to manage the risk of insider threat.

Using the risk management process provides a standardised approach to identification, assessment, and evaluation of insider threat. A standardised approach

allows for comparisons within and across organisations, enhances shared understanding and facilitates decision making and judgment (Homeland Security 2011).

The use of a risk-based approach to insider threat may also assist to justify an organisation's investment in an insider threat program. It is understood that standard risk management principles offer broad guidance to effectively address insider threat. However, tailoring risk management principles to the specific needs of an organisation creates the most benefit (Homeland Security 2011).

To date, it appears there is limited literature that has explicitly expressed insider threat through use of risk management process as defined by the Australian Standards (AS/NZS ISO 31000:2009). This is a unique contribution made by the current thesis. Section 2.2.8.1 through 2.2.8.3 discusses the seven-step risk management process. The discussion allows the reader to understand the current literature on insider threat and how it can be applied to or support risk management methodology. Whilst all components of the risk management process are explored, particular attention is given to the *risk assessment* section (see Figure 7 and Table 1). The risk assessment process underpins the current research providing the importance of the utility of assessment of organisational vulnerability to insider threat.

2.4.8.1 Communicate and consult

Communication and consultation with all stakeholders, internal and external, is the first stage and an important consideration in combatting insider threat. During this stage, issues relating to insider threat risk, its causes, its consequences and any measures currently in place to mitigate insider threat, should be addressed. By adapting the AS/NZS ISO 31000:2009 (Standards Australia 2009) and relating it specifically to insider threat the following objectives may be achieved:

- Ensuring that interests of all stakeholders are understood and considered;
- Ensuring that insider threat risks are adequately identified;

- Bringing together a multidisciplinary team of experts to analyse insider threat risks;
- Allowing different views to be considered when defining insider threat risk criteria and evaluating insider threat risks; and
- Securing endorsement and support for an insider threat program.

The HB 167:2006 (Standards Australia 2006, p. 16) states that ensuring the participation and commitment of senior management is a "fundamental requirement" in the success of any risk management program. Such a commitment is essential to an insider threat program as it will result in outcomes for which management will be responsible, including time, costs, and resources. Support and commitment of management to risk management also provides a consistent message on the priority (Clarke & Varma 1999; Dionne 2013; Standards Australia 2006) of insider threat management and can also affect organisational culture.

Hu et al. (2012) determined that management participation in information security initiatives positively influences organisational culture, employee attitude, and compliance with security. Insider threat programs are not able to succeed if executives are not fully engaged in the program (Intelligence and National Security Alliance 2013; Sarkar 2010).

In addition, engagement and participation of staff can help to further integrate insider threat management into the organisation (Standards Australia 2006). Research outcomes suggest that networks of insider threat actors are often aware of insider threat activity (Randazzo et al. 2005; Shaw & Stock 2011). As such employees are a strong alliance to an insider threat program and implementation of strategies such as confidential reporting can increase organisational awareness of suspicious incidents (Intelligence and National Security Alliance 2013). Staff can contribute across stages including the identification and assessment of risk as well as participate in risk treatment arrangements (Standards Australia 2006).

Building strong partnerships internally is key to an effective insider threat management program (Intelligence and National Security Alliance 2013).Engagement of staff can facilitate the transfer and communication of risk information within the organization. Improving employee awareness through training, security awareness programs and communication (Alavi et al. 2014) and ensuring employees know how to report suspicious behaviour are recommended as insider threat risk management strategies (Farahmand & Spafford 2013; Randazzo et al. 2005). Involving staff in the various layers of the risk management process, including design and implementation of insider threat controls, is encouraged (Theoharidou et al. 2005).

As described in Chapter 1, the definition of an insider includes any person with knowledge and access. Therefore, in the communication and consulting phase, external stakeholders, vendors, and suppliers should be included. External communication is considered integral to effective risk management by Homeland Security (2011). The Standards Australia (2006) recommends that a security risk management approach that includes such stakeholders can benefit the organisation through developing partnerships, building shared understanding, gaining additional perspectives, and understanding how an insider threat program may affect stakeholders. Research has also found that satisfactory collaboration and communication may play a role in insider threat prevention. If insider threat experts can learn from incident response research, then collaboration is important to obtain knowledge, rely on stakeholder notification of threats, and verify actual threats (Werlinger et al. 2010).

2.4.8.2 Establish the context

The context in which an organisation operates will determine its objectives, parameters and scope with relation to insider threat. Not all organisations operate within the same context and that is why establishing the context is one of the most important activities in developing any security risk management process (Standards Australia 2006). The AS/NZS ISO 31000:2009 (Standards Australia 2009, p. 3) describes establishing the context as “defining the external and internal parameters to be taken into account when managing risk”. Establishing the context requires

taking into consideration the type of organisation, its relationship to other organisations, and organisational culture. It involves a review of the external and internal environment in which the organisation operates and seeks to achieve its objectives (Standards Australia 2009). Further the establishment of the objectives, strategies, and scope of the process is determined (i.e. establishing the context of the risk management process). In addition defining risk criteria in terms of evaluating the significance of risk is undertaken (Standards Australia 2009). Information gathering can involve interviews, questionnaires, document reviews, and use of other monitoring tools (Sarkar 2010).

As HB 167:2006 (Standards Australia 2006) expresses, the risk management process describes the external context, internal context, and risk management context separately, however, the utility of such a distinction is not necessary. In practice, all three tiers relate to each other, will inform the other, and will influence insider threat risk management. In order to represent the literature on insider threat, each of the contexts has been separated out below, keeping in mind that the danger of doing so in practice may underrepresent the interdependencies and interfaces between the contexts (Standards Australia 2006).

External context

AS/NZS ISO 31000:2009 (Standards Australia 2009, p. 15) defines the external context as "the external environment in which the organization seeks to achieve its objectives". It is an important step in determining how the external environment can affect the way an organisation does business (Standards Australia 2006). A consistent monitoring process allows organisations to be aware of all the risks they face (Clarke & Varma 1999). When considering the external context in relation to insider threat there are three main shifts that occur; (1) heightened political attention, (2) introduction and continued development of technology, and (3) the growing consideration of legal/ethical understanding.

Policy requirements have altered the state of insider threat management. Organisations, certainly within government, across the world are expected to

implement relevant and necessary insider threat controls and develop a greater level of security consciousness (Sarkar 2010). For example, in the USA the *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*, directs government departments and agencies to establish insider threat programs with emphasis on risk management principles of deter, detect, and mitigate. As has previously been discussed the Australian Government also mandates government entities, through the PSPF, to adopt a risk management approach to insider threat.

In his book on insider threat, Gelles (2016) discusses how insider threat has been changed by the introduction of information technology. He argues that insider threat activity is significantly enhanced by technology and that traditional methods of countermeasure, namely physical security, are no longer effective. Gelles suggests that the external context has changed – destructive behaviour is more easily performed and societal norms have shifted. However, the threat of insider behaviour remains. Further, from a technology perspective the proliferation of the Internet of Things (IoT) – increasing the connectivity of everyday devices - is challenging organisations to consider new insider threat attack vectors (Choo et al. 2018; Nurse et al. 2015).

Finally, a discussion of the external context and insider threat is not complete without consideration of the legal and regulatory environment. As discussed in the previous chapter challenges in addressing insider threat relate to ethical and legal considerations regarding the use of employee information. Whilst organisational data may be an appropriate way to address insider threat concerns, use of specific employee information is likely to be inappropriate and perhaps illegal. There is a requirement to balance the protection of employee privacy against organisational insider threat protection (Gelles 2016). Unfortunately, current guidance is limited by a lack of research and applied focus on legal and ethical implications. Further legal responses have been described as “confusing” (Ford et al. 2015). Legal, ethical and privacy related questions are being raised and some researchers have begun to explore these topics further (Carpenter et al. 2018; Greitzer et al. 2009; Hunker & Probst 2011; Huth 2013; Nurse et al. 2014b; Reid 2018; Williams 2008). Certainly the

discussion is made more difficult by the variation in legal frameworks across countries. A review of Australian law and insider threat is outside the scope of this thesis. However, to date, there does not appear to be easily identifiable legal advice or substantial commentary in relation to legal, ethical, and privacy issues as it relates to insider threat in Australia.

Internal context

Each organisation will have a different internal context to consider. It is important that an organisation's culture, processes, structure and strategy are considered when establishing the internal context (Standards Australia 2009) of an insider threat risk management process. In the insider threat literature there are many case studies and sector specific research that can contribute to understanding insider threat in terms of the internal context and risk management. As a result there is a growing body of literature determining how organisational culture, including security culture, contributes to (or mitigates) insider threat.

For example, research into the banking and finance sector by Randazzo et al. (2005) found that 15% of insider attacks were motivated by dissatisfaction with company management, culture, and policies. An Australian study by Parsons et al. (2015) also found that improving security culture can lead to positive employee behaviour. In reviewing the literature Renaud and Goucher (2014) found that security culture is tied with security behaviour. However, empirical research is limited and future longitudinal studies are needed to assist understanding the effect of implementing and fostering security cultures.

Location of business sites is an area that is explored under the internal context (Standards Australia 2006). It is important to note that while work-life balance and employee engagement practices promote flexible work arrangements, including working from home; this can raise insider threat risk. Randazzo et al. (2005) found that remote access is a source of vulnerability and that strategies to lower risk should be employed such as layered security, access only to non-critical data, and closer logging and auditing of remote transactions. Sarkar (2010) states that organisations

that outsource operations need to be alert to differences in culture, values, and serviceability that may affect insider threat and its assessment.

Insider threat risk management context

Organisations need to understand what they are trying to achieve from applying an insider threat risk management process. Therefore, it is important that "objectives, strategies, scope and parameters" are established (Standards Australia 2009, p. 16). Successful insider threat management must move beyond the concept of 'one size fits all' and look directly at bespoke strategies and organisational circumstance (Borrett et al. 2013).

Defining insider threat is an important consideration here. It is thought that few organisations have an operationalised definition of insider threat, without which an insider threat program cannot be fully formulated (Gelles 2016). As discussed in the previous chapter there are many definitions of insider threat and organisations should work to use (or develop) one that best fits their specific risks and circumstance.

After defining insider threat organisations are better placed to understand their objectives, scope of interest, and any parameters of the insider threat risk management approach and determine who is responsible for risk management in the organisation. Also, who is accountable and what resources are to be deployed (Standards Australia 2006). Gelles (2016) recognises the importance of determining not only who is accountable but also the cross-functional key stakeholders who are responsible for implementing risk mitigation measures.

Organisations must also understand their tolerance to risk. Understanding the risk tolerance of the organisation, as well as key stakeholders, will provide direction to the insider threat program. What level of risk is the organisation willing to accept when it comes to insider threat? What are the critical assets it is protecting? And, how can the organisation balance security and efficiency (Gelles 2016)? Responses to

these questions will help determine which insider threat management tools and approaches will be utilised (Standards Australia 2006).

Defining risk criteria

The way insider threat risk is evaluated should be considered during stage one, establishing the context. Criteria to be used in the evaluation of the significance of insider threat risk are established during this stage and should "reflect the organizations values, objectives and resource" (Standards Australia 2009, p. 17). It should also be consistent with the organisations broader risk management policy. Generally risk criteria cover consequence, likelihood, measurement, and treatment (Standards Australia 2006, 2009).

2.4.9 Risk Assessment

Risk assessment is defined as "the overall process of risk identification, risk analysis and risk evaluation" (Standards Australia 2009, p. 17). According to Rowe (1977) formal assessment of risk is not only possible but something that should be pursued. Risk assessment is the third stage and an integral component of insider threat management. Insider threat assessment should incorporate technical, people, and organisational vulnerabilities (Sarkar 2010). Bishop et al. (2010) indicate that insider threat assessment should include an appreciation of who has the capability to attack but also who is likely to attack. However, this is difficult to measure and has been indicated as a limitation of insider threat research, application and management by a number of authors (Hunker & Probst 2011; Sarkar 2010).

Organisations perform basic tasks through the lifecycle of employment. It is during these interactions that organisations can mitigate or magnify insider threat behaviour, but also "act to prevent, deter, detect, and manage insider threat risk". with Shaw et al. (2009, p. 4). For example, both work overload and perceived invasion of privacy can result in employee stress. However, organisations may be able to mitigate these stressors through improving attitude towards compliance with information security policy and increasing staff security knowledge (Lee et al. 2016).

Webb et al. (2014b) noted, that with regard to information security risk management, opportunities are being missed due to perfunctory and occasional risk assessment. Flowerday and Tuyikeze (2016) found that when it comes to security information policy, the risk assessment stage is the most important in identifying threats and vulnerabilities.

Previous research suggests that insider threat is misperceived due to limited measurement tools and that a good assessment methodology may advance insider threat assessment and focus (Chinchani et al. 2005). Hence the utility of developing an insider threat assessment inventory focused on organisational vulnerability.
It is the risk assessment stage of the risk management process that is directly relevant to the current research. A diagnostic inventory is being developed to assist organisations to understand their own potential insider threat vulnerabilities. The inventory will assist organisations to identify areas of vulnerability, gain a baseline assessment of potential insider threat risk, and provide information to evaluate whether to treat identified insider threat risks.

2.4.9.1 Identify risk

A thorough exploration of potential insider threat risk is undertaken during the risk assessment stage of the risk management process. According to the ISO Standards Australia (2009, p. 17) identifying risk includes identification of "sources of risk, areas of impacts, events … and their causes and their potential consequences". Use of up-to-date information and involvement of subject matter experts can help identify risks (Standards Australia 2009). It is also recommended that identification of threats is an on-going process due to the dynamic nature of threat agents (Sarkar 2010).

The HB 167:2006 (Standards Australia 2006) describes that the interaction between a threat and something or someone else, creates risk. Applied to insider threat it is the 'insiders' interaction with someone or something (organisational structure, supervisor, culture, personal stress, etc.) that causes an event (theft of IP, fraudulent transactions, etc.) and results in consequences (disruption to organisation services, investment losses, etc.).

This interplay can be demonstrated by the critical pathway approach described in an earlier chapter (see section 4.5.1). The model (Figure 1) portrays how personal predispositions and stressors can affect judgment and reliability leading to concerning behaviours. If these behaviours are met with maladaptive organisational response then a hostile event is more likely.

The identification of risks can be determined through a variety of data and information sources, including organisational loss and incident data, employee satisfaction surveys, IT specific data, and exit interviews. A broad approach to identifying risks should be undertaken and include the viewpoints of varied stakeholders (both experts and staff). The team must be able to assess, challenge, integrate, and progress insights obtained from these stakeholders (Aven & Zio 2014). The potential sources of risk in the HB 167:2006 (Standards Australia 2006) that appear most relevant to insider threat include people, technology, strategy, leadership, stakeholder management, processes, and competition. When considering intentional insider threat the threat type is malicious. A malicious threat is one that includes, among others, sabotage and unauthorised disclosure. It is "usually a specific direct attack on the targeted organisation and is often motivated by revenge, fame, association or challenge" (Standards Australia 2006, p. 53). As explained earlier very few organisations have a working definition of insider threat, even though it is an important first step to mitigating risk.

Threat can be understood in terms of intent (motivation) and capability, with some also including opportunity (Sarkar 2010; Standards Australia 2006; Theoharidou et al. 2005). Rowe (1977) discusses motivation, in terms of risk, as being the avoidance of an undesirable state or the pursuit of a desired position. It is not surprising therefore to find research in the insider threat space on intent/motivation and capability (skills, knowledge, access; see previous chapter). As Nurse et al. (2014a, p. 226) write "[f]oundational work in risk management suggests that if an individual has motive, capability and opportunity, then they are likely to conduct an [insider] attack".

Still, the likelihood of an insider threat is difficult to determine as there is a large degree of uncertainty around occurrence. Some authors argue that assessment of likelihood is flawed (Funston & Wagner 2010) and in the case of intentional insider behaviour, offenders are likely to adapt their tactics in response to controls and countermeasures. Several researchers raise concerns regarding the limitations posed by underreporting (Randazzo et al. 2005) and the lack of real (not anecdotal) data (Hunker & Probst 2011). Limited reporting of insider threat is not necessarily confined to incidences and events but organisations also demonstrate a reluctance to discuss their own specific insider threat programs (Intelligence and National Security Alliance 2013).

There remains debate as to whether current prevention and detection responses are effective in reducing the insider threat (Hunker & Probst 2011) or whether they are generally an inconvenience (Chinchani et al. 2005). Regardless, identifying potential vulnerabilities using risk assessment and implementing relevant countermeasures is recognised as a necessary organisational activity (Sarkar 2010). Mitigation strategies and countermeasures can reduce the likelihood of a successful insider threat event when applied appropriately. Merely the presence of a security measure or an enforced policy can lead to deterrence of insider threat behaviour (Chinchani et al. 2005).

In order to mitigate threats organisations can introduce controls that can reduce the likelihood of occurrence (Baracaldo & Joshi 2013). Research consistently demonstrates that a greater likelihood of detection and consequence reduces the attractiveness of insider threat activity. For best outcomes, controls are encouraged to be customised to the organisational needs (Vaidyanathan & Berhanu 2012). Such tools may be technical or non-technical (Borrett et al. 2013) and include data leak prevention systems (Epifantsev et al. 2016), auditing and monitoring (Bishop et al. 2010; Hunker & Probst 2011; Randazzo et al. 2005; Sarkar 2010; Stafford et al. 2018), role based access control and separation of duties (Baracaldo & Joshi 2013; Dorminey et al. 2012; Hunker & Probst 2011; Randazzo et al. 2005; Sarkar 2010; Theoharidou et al. 2005), pre-employment screening (Chinchani et al. 2005; Randazzo et al. 2005;

Shaw & Stock 2011; Theoharidou et al. 2005), active education and training regarding policies (Randazzo et al. 2005; Shaw & Fischer 2005; Theoharidou et al. 2005), security awareness programs (Chinchani et al. 2005; Randazzo et al. 2005; Sarkar 2010; Shaw & Stock 2011), and whistle-blower hotlines and protections (Dorminey et al. 2012) among others.

The usefulness of up-to-date, relevant, and enforced organisational policies should not be discounted. As Randazzo et al. (2005, p. 10) indicate, based on their research in the financial sector, "inadequate or non-existent practices, policies, and procedures" are often exploited. In addition, Vaidyanathan and Berhanu (2012) emphasise the importance of organisations sharpening their security policies to ensure a successful security program. Further, Zafar et al. (2014) conducted a case study looking at security risk management in healthcare and discovered that a risk management program can be rendered ineffective if not *all* employees are fully committed and aware of risk management policies.

It must be acknowledged that even the most sophisticated insider threat controls may be seen as a challenge by some insiders who will not be deterred (Theoharidou et al. 2005). There is a growing acceptance that not all risks, including insider threat risks, can be easily identified or understood (Funston & Wagner 2010); Hence the importance of a multifaceted approach to insider threat and its management.

An organisation's ability to respond to insider threat can be improved by incident management capability. According to Funston and Wagner (2010) efficiency and effectiveness of an organisation's recovery is directly related to its crisis response capability. That is why embedding insider threat management within risk management is of importance. It allows consideration of existing controls such as critical incident management capability and security planning and response capability. The existence of crisis management is suggested by Rowe (1977) to directly and positively influence a group's ability to deal with negative events. Organisational resilience may also be positively affected by such capabilities. In practice less than half of the organisations surveyed by the Intelligence and National

Security Alliance (INSA) indicated having formal incident management plans (Intelligence and National Security Alliance 2013). The INSA (2013) described that a formal insider threat mitigation program should have authority to conduct investigations and enquiries.

Understanding vulnerability is an important component of the current study. Assessing an organisations vulnerability level provides organisations with an understanding of strengths and weaknesses when it comes to existing controls. It also provides a focus for future development of countermeasures and mitigations that can be put in place to further protect the organisation. Hence, the aim is to elucidate the effectiveness of controls against insider threat risk by determining an organisations ability to deter, delay, detect, respond, and recover from an insider attack. Insider threat control elements (adapted from Standards Australia 2006) may include:

- *Deter*: bag checks, security awareness training, codes of conduct, vetting, physical and procedural security controls
- *Delay*: physical barriers, password protection, biometrics/iris scanners
- *Detect*: CCTV, automated IT programs, database mining, staff vigilance, security awareness
- *Respond*: security breach response, organisational intervention – noting that organisational response can both magnify and mitigate risk
- *Recover*: Provision of employee assistance programs, repair/rework, staff training, and an insider threat management plan.

2.4.9.2 Analyse risk

Risk analysis is part of stage three of the risk assessment process that allows a greater understanding of the risks (Standards Australia 2009). This is an important stage given the correct analysis and understanding of causes of risks is a highly valuable position providing a sound foundation for successful risk management (Paté-Cornell & Cox 2014). With respect to insider threat the risk analysis stage is a consideration of the causes of insider threat, the consequences of an insider threat attack (e.g. financial

loss, damage to reputation, loss of IP), and how likely a consequence is to occur. It also allows organisations to determine which risks need focusing on.
Bishop et al. (2010) describe there are too many possibilities of insider threat risk and organisations need to find a way to prioritise their focus. Use of risk rankings is one way to achieve this, recognising the potential issues of quantitative and qualitative ranking systems (see Rozell 2015). Managerial review and judgement may also be required in order to make decisions on any data available (Aven 2013).

It is, however, argued that in the case of intentional insider threat, where by definition the offence is undertaken in a veil of secrecy, a full risk analysis may not be possible. Not all intentional insider risks are foreseeable to an organisation and hence difficult to analyse and to fully understand their consequences. Intentional insider threat analysis is a challenging function as many risks are likely to be a low occurrence but with potentially high consequence (Chinchani et al. 2005; Lundberg & Willis 2015). Some industries and sectors face a greater risk level as the victim of insider threat and receive heightened attention, for example, banking and finance, information and telecommunications, energy and transport (Australian Cyber Security Centre 2015; KPMG 2012; Randazzo et al. 2005).

In the literature, insider threat reportedly occurs at a low rate compared to external threats, however, the consequences of an insider threat event can be more deleterious (Schultz 2002). For example the actions by Aldrich Aimes and Robert Hansson (two well-known betrayers of their Government) demonstrate that insider threat actions can have significant consequences, including the loss of lives (Shaw & Sellers 2015).

Risk analysis allows organisations to better understand the controls already in place including their "effectiveness and efficiency" (Standards Australia 2009). Appropriate selection and enforcement of controls can provide protection against insider threat. For example, Bishop et al. (2010) discuss how abuse of computer systems and information can be prevented with properly specified security policies.

Still, there are flaws even when controls, such as security policies, are in place. For example, gaps that exist within or between policies, rigidity of security systems, security practice which can be different to security policy, and the imprecision of detection mechanisms. Further, Flowerday and Tuyikeze (2016) found in their research that poorly thought-out, incomplete, irrelevant and redundant policies are not supported by employees and relevant users. Results of an Australian study found that employee knowledge of policy and procedures influences their attitude. Hence improving employee knowledge, expectations, and understanding is positively related with compliance to policy and procedures (Parsons et al. 2014).

Hunker and Probst (2011) also discuss that policy language needs consideration and should be chosen to match the organisation and its needs. They explain that when it comes to insider threat, best policy should (1) regulate some part of the organisations workflow, and (2) monitor and enforce important aspects of the organisation and the insider threat policy. From a socio-technical perspective policy should set boundaries for behaviour that are permissible and not-permissible. Building effective policies and ensuring these are periodically reviewed, are compliant, and legally upstanding provides organisations one way to prevent misconduct (Ford et al. 2015).

Another outcome of this stage is for organisations to better understand their level of vulnerability to insider threats. Insider threat may be a low likelihood event for some organisations, it appears to be a growing concern especially since the introduction of computers. Trends in social networking, cloud computing, and businesses offering ‘bring your own devices’ (Webb et al. 2014a) as well as the Internet of Things (Nurse et al. 2015) are presenting new avenues for insider threat.

In undertaking this stage a business case can be developed regarding the value of protection against insider threats and whether increasing or decreasing resource input is required. When it comes to insider threat, Shaw and Stock (2011, p. 26) suggest that organisations understand if they are at greater risk due to “remote offices, suppliers, or subcontractors where differences in cultures, policies, or language could lead to potential conflicts”. Clarke and Varma (1999) note that while

greater opportunities are available from engaging with suppliers and customers around the world, it comes with the need for increased risk consideration.

The measurement of risk, as it applies to insider threat, can be difficult. As already discussed insider threats are rare events, that are attempted to be concealed, and not all insider threats can be identified. Still, the importance of considering organisational factors in addressing insider threat is considered one way to increase sophistication of risk measurement (Cho & Lee 2016), assessment (Shaw & Stock 2011) and management. By developing a diagnostic organisational assessment tool, which is the aim of the current study, a broad understanding of controls can be established by organisations. The inventory will allow organisations to easily measure identified organisational vulnerabilities based on literature review and expert opinion. The inventory will not be a measure of the likelihood and consequence of insider threat and associated risks (as this is an organisationally specific undertaking and may have minimal utility under a risk intelligent approach for likelihood). The value of the tool will be in how it is applied through a risk management process where outputs can be tailored to specific organisational needs. Organisations that have not included insider threat as part of their risk management will at least have some level of understanding of their vulnerabilities and strengths when it comes to insider threat through implementation of the organisational vulnerability inventory.

2.4.9.3 Evaluate risk

Risk evaluation as described by the Australian Standards assists decision making by identifying those risks that require treatment and the priority that should be assigned to treat each risk (Standards Australia 2009). Risk evaluation is related to an organisations risk attitude/tolerance (as discussed above) but should also be made with consideration of any "legal, regulatory and other requirements" (Standards Australia 2009, p. 18). The outcome of an evaluation may result in a decision: that a risk is tolerable; that treatment is not required; to maintain existing controls; to improve/implement further controls; and/or to complete further analysis (Standards Australia 2006, 2009). In describing a risk intelligent organisation, Funston and

Wagner (2010) also identify that risks can be exploited, creating value and opportunity for organisations.

Within insider threat consideration also needs to be given to whether proactive mitigation can be viewed as excessive and invasive by employees and inadvertently lead to greater risk (Hunker & Probst 2011). Or alternatively whether inaction and lack of attention could increase insider threat activity (Hunker & Probst 2011; Shaw & Sellers 2015; Shaw & Stock 2011).

2.4.9.4 Treat risk

Rowe (1977) suggested that technology development aided the control of risk but also created new risk. Whilst he was not talking specifically about insider threat he recognised how technology could increase risk to individuals and organisations. He had the foresight to acknowledge the potential for technology misuse and the constraints in our capacity to control such misuse. Rowe (1977) began the discussion and emphasis on the nexus between technology and risk management. Forty years later his sentiments remain relevant and there has been some effort to begin research and more direct focus on controlling technological risk associated with insider threat.

Noting that removal of all forms of insider risk is not possible, organisations must decide on what controls are modified or implemented in order to manage risk (Paté-Cornell & Cox 2014; Standards Australia 2006). The AS/NZ ISO 31000:2009 (Standards Australia 2009, p. 19) describes the treatment of risks as a cyclical process of assessing a risk treatment, deciding on the tolerability of residual risk levels, considering new risk treatments where tolerability is assessed as low, and cycling back to assessing the effectiveness of the new treatment.

Risk treatment options vary and selection of the most appropriate risk treatment will require a cost benefit analysis (Khan & Khan 2014; Standards Australia 2006). As discussed by Lundberg and Willis (2015) an understanding of the expected damages is useful to determine and weigh up against the cost of any risk reduction strategies.

Reducing risk at the lowest possible cost (Fenz et al. 2011) and ensuring countermeasures do not exceed the expected loss of an asset (Fenz et al. 2014) are important, and sometimes overlooked, considerations.

Identifying risk treatment alternatives, challenges in implementation, and the difference each treatment makes is an important step (Paté-Cornell & Cox 2014). Risk treatment options include avoiding the risk, increasing the risk, removing the risk, changing the likelihood and/or consequences of the risk, sharing risk with another party, accepting the risk, or any combination of these (Bojanc & Jerman-Blažič 2013; Homeland Security 2011; Standards Australia 2006, 2009). Identifying the priority of risk treatment options is also an important consideration in this step. So too is the consideration of whether risk treatment itself produces further risk.

Possible insider threat treatments have already been described above when discussing *controls*. In defining the difference between a treatment and control, the HB 167:2006 (Standards Australia 2006, p. 83) described 'treatments' as "controls that are to be introduced" and therefore are the same countermeasures and mitigation strategies previously discussed. These include pre-employment screening, policies and practices, and training and education among others.

Whilst many strategies are available to strengthen insider threat response, Homeland Security (2009, p. 30) report that for various reasons strategies are not "consistently and stringently applied". Further the use of physical, technical, and organisational countermeasures is important (Fenz et al. 2014). Hunker and Probst (2011) declare that the effectiveness of controls and countermeasures in reducing insider threat and insider risks remains unclear. Notwithstanding, evidence in the literature on security management suggests that proactive approaches are more beneficial than reactive approaches (Hunker & Probst 2011). In the insider threat space this would suggest that prevention controls such as employee screening and establishing a robust security culture have longer-term promise over detect and respond controls and punitive approaches. Although the combination of proactive and reactive approaches perhaps provides the best security response (Hunker & Probst 2011).

An output of the risk treatment step is the risk treatment plan. Rowe (1977) discusses through planning and implementation of controls, systemic control of risk can be achieved. According to the Standards Australia (2009, p. 20) a risk treatment plan involves describing the treatment options and reasons for selection, who is responsible and accountable for the plan, proposed actions, resource requirements, performance measures and constraints, reporting and monitoring requirements, and timing and schedule.

2.4.10 Monitor and review

Regular review is an important part of the risk management process and is used to determine the effectiveness of controls, improve risk assessment, learn from experience, detect changes in contexts, and identify emerging risks (Standards Australia 2009). As Shaw and Stock (2011) report, insider threat can escalate when a lapse in compliance results from a lack of on-going monitoring and enforcement. In order to move away from reactive and conformance based risk management, performance based organisations will become increasingly more agile and learn from security breaches, look to improve on performance and prevent future security incidents. The implementation of active testing of assumptions and systems is a key principle for effective risk management (Paté-Cornell & Cox 2014). This is consistent with a risk intelligent approach to risk management and the development of greater risk leadership.

The insider threat landscape is undergoing change. Sarkar (2010) encourages on-going monitoring and review due to the dynamic attributes of insider threat and threat agents. As already described the introduction of technology and the internet has had a great effect on the type and amount of insider threat activity. As such monitoring and review practices need to be on-going. Within security risk management there are four levels of monitoring practice including continuous monitoring, line management reviews (periodic), centralised reviews (audits), and scanning (reviewing the environment for changing or emerging risk; Standards Australia 2006).

Standards Australia (2006) suggests a number of triggers for the review of security risk and these can be adapted and applied to reviewing insider threat risk also. Such triggers include: organisational restructures, change in management, mergers or acquisitions; significant changes to organisational premises; changes to critical assets; changes in the local security environment; changes to national security threat levels; changes in vendors/suppliers, changes in technology; increased security risks identified by other similar industries/sectors/markets; and development of significant new intellectual property. The execution of the organisational vulnerability inventory (an outcome of the current study) during the monitoring and reviewing stage may provide benefit. Given there will be initial baseline of responses any future reapplication of the inventory will allow organisations to understand positive and negative change in organisational vulnerability.

2.5 The Future of Insider Threat Risk Management

The International Standards for Risk Management have proven to be useful tools in addressing risk in many organisational settings. Certainly there is promise in underpinning an insider threat inventory with the International Standards. As it currently stands many public and private organisations refer to, and perhaps rely upon these standards in their approach to risk management. Further, the Australian Government has mandated public departments, and recommended private enterprises, to develop an approach to manage insider threat that is consistent with these guidelines. As such the ISO remains a relevant consideration.

However, there has been some criticism about the utility of the standards generally and specifically with regard to insider threat. For example, insider behaviour is not well explained by traditional methods of risk analysis (Farahmand & Spafford 2013). Reliance upon traditional corporate risk processes is no longer viewed as supporting business decision making and other management functions (Leitch 2017). Further new forms of risk, including cyber risk, will require the evolvement of current risk functions (Harle et al. 2016).

Organisations will continue to be challenged by the ever changing risk of insider threat. As previously discussed, there is growing recognition that not all insider threats can be identified or forecasted and therefore the mitigation of all risk is an unrealistic expectation. Further, it is acknowledged, at least with respect to cyber threats, that such threats are dynamic, evolving, and adapting (Borum et al. 2015).

Concurrently, in risk management there is growing acceptance that in the absence of being able to recognise all risks, a risk leadership or risk intelligent approach shows promise. Organisations that are best able to consider how risk elements relevant to insider threat interact, obtain more diverse and foresightful results. Even more so, organisations are judged on how well they respond to unexpected crises and this include insider threats. Insider threat is not commonly referred to as a crisis; however, it often requires a response akin to a crisis. What will benefit organisations will be a move from, an old paradigm of risk management to a new paradigm of risk leadership and intelligence and integration of current international standards. In fact, some in the risk field suggest that risk management over the coming decade will see more transformation and change than seen in the previous decade (Harle et al. 2016).

In order to be able to identify unexpected risk, such as that with insider threat, a close look at Futures Studies seems appropriate as a framework for informing a more proactive and realistic approach to IIT mitigation. The use of foresight theory can add value moving an organisation beyond its ability to identify short-term risk and implement capabilities of creativity and innovation to identify unexpected and emerging risk. Traditional risk management will pave the way for risk leadership and intelligence, where a close focus on risk appetite, strategic direction and disruption will be key factors of success.

2.5.1 What is Futures Studies and Foresight?

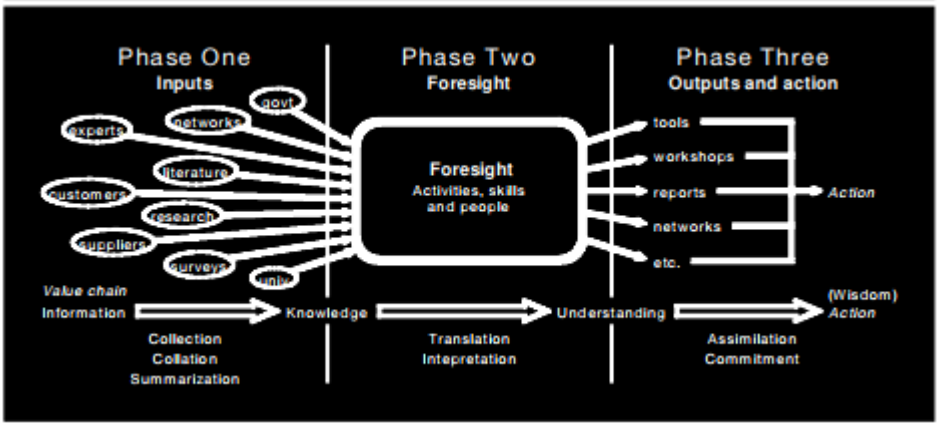
van der Laan (2008, p. 25) discussed that “[t]he future is not linear but is the result of possible trajectories that are formed in the past and the present”. In risk management it is these possible trajectories that are of keen interest. Being able to mitigate against future threats by applying what we currently know and fathom,

underpins many organisational risk processes. However, as has already been posited, in the field of insider treat there are many 'unknowns' which create an environment of instability and uncertainty. It is in this ambiguous and ever-changing environment that Futures Studies can pave a path forward providing insight and foresight to what may be.

Futures Studies allow organisations to understand change and the complexity of their environment, through the use of a foresight process, resulting in an appreciation of possible, probable and preferable futures (van der Laan 2008; van der Laan 2014; van der Laan 2010). As defined by Horton (1999, p. 5), "[f]oresight is the process of developing a range of views of possible ways in which the future could develop, and understanding these sufficiently well to be able to decide what decisions can be taken today to create the best possible tomorrow". Foresight processes therefore offer organisations the opportunity to create and prepare for future scenarios by exploring alternatives and possible futures (van der Laan & Yap 2015).

According to Horton (1999), in practice there are three phases of a successful foresight process (see Figure 8). The first phase involves the collection, collation, and summarisation of foresight knowledge. The second phase requires the translation and interpretation of foresight knowledge. The third results in the assimilation and commitment to the future.

Figure 8: A Successful Foresight Process



Source: Horton (1999, p. 6).

2.5.2 Applying Foresight to Insider Threat

2.5.2.1 Insider threat - the present

According to Horton (1999) the first phase of the foresight process requires the collection, collation, and summarisation of available sources of data. Information is gathered through various means including research, surveys, literature, government, and networks. This results in foresight knowledge which is then presented in manageable form (van der Laan 2008). The current research successfully contributes to this narrative by addressing the first phase of the foresight process. The gathering of relevant source material and presentation of the current state of insider threat provides a sound basis for greater understanding of the future of insider threat.

In summary there are a number of important factors which have influenced the narrative on insider threat and will continue to affect the future of insider threat study and activity. These include:

1. Insider threat is an ongoing concern for public and private enterprise;
2. The Australian Government has instigated measures to attempt to reduce insider threat and associated vulnerabilities, including the mandating of Government Departments to apply risk management methodology to address the issue;
3. Many definitions of insider threat exist and tend to distinguish between intentional and unintentional insider behaviour;
4. There are several frameworks and models that describe insider threat;
5. Research and response to insider threat is becoming increasingly multi-disciplinary in approach;
6. Vulnerabilities within organisations continue to be leveraged by means of variety of insider attack vectors;
7. Individual, Technical, and Organisational countermeasures are important;
8. There are significant limitations to the current research on insider threat; and
9. Approach to risk management is evolving and our approach to insider threat should also.

These summary points are a simplistic overview of the current knowledge of insider threat and are well attended to in the preceding chapters. The points serve as a broad reminder of the available information providing context to the possible futures of insider threat as discussed below.

2.5.2.2 Insider threat – the future

The available literature on insider threat has discussed the possible future of the field. A search for specific articles applying futures studies, and foresight processes, along with Insider Threat yielded no results. To the author's knowledge, recommendations and possible futures and recommendations within the available information sources have not been specifically based on an exercise in future studies or foresightedness as per the foresight process (Figure 8), however, there have been attempts to discuss what the future might hold (Cappelli et al. 2006; Gelles 2016; Nurse et al. 2014b; Sarkar 2010). These expert opinions and research outcomes offer a view of the possible, and perhaps probable, future of the insider threat.

One of the more obvious and most published outcomes is that insider threats will continue to be cause for concern in the future (Agrafiotis et al. 2015; Cappelli et al. 2012; Gelles 2016; Probst et al. 2010a). This concern may be amplified by the growing freedoms afforded to insiders such as the increasingly flexible work arrangements and options such as bring your own device (BYOD). The rate at which technology changes and affects how people work remains a challenge for the management of insider threat. As such, experts in the field of risk management and insider threat management are likely to find it difficult to keep up with the evolving technological landscape. The increasing technical knowledge of insiders, through general use and education, is likely to result in an increasing sophistication of cyber related insider threats. Positively, technological advancement will help to reduce risk through mechanisms such as data analytics and machine learning. However, these are likely to be informed by forecasts and patterns of change in the past and are unlikely to detect possible system breaks that have no precedence.

In future, the technology generation will hold the majority of employment positions and eventually, power. The power holder's attitude and practices to technology will filter through and change policy and process. There is much discussion on the ease with which younger generations provide information online. This will continue to create challenges for organisations as they attempt to balance security (and reduce vulnerability) with increasing employee demands such as BYOD, working away from the office, and flexible work arrangements (Borrett et al. 2013).

The most intelligent organisations of the future will gain advantage by their ability to create a seamless connection between technology-enabled insights, understanding of human decision making (Schoemaker 2015), and the development of foresight contribution. The future of insider threat management is likely to see organisations work more collaboratively internally and with external stakeholders. There will be a rise in strategic and senior level influence (Borum et al. 2015) and more organisations will have a Board member dedicated to security, including insider threat issues.

There is an increasing expectation that organisational leaders will be more responsible for security (Borrett et al. 2013). Training organisational leaders in risk management decision capabilities is considered to offer sound risk mitigation (Eastburn & Sharland 2017). From a general leadership perspective, initial investigations by van der Laan (2008) reveal that in an environment of uncertainty leadership competencies in futures thinking are connected to organisational performance. Therefore, enhancing the competence of organisational leaders, by including foresight education in professional development, may contribute successful countermeasure against insider threat.

The increasing regulation and implementation of strategies to reduce insider threat will continue. The Australian Government, since 2000, has required more of its public departments to engage in threat reporting. It has also required more of its employees, especially those working in sensitive areas, to go through vetting and psychological assessment. It is likely that a stronger focus on improving compliance will result in benchmarking initiatives. Harle et al. (2016) suggest that, within the

banking sector, the enhancement of risk culture will be critical to the success of its risk functions. This is considered a desirable outcome for organisations and broader sectors looking to reduce their insider threat vulnerability. Enhancing organisational culture, assessing security culture, and implementing strategies to promote cultural enhancements will blossom if this approach is followed.

There is already an increasing interest and expectation from the public around privacy and information sharing (Pulver & Medina 2018). There will be a growing expectation from the public that organisations are giving due attention to their privacy and the use of personal data. Within organisations the increasing acceptance of a multidisciplinary approach to insider threat will allow for greater cross-departmental collaboration. Working together, security teams along with Human Resources and Legal departments can ensure that employee privacy is not infringed upon, that ethical action is promoted, and that whistle-blower protection is afforded. The growing body of literature on insider threat does elucidate a growing focus on cyber and IT threat vectors and countermeasures. This appears to create a future vulnerability as organisations experience tunnel vision, focused solely on technical threats, and losing sight of more "traditional" insider threats. Perhaps mundane when compared to the rapidly evolving and ever-changing technological threat, historical insider threat activity (espionage) through placement of 'moles' and 'spies' could see resurgence.

Finally, there has been little discussion in the insider threat literature regarding how insider threat opportunities may be more positively integrated in the risk management process. Within the fields of risk management, risk leadership, and risk intelligence there is an expectation that vulnerabilities can be exploited to the benefit of organisations. Further research and expert commentary on how this may be achieved is an exciting avenue of future study. Where vulnerability lies, opportunity exists.

2.6 The Organisational Vulnerability to Intentional Insider Threat Inventory (OVIT)

The purpose of the current study is from an academic and applied perspective and is two-fold: develop an inventory which helps organisations diagnose their vulnerability to intentional insider threat; and, positively contribute to the growing narrative on insider threat. It is commonly recognised that intentional insider threats are difficult to detect and that all insider risks cannot be discovered. However, this should not be a deterrent to improving our understanding of insider threats nor to implementing ever-improving strategies to try to reduce vulnerability to such threats. Organisations require tangible, reliable, and valid means in order to better protect themselves. A benchmark and baseline opportunity to determine current vulnerability and assess future progress can be achieved. An organisational vulnerability inventory is one that is derived from the literature, incorporates expert opinion, is able to measure vulnerability in an efficient, reliable and valid way, and contributes to growing understanding of insider threat is the outcome of the current research. Given this intention, the current section will explain how the OVIT is underpinned by the research, addresses frameworks and models relevant to insider threat, and provides future benefit to the field both in theoretical and practical sense.

2.6.1 Redefining insider threat

In the absence of an Australian definition of insider threat, the current research is underpinned by the commonly referenced definition of the CERT program at Carnegie Mellon University (CMU).

> A "current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organisation's information or information systems" (Cappelli et al. 2012, p. xx).

Building on this the current research determines a relevant and comprehensive definition of intentional insider threat from Australian experts. This is an important contribution to the existing research of insider threat. Gelles and Mitchell (2015) state, a critical first step in formulating an insider threat program requires a specific internal working definition of insider threat. In the current study the development of an Australian definition also helps to determine the scope and parameters of the development of the OVIT. The opportunity to provide a working definition, based on the Australian context and developed by Australian experts, is a unique contribution of the current study and will be posited in the discussion of results (see Chapter 4, Section 4.3.1).

2.6.1.1 Intentional versus unintentional insider threat

As already discussed in Section 2.1.3, the current thesis focuses on *intentional* insider threat, where a person is motivated and acts to deliberately cause harm to an organisation. This particular emphasis on intentional insider threat has delimited the research. However, the organisational vulnerability inventory that is developed provides invaluable understanding of the vulnerability to all forms of insider threat and more broadly to general counterproductive workplace behaviours. This is due to the strong overlap in the etiology of all forms of intentional and unintentional counterproductive behaviour in the workplace. The absence of countermeasures and protective strategies in an organisation results in vulnerability to various forms of counterproductive behaviour. By identifying areas of organisational vulnerability related to intentional insider threat there is greater opportunity to develop appropriate interventions and countermeasures for both intentional and unintentional insider threats.

2.6.2 A Holistic Conceptual Model of Insider Threat

Given the current status of research on insider threat there is potential to expand our understanding of the insider threat phenomenon. There is a growing recognition of the multi-factorial contribution to insider threat. Organisations, and experts in security, risk management and insider threat, are moving towards a more holistic appreciation of the threat. Understanding that the intersection of vulnerability across

individual, organisational, and technical factors is the point of greatest risk can be conceptualised and visually presented (see Figure 9). Given that insider threat involves multifactorial risk indicators, and is a multidisciplinary concern, it requires a holistic approach for effective identification and countermeasure. This is the purpose of the OVIT; to provide a diagnostic inventory that addresses the individual, organisational, and technical risk areas and determines potential vulnerability of an organisation to intentional insider threat.

Figure 9: A conceptual model of insider threat

Source: Developed for this study.

As Gelles (2016) indicates developing an insider threat program requires the conduct of an organisational assessment. The outcome of this thesis is an inventory intended to improve the capacity of organisations to diagnose organisational vulnerability to intentional insider threat. The study is also based on the conceptual model represented in Figure 9. The findings of the study will further serve to validate or adapt the model. Through a collaborative effort, this tool can help organisations assess potential organisational vulnerabilities and strengths related to individual, organisational, and technical factors.

It is recognised that whilst intentional insider threat is perhaps a rare event, the outcomes are potentially catastrophic. The negative effects expand beyond the event itself and can have significant repercussions within the assaulted organisation. A

multidisciplinary approach is required that includes a thorough investigation of organisational vulnerabilities and protective factors, where no immunity exists, to provide the best response. Whilst the resulting inventory does not offer specific risk management advice it provides guidance towards relevant interventions, protective actions, treatments and controls, to manage and reduce the risk of intentional insider threat.

2.6.3 Application of the OVIT across current models and frameworks of insider threat

The effort required to better understand organisational vulnerabilities to intentional insider threat is well worth the investment. Through this thesis, outcomes can contribute to the growing advancement in threat assessment and specifically in the insider threat space. The OVIT can provide a systematic means for assessment and understanding of relevant insider threat vulnerabilities (as well as mitigation strategies). The OVIT is theoretically and empirically derived and is able to complement insider threat frameworks and tools so that organisations can be proactive in insider threat assessment and management. The OVIT itself is not married to one specific model or framework. Rather it allows for the implementation of the inventory across organisations with different methods and models for addressing the insider threat.

2.6.4 OVIT and risk management

The continual exploration and discussion of insider threat, including its causes and controls, is important for effective risk management. This study is underpinned with the ISO 31000:2009 and therefore the OVIT is aligned with this generic risk management methodology. Focusing on the generic approach to risk management as per the ISO 31000:2009 allows the OVIT to be applied to a broad range of organisational risk management methodologies (Fenz et al. 2014) and expands its utility and applicability to all organisations. Moreover, the alignment of the OVIT with the ISO 31000:2009 and Australian Standards HB 167:2006 Security Risk Management ensures that it is an appropriate tool to implement within Government

departments. The OVIT adheres to the Australian Government mandate that public departments "adopt a risk management approach to cover all areas of protective security activity across their organisation, in accordance with the Australian Standard for Risk Management AS/NZS ISO 31000:2009 and the Australian Standards HB 167:2006 Security Risk Management".

The OVIT contributes to an organisation's risk management framework, risk assessment, and risk management plan by addressing one area of risk, which is the intentional insider threat. This is consistent with the AS/NZ ISO 31000:2009 Standards Australia (2009, p. iv) which states that "risk management can be applied … to specific functions, projects, and activities". The OVIT therefore helps reduce an organisation's risk by anticipating, understanding, and deciding whether to act on potential insider threats; with the ultimate aim to protect vital assets and/or critical information.

2.6.5 The OVIT addresses limitations in insider threat

Insider threat is a complex and difficult area of study. Certainly there has been concern that it is flawed by bias, government funding, and lack of attention to all organisational forms. Further, the majority of research on insider threat appears to be generated by the USA and the UK. The current research is the first Australian based research focusing on establishing an inventory to address intentional insider threat that includes individual, technical, and organisational components.

Current research has its limitations due to being speculative, case driven, and lacking in predictive ability. The retrospective nature of investigation has raised concern about the applicability of research outcomes. Whilst the current research project is not able to provide predictive ability, the implementation of the OVIT can result in a baseline from which future incidents can be measured. The continued use of the OVIT, allows a temporal overview of change in an organisation (and more broadly across industry). Should there be an insider threat incident, revisiting the information obtained from the inventory may provide invaluable information and greater understanding of the potential to develop a range of possible insider threat changes.

The caution around legal, ethical, and privacy concerns related to the application of insider threat countermeasures is not specifically addressed by the OVIT. However, when completed by organisational members, with an understanding of organisational processes and positioning, the inventory can identify a baseline of vulnerability. The results present organisational level vulnerability and do not target specific individuals. The OVIT can demonstrate to organisations where vulnerabilities may exist and therefore provide real-time feedback on how organisations can address deficiencies in intentional insider threat risk management.

2.6.6 The OVIT and futures studies

Employing a futures perspective is an essential component of the current study. The use of foresight theory enhances this research by providing creative and innovative approaches to identify unexpected and emerging risks. Futures studies is necessarily associated with a meaningful study of IIT as it posits that multiple possible futures exist and that an awareness of these multiple alternate futures, rather than predicting 'a future', is what differentiates its utility from traditional risk management approaches.

The development of the OVIT has required a thorough investigation of the existing research and understanding of the extant literature. Consistent with Future Studies the collection, collation, and summarisation of literature is a direct contribution to stage one of a successful foresight process (Horton 1999; van der Laan 2008). Aside from the review of available literature, foresight knowledge may also be attained via other methodologies. As Horton (1999) stated, the employment of Delphi surveys is another mode of input to the foresight process. In the current study the Delphi technique is implemented, providing an avenue for Australian experts to provide input to the OVIT and also to contribute to the growing knowledge base on insider threat and how it may evolve into the future.

Finally, the OVIT itself, when deployed in an organisation will provide direct and organisationally specific contribution to foresight knowledge as part of Horton's Phase 1 (inputs) and Phase 2 (foresight interpretation). The use of the OVIT can

provide organisations real-time understanding of the scope of their vulnerability to intentional insider threat. It also delivers a means of collecting and collating a large volume of information so that it is presented in a manageable form.

Horton (1999) encouraged organisations to carry out (or at least manage) stage one of the foresight process. Horton (1999, p. 7) suggested that doing so creates "some sense of ownership and credibility of the resulting knowledge". She also acknowledged that third parties are useful contributors to phase one, helping organisations unfamiliar with the subject matter (in this case intentional insider threat) and/or preventing narrow sightedness. The OVIT demonstrates its utility in providing a means of evaluating organisational vulnerability to intentional insider threat regardless of the organisation's (or staff) expertise in the area or any bias in assumptions (such as the insider threat only being of technical concern).

2.7 Summary - Research Questions

This chapter provided an overview of the current status of insider threat research, a comprehensive discussion of the available extant literature on insider threat, as well as the related discipline of risk management and their limitations. In reviewing the core concepts of insider threat a conceptualised approach to the assessment of vulnerability, with a multidisciplinary overview, emerged. Australian Government's approach to insider threat, existing risk management standards, models and frameworks of insider threat, and the future of both insider threat and emergence of new paradigms of risk intelligence, have guided the approach to the development of the OVIT.

There are two main aims of the current study. The first is to develop a diagnostic inventory to assess organisational vulnerability to intentional insider threat and, secondly, based on these findings present a preliminary model of organisational vulnerability to intentional insider threat with both practical and academic utility. In order to address these aims the research proposes three research questions. Chapter 3 discusses the research design, methodology, research questions and proposed analysis of the data.

3 Research Design and Methodology

3.1 Introduction

The previous chapter provided the foundational knowledge on insider threat and the risk management required to advance a conceptual framework for the development of an Organisational Vulnerability to Intentional Insider Threat inventory (OVIT). This chapter describes the research design and methodology of the study. The purpose of this chapter is to demonstrate the theoretical underpinnings that inform the research design and to provide an overview of the relevant stages of enquiry and the systematic research process of the research methodology.

3.2 The Research Questions

The previous chapter provides a comprehensive review of the literature on insider threat and risk management as it relates to the study of insider threat. The aim of the literature review is to provide a summary of existing knowledge of a subject of interest which supports the identification of specific research questions through identifying and organising the relevant concepts (Rowley & Slack 2004). The literature review demonstrates that insider threat is a multidisciplinary concern but is oftentimes studied and managed with a singular focus (predominantly technological). More recent literature encourages both an academic and applied shift in support of collaboration and refocuses on individual, organisational, and technical means for prevention, detection, deterrence, and management. While there is an increasing interest in the study of insider threat, there remain limitations and clear gaps in the available literature that relate to its specificity, poor generalisability, lack of controlled studies, and limited access to insider threat data. There is scarce contribution to the field from an Australian perspective. There is also no clear valid and reliable assessment tool that comprehensively addresses the multifactorial nature of the insider threat problem for organisations.

The Australian Government mandates that public departments address insider threat in accordance with the ISO31000:2009 risk management methodology (Protective

Security Policy Section Attorney-General's Department 2010). This directive creates an opportunity for empirical and applied studies to better assess current organisational vulnerability to intentional insider threat, as well as set a baseline of organisational functioning and positioning that can be compared across organisations (and even across industries/sectors).

A simple conceptual model to understand the insider threat from a multidimensional view has been presented (see Figure 9). This simplified view of the insider threat provides a framework to empirically derive a valid and reliable assessment of organisational vulnerability to intentional insider threat. Therefore the general aim of this research is to develop an inventory that can be employed regardless of the many different insider threat models and frameworks, as well as the uptake of different risk management methodologies within organisations.

The state of the current literature on insider threat underpins the questions which aim to address the identified limitations and development of an inventory to assess organisational vulnerability to intentional insider threat.

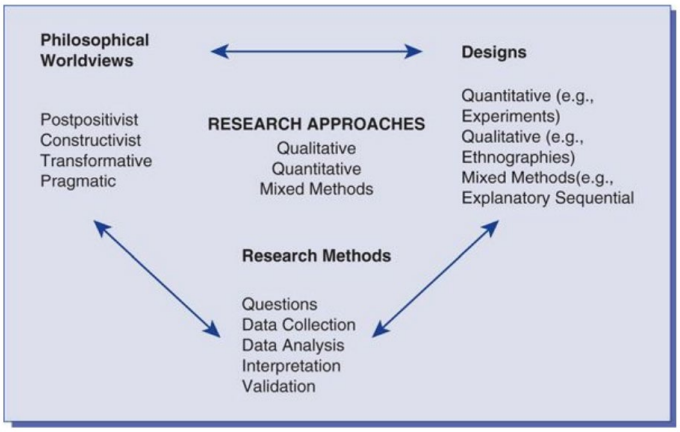
Research Question 1: *What are the main organisational influences on intentional insider threat (IIT) based on available literature?*
Research Question 2: *What are the main organisational influences on IIT based on expert opinion?*
Research Question 3: *How is organisational vulnerability to IIT operationalised by the study?*

3.3 The Research Design and Strategy of Enquiry

When undertaking research, Creswell (2014) encourages the researchers to make explicit the framework for the research which includes their worldview. In doing so, the researchers are better able to explain their approach to the research, the research design, and research methods (see Figure 10). This section explains the philosophical worldview that underpins the research, the research design, the

research approach, and research methods as they apply to the development of the OVIT.

Figure 10: A Framework for research



Source: Creswell (2014, p. 35)

3.3.1 Research design

In order for the research to achieve its goals it is important to identify the most suitable research design, strategy for enquiry, as well as tools and techniques (Romeu 2006). Providing justification of the research design and investigative strategy is an important component to demonstrate the approach to meeting the aims and objectives of the research as well as the research questions.

It is important to note that the current research is designed in three phases. The first phase answers Research Question 1, which is a review of the literature and extraction of the main influences of intentional insider threat. This information is then used to inform the second phase of the research design, the Delphi Study, aimed at addressing Research Question 2; the main influences of intentional insider threat as agreed by Australian experts. The research design then progresses to the third phase which addresses Research Question 3, the development and validation of the OVIT and a working conceptual model of organisational vulnerability to IIT.

3.3.2 Research Paradigm

Creswell (2014) encourages researchers to make explicit the worldview - that is the epistemology, ontology, and methodology - proposed by any study. According to Creswell (2014) there are four widely discussed worldviews in the literature. These include: post-positivism, constructivism, transformative, and pragmatism. The researcher's choice of worldview is often influenced by the discipline of study, previous research experiences, and, in the case of students, the influence of supervisors (Creswell 2014).

In determining an appropriate research paradigm to underpin the current project, both the post-positivist and pragmatist knowledge claims were considered. According to Creswell (2014) postpositivism represents the more traditional form of undertaking scientific research. As such it suits quantitative methods of enquiry in which the researcher aims to explore cause and effect relationships. In contrast to the post-positivist worldview which focuses on antecedent conditions and therefore an empirical response, the pragmatic paradigm considers actions, situations, and consequences and employs pluralistic methods which can offer best solutions and application to a particular problem (Creswell 2014).

The pragmatic paradigm was chosen for the current research as it does not have a focus on antecedent conditions and "is not committed to any one system of philosophy or reality"(2009, p. 4). Instead it focuses on knowledge claims being a result of action orientation and consequences in order to find solutions (Creswell 2009). It further provides for the inclusion of both qualitative and quantitative methods and as such captures both elements of the constructivist and post-positivists approaches.

Utilising a pragmatic approach requires that the research problem itself is held central and that data collection and analysis techniques are chosen based on their ability to provide insight to the research question (Mackenzie & Knipe 2006). By determining the research problem as the most important factor, any approach to understanding the problem may be introduced. Rowe (1977) discusses that any

methodology is proven by its pragmatic acceptance, ability to solve real problems, and adaptability to application.

It is acknowledged within the pragmatist paradigm that there is not one absolute truth (Creswell 2009) and therefore reality can and does change. Pragmatic approaches help facilitate human problem-solving and deal with problems as they arise (Powell 2001). As Pansiri (2005, p. 197) explains "pragmatists refute the idea that 'truth' can be determined once and for all". Given this, pragmatists are not committed to one research paradigm, system, or reality (Mackenzie & Knipe 2006). Instead, pragmatists favour methods that provide the most benefit and insight.

The pragmatic paradigm underpins the current research as it aims to provide solutions to real-world problems without the influence of a specific worldview and underlying paradigm assumptions. In choosing the pragmatic paradigm there is an acceptance of the use of mixed methods design. In fact, Creswell (2014) promotes mixed method design and encourages researchers to draw liberally from qualitative and quantitative assumptions.

3.3.3 Quantitative, qualitative, and mixed methods research approaches

Creswell (2011) identifies the importance of the research approach in determining the most relevant procedure for the collection, analysis, and interpretation of data. Further, a clear template and justification of the data collection method provides a means of establishing reliability (Hair et al. 2010). Within the pragmatic framework, mixed methods approaches are considered appropriate, if not necessary. However, Creswell (2014) cautions that in choosing a mixed method approach, providing the reasons why quantitative and qualitative data are being mixed remains important.

3.3.3.1 Qualitative research

Qualitative research aims to provide construction of social reality and meaning and is underpinned by the constructivist worldview as discussed by Creswell (2014). The purpose of qualitative research is to explore and describe complex phenomena through designs that seek to gain a deeper understanding of a phenomenon (Creswell

2014). Qualitative research can develop deeper meaning through content based analyses and interpretation (Creswell 2009). In contrast to quantitative research, qualitative approaches tend toward small samples sizes that are targeted and chosen for purpose. Given this, limitation of small sample size makes it difficult to validate and generalise the findings.

3.3.3.2 Quantitative research

Creswell (2014) suggests that the identification of inherent relationships between variables is most appropriately studied with quantitative methods. Quantitative approaches are aligned with post-positivist knowledge paradigms as they attempt to explain and describe relationships between variables (Creswell 2009, 2014). The use of experimental or survey methods are common strategies of enquiry that rely on statistical analysis (Creswell 2014). In quantitative research, samples are selected to represent a greater population through large sample sizes and random selection processes. The primary aim of quantitative research in social sciences is to be able to predict human behaviour.

3.3.3.3 The current study – mixed methods

The objectives of both qualitative and quantitative approaches satisfy the aims of the current study and have ability to contribute valuable insight to intentional insider threat. However, it seems that the strength is in combining the two approaches as part of a mixed method design. Here the limitations of one approach are minimised by the strength in the alternative approach. As such a mixed method design is able to provide the best response to the research problem; contributing depth, and unique insight, to the underrepresented aspects of insider threat whilst also providing an empirical basis for the resultant OVIT. This rationale is consistent with the teachings of Creswell (2014) that mixed methods are gaining in popularity as a way to understand research problems by contributing to the depth of meaning as well as providing an empirical basis for any claims.

A number of typologies of mixed methods research designs have been developed and inform data collections procedures (Hanson et al. 2005). Based on four decision

criteria – implementation, priority, integration, and theoretical perspective - Creswell et al. (2003) determined a typology for classifying mixed method research designs. The authors specified six types of mixed method designs; three sequential and three concurrent designs (a full overview of the typology for classifying mixed method research designs is outside the scope of the current thesis, however, further information can be found in Creswell et al. 2003 and Tashakkori & Teddlie 2003).

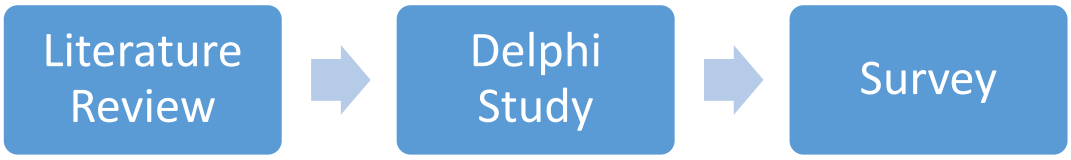
Following the decision criteria provided by Creswell et al. (2003) the current research fits a sequential mixed method research design, specifically the sequential exploratory design. In the sequential exploratory design both qualitative and quantitative data are collected and analysed (Creswell et al. 2003; Hanson et al. 2005). This option does not use an explicit advocacy lens (Hanson et al. 2005), allows for the collection of qualitative and quantitative data, is used to develop instruments, and may utilise surveys and factor analysis (Creswell et al. 2003, see Tashakkori & Teddlie 2003 for further discussion on mixed method typologies).

Under the pragmatic paradigm the research approach should relate to the purpose of the study and be equipped to answer the research questions. The aim of this study is to understand the influences on organisational vulnerability to intentional insider threat and use these insights to develop an inventory that can measure the strengths and limitations of an organisation as it relates to the individual, organisational, and technical factors associated with insider threat. In the current research, content analysis of the extant literature, the Delphi method, and surveys are the chosen methods of enquiry (Armsby 2000).

3.4 Phases of research

In addressing the research aims and questions an exploratory sequential design is considered appropriate. For the current research this began with content analysis of the extant literature, before progressing to the Delphi method, and finally survey development and validation.

Figure 11: Phases of Research



Source: Developed for this study.

3.4.1 Phase One - The literature review

A literature review is defined as "the selection of available documents (both published and unpublished) on the topic, which contains information, ideas, data and evidence written from a particular standpoint to fulfil certain aims or express certain views on the nature of the topic and how it is to be investigated, and the effective evaluation of these documents in relation to the research being proposed" (Hart 1998, p. 13). The aim of the literature review, as it relates to the current study, is to identify and organise the concepts associated with intentional insider threat (Rowley & Slack 2004). Identifying, organising, and distilling the concepts, theories, and empirical support in the literature can help identify any limitations as well as point to specific research questions (Rowley & Slack 2004).

The current research commenced with a comprehensive review of the literature on insider threat. Consistent with the recommendations of Creswell (2014) a priority for selecting literature began with a broad synthesis of the literature, followed by more targeted review of journal articles, appraisal of relevant books, an exploration for recent conference papers, and a search for web-based materials.

The existing literature on relevant key word searches (including but not limited to "insider threat" and "insider risk") resulted in a range of academic articles, books, research projects, whitepapers, conference proceedings, journal articles, and government documents relevant to the topic area.

3.4.1.1 Phase One – Data capture and analysis

Phase one of the data collection addressed RQ1 (What are the main organisational influences on Intentional Insider Threat (IIT) based on available literature?) and was a thematic analysis of the literature that is already available on insider threat. The purpose of the literature review is to determine the pertinent factors and dimensions related to the relationship between organisational vulnerability and IIT which can then be further validated by the Delphi process.

As previously mentioned, the literature review presented an opportunity to qualitatively analyse available publications to determine the main influences on organisational vulnerability to intentional insider threat. As Elo and Kyngäs (2008) discuss, content analysis can allow for concepts to be derived from the available data and is especially useful in research where there is limited contribution to the topic under investigation – such as the study of insider threat.

Each article was reviewed for potential variables related to intentional insider threat from strength or vulnerability based perspective. These variables were extracted from the literature and recorded on a spread sheet. Any potential influences on intentional insider threat were recorded in Phase One.

The variables were grouped according to the main aims of the current research resulting in the following categories: (1) words related to the definition of intentional insider threat; (2) variables considered to increase intentional insider threat; (3) variables considered to decrease insider threat; and finally, (4) organisational conditions that may moderate or mitigate IIT. The outcomes of the literature review and content analysis were then used in the initial development of the Delphi Study.
Based on the literature review, a basic conceptual framework to understand and further explore intentional insider threat was developed (see Figure 9). Consistent with the conceptual model, the variables ascertained from the literature were presented under each concept category (individual, organisational, and technical) throughout the Delphi study.

3.4.2 Phase Two - The Delphi study

The Delphi method philosophically underpins the paradigm of pragmatism (Brady 2015). Given the emphasis on pragmatic worldview, the Delphi method is favoured in this pragmatic research. The Delphi method has the ability to contribute to and inform real-world problems especially those which relate to intentional insider threat. According to Brady (2015) the Delphi method is underpinned by the pragmatic paradigm in the following ways: it is flexible and able to utilise qualitative and quantitative forms of data enquiry; it is affordable and can be conveniently and efficiently distributed via email; it is able to eliminate response bias; it does not require generalisability, it rather focuses on participants with specific expertise; and, can be employed across a diverse range of industry and practical applications as it does not require specialised education.

The original Delphi method was introduced in the research conducted in 1950s by the RAND Corporation (Von der Gracht 2012). It involved a structured survey presented to a panel of seven specialists to reach consensus on the topic of bombing requirements. According to Dalkey and Helmer (1963) in the first Delphi method, the technique involved a series of questionnaires and interviews, interspersed with controlled feedback, in order to obtain a reliable consensus of opinion. The structure of the Delphi method resulted in both qualitative and quantitative outcomes.

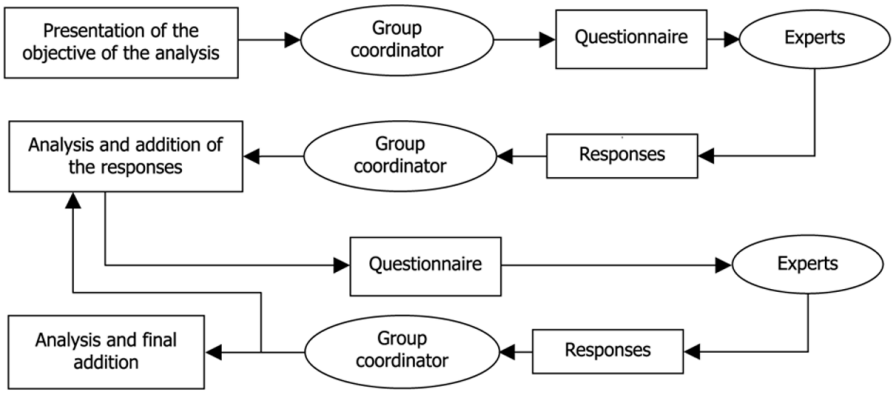
Since the introduction of the Delphi method it has been modified in subsequent research studies. Given these changes, researchers refer to the *Classical* Delphi method and the *Modified* Delphi method to distinguish those that are more consistent with the original reference of study. Some of the more obvious changes include the deletion of the interview component, the varied ways of beginning the survey from open-ended question/s through pre-determined and constructed items, as well as the increasing uptake of modern technology (including email and online survey tools).

Skulmoski et al. (2007) report that the Delphi method is an attractive tool for graduate students as it is a flexible research technique that is suited to addressing

problems or phenomenon where limited information exists. It is a versatile method for exploratory study (Okoli & Pawlowski 2004), and, as is the case with insider threat, where the topic is delicate, sensitive or undocumented (Lilja et al. 2011a).

A Delphi study is an iterative process (see Figure 12) which endeavours to gather opinions from subject matter experts whilst attempting to discover new insight and gain consensus. As a research technique, the Delphi method has been employed in a significant number of published works and addresses numerous research topics in varied fields of interest.

Figure 12: The Delphi Processes



Source: Adapted from Landeta (1999).

A modified Delphi method was chosen to complement the mixed methodology approach and pragmatic paradigm that underpins the current research. The modified Delphi method was deemed appropriate to address RQ2 (What are the main organisational influences on IIT based on expert opinion?) and was chosen as a suitable means of gathering expert opinion through a multi-stage email survey.

Given insider threats are statistically rare (Shaw & Fischer 2005), or more likely seldom reported, then quantitative methods alone do not provide a full picture of this threat. As such this research utilises both quantitative and qualitative methods of enquiry during the modified Delphi process. The inclusion of qualitative methods, through information provided by subject matter experts, was considered an effective

way to gather relevant and purposeful information on insider threat (Catrantzos 2012). Other qualitative means of inquiry, such as case study interviews, were not adopted as the research design was not a broader qualitative enquiry. The Delphi method was considered the most appropriate method of enquiry allowing for deep interrogation of emerging insights whilst addressing the limitations and difficulties of research on IIT. Further, as the Delphi method provides anonymity (panellist identities are unknown to other expert members) it allows experts to provide information and opinion without bias or attribution.

The use of expert opinion in studying insider threat is well established (see Catrantzos 2012; Greitzer et al. 2013; Greitzer et al. 2009; Kraemer et al. 2009). Consistent with the themes addressed by Okoli and Pawlowski (2004) it is considered a practical and applicable research method as it can investigate a complex issue, provide a group method where experts do not need to meet yet interact with emerging views, is a flexible design that allows for follow up (leading to richer data/deeper understanding), can allow for solicitation of information and, if required, ranking importance of organisational vulnerabilities. It also provides a group opinion which may be more valid than an individual opinion (Keeney et al. 2010). The overall aim of the Delphi study was to provide the most pertinent and important variables associated with insider threat to assist in the development of the OVIT and identify aspects of IIT not yet reported in the extant literature.

3.4.2.1 Choosing Delphi participants/experts

The choice of Delphi participants is perhaps the most critical component to a successful Delphi process including the quality of overall conclusions (Lang 2001). In order to generate reliable expert-based contribution the practice of randomly selecting participants is not acceptable (de Meyrick 2003). Therefore, the Delphi method requires the use of non-random, purposive samples (Shariff 2015).

Choosing participants for a Delphi study has been the cause of contention in the literature. Even the use of the term ‘expert’ has created debate. According to Trevelyan and Robinson (2015) when designing a Delphi study consideration should

be given to how an 'expert' is defined as knowledge and experience cannot be easily assumed. Instead, these authors suggest that researchers should be explicit about participant's expertise, and avoid labelling participants as 'experts' altogether. Whilst this is an interesting recommendation, the use of the term 'expert' is commonplace in much of the Delphi research. As such, this study will use the term 'expert' to define the participants of the panel but will make clear how expertise was determined a priori.

Adler and Ziglio (1996) promote that Delphi participants should meet four requirements to ensure expertise: 1) knowledge and experience with issues under investigation; 2) capacity and willingness to participate; 3) sufficient time to participate; and, 4) effective communication skills. Further, Gutierrez (1989) refers to an expert as one who has an intimate knowledge of the subject under investigation, remains actively involved in the area, and is committed to the development of further insight and understanding. According to Campbell (2004) the definition of an expert will depend on the subject matter being explored, therefore clear representation of the way panel members are chosen is imperative.

de Meyrick (2003) encourages researchers to make explicit the basis for selecting panel members, providing a means of verification and transparency. For the purpose of the current study, experts were selected based on demonstrated expertise in the field of insider threat and specifically targeted to ensure coverage of the private and public sectors. This was considered important given one criticism of research has been a narrow focus on organisational types (Hunker & Probst 2011).

In addition to at least 10 years of involvement in Justice, National Security, Crisis Management, Counter Intelligence, Cyber Security, Risk Management, and/or Fraud Investigation, experts also had to meet one of the following recruitment criteria: (1) postgraduate qualifications in insider threat related research, (2) published articles on insider threat or related phenomena, (3) involvement in investigating insider threat cases, or (4) involvement in the assessment and mitigation of insider threat within organisations.

3.4.2.2 Anonymity

Keeney et al. (2010) stated that complete anonymity in a Delphi process cannot be guaranteed, given at least the primary researcher is aware of who is participating as an expert. In the current project the identity of participating panel members was only known to the primary researcher. This was seen as a method to reduce any concerns regarding identity and allow for participants to be open and truthful in their responses. A strength of using the Delphi method is that experts do not interact directly with each other, providing their thoughts independently, thereby avoiding groupthink (Catrantzos 2012) and protecting individual identities (for example those working in policing or security related organisations). Anonymity also ensures objective responses and results (Lilja et al. 2011b).

3.4.2.3 Participant details

There is debate in the literature about the required size of an expert Delphi panel and no specific direction on the number of experts that ensure a representative sample (Keeney et al. 2010; Shariff 2015). Delphi panel sizes do vary considerably and are influenced by factors including the level of problem complexity, resourcing, and whether the sample is homogenous or heterogeneous (Trevelyan & Robinson 2015). Skulmoski et al. (2007) suggest that using a homogenous sample of between ten and fifteen experts can yield sufficient results. Given the small number of participants the importance of a high level of panel expertise assists individuals to fully contribute to the process (Ludwig 1997).

Ensuring reliability in the Delphi method was an important consideration. As (Lilja et al. 2011b) noted, the size of the sample itself is not the most significant factor for reliability but the representativeness of the sample, with bias being minimised by the iterative Delphi process and anonymity of respondents. As the Delphi process did not use a random sample to represent the target population (Keeney et al. 2010), to minimise this concern experts were recruited from both public and private sectors and across a range of industry. It is acknowledged in the literature that random samples are not always viable or appropriate as long as experts represent a considerable diversity in viewpoints. The use of convenience sampling and snowball

techniques are commonplace in research employing the Delphi method (Keeney et al. 2010). The researcher aimed to recruit between 10 and 15 participants for this research in line with the recommendation of Skulmoski et al. (2007). Experts were initially contacts of the researcher and then a snowball technique was used to identify more members to achieve a higher participation rate (Lavrakas 2008).

Email was chosen as the method for the distribution of questionnaires due to its convenience and potential to reduce the turnaround time between questionnaires (Okoli & Pawlowski 2004). Email invitations including consent forms and participant information sheets (see Appendix A, B, and C) were emailed to 28 experts. The invitation was designed to explain the aim of the study, describe and define the Delphi process, and present the requirements of participation (anonymity, commitment, expected risks and benefits, etc.). Participants were also informed of the process for selection of experts as this has been shown to improve participation rates (Wee Yong et al. 1989).

Of the 28 experts who were invited to participate in the study, two (7%) declined participation, nine (32%) did not respond to the email, and 17 (61%) consented to participate in the research. To enhance participation, follow-up emails were sent to those who had not responded to the initial request for participation. After emailing the first round of the Delphi, two experts withdrew from the process. This left 15 experts participating in Round 1 of the Delphi. Of the 15 experts, seven were male and eight were female. Seven were from private organisations and eight were Government employees. Three participants had completed PhDs related to insider threat and seven had conducted work based research on insider threat. Finally, all Delphi participants met the criteria of experience investigating insider threat cases and in the assessment and mitigation of insider threat within organisations.

Attrition of participating experts did occur between round one and round two but was minimal (13%). Research suggests that attrition reduces as the Delphi process progresses (van Zolingen & Klaassen 2003) which is consistent with the drop out data in the current study. No further attrition occurred between round two and round

three of the Delphi resulting in 87% of panel experts remaining in the Delphi processes through all stages.

3.4.3 Delphi analysis

Hasson et al. (2000) reported that after an extensive review of Delphi literature there was no universal guideline available to assist researchers in how to perform data analysis. As expressed by Brady (2015) specific analytic techniques are not enforced by the Delphi method and the choice of data analysis is guided by the aim of the research, its design, and the type of data collected. Due to the iterative nature of a Delphi study, data analysis is continuous and conducted throughout the course of the research. As such, previous rounds of analysis help to inform the following rounds of the Delphi process (Brady 2015). Both qualitative and quantitative analysis techniques were utilised for the current study.

3.4.3.1 Quantitative analysis

The data was primarily quantitative in a question and answer format utilising Likert scales (see Appendix D, E, and F). As the Delphi survey was emailed to participants all of the responses required entry into SPSS; questions were represented by columns and each row represented one participant. Each question was given a code and values were attributed to ratings on the Likert scale. As participants had the choice to respond to questions, there were some questions with missing data. These values were not replaced.

The group's collective opinion was determined through descriptive statistics (Shariff 2015). Frequencies and P-P plots were used to assess the responses from the Australian panel experts and determine the level of consensus reached and the identification of any emerging issues or major discrepancies.

According to some authors optimising a Delphi study requires a priori definition of consensus (Diamond et al. 2014; Meijering et al. 2013). Consensus measurement in Delphi studies has been presented in both qualitative and descriptive statistics including; the stipulation of a number of rounds, level of panel members agreement,

mode, mean/median rankings, coefficient of variation, and post group consensus (Von der Gracht 2012). For the current study, consensus was defined a priori and primarily agreement driven. The use of expert agreement as an indicator of consensus is considered particularly meaningful when Likert scales are utilised as in the case of the current study (Trevelyan & Robinson 2015). Hence, consensus was deemed to be achieved if a) using the valid percentage at least 70 percent, typically acceptable in Delphi research (Brewer 2007), of panel members agreed on the direction of the response and b) using the P-P plot there was normal distribution with a low variability and minimal outliers. Where any item achieved at least 70% agreement and there were no 'polar-opposite' responses of concern it was considered to have reached consensus. Items that reached consensus were eliminated from further rounds of the Delphi study. These items were deemed 'pertinent' and included in the development of the OVIT.

It is important to note that the quantitative analysis process reduced the original number of items for Round 2 of the Delphi Study. This was considered important for the sustainability of the research including the consideration of participant fatigue and diminishing potential attrition (Keeney et al. 2010; Trevelyan & Robinson 2015).

3.4.3.2 Qualitative analysis

While thematic analysis is encouraged in the Delphi method, there is limited direction in the literature about how to undertake this task (Brady 2015). As such the literature has revealed various processes for qualitative data analysis and in some cases clear direction on the analysis is not available. For the purpose of the current study classical content analysis of qualitative data was used to determine emerging themes from responses to open ended questions in all three Delphi rounds. This process involved the identification of concepts and dimensions found in the text responses of participants.

The Delphi method can utilise computer packages or be processed manually (Shariff 2015). For the purpose of the current study, manual qualitative data analysis was

employed. Under the direction provided by Elo and Kyngäs (2008), the process of data analysis involved the preparation, organising, and reporting of data.

To prepare the data for analysis, text responses received from the Delphi rounds were transcribed verbatim to excel database. Consistent with the Profile Matrix (also referred to as a thematic matrix) presented by Kuckartz (2014), the questions of the Delphi survey were the structuring elements in the columns, and each row represented by one expert participant. As such the profile matrix allowed for both person- and question-oriented analysis.

The information contained within each text cell was then deductively analysed to identify patterns, new information, and further curiosities. Prior knowledge from the literature, along with expert consultation through supervision, also assisted in identifying pertinent details and avenues for follow up. The content analysis was targeted by ensuring the research question was the primary focus (Elo & Kyngäs 2008). Setting this parameter allowed the researcher to concentrate on units of analysis that were relevant to the topic and contributing to understanding of organisational vulnerability to intentional insider threat.

Commonly the results of qualitative analysis are fed back to participants in quantitative form (Hasson et al. 2000). This method of feedback along with the use of further open-ended questions was utilised in the current study.

3.4.4 Delphi Rounds

3.4.4.1 Delphi Round 1

In contrast to the Classical Delphi technique, round one of this modified Delphi study was developed based on the results of the phase one literature review. The use of systematic review of the literature to inform round one of the Delphi method is established in previous research (Shariff 2015; Slade et al. 2014). Through the phase one examination of the research, relevant items related to intentional insider threat were determined. These items were considered to be of high pertinence (Keeney et

al. 2010) and the expert panel was required to give feedback and make judgements on these pre-selected items.

It has been cautioned that using pre-existing information in a Delphi study may lead to bias or limit expert contribution (Hasson et al. 2000). To avoid such bias and ensure broad coverage of the topic of intentional insider threat, the addition of qualitative questions and options to provide additional comment via text boxes was implemented.

The items identified through phase one of the research were translated into survey format questions. A Likert scale was chosen as it is commonly used in the design of Delphi questionnaires and provides the key ability to interpret data through level of agreement and consensus (Keeney et al. 2010). Trevelyan and Robinson (2015) suggested that Delphi research is best with four to seven Likert scale categories. Consistent with this recommendation, a five point Likert scale was chosen. However, a neutral response was included in the current study, which was discouraged by the same authors. In addition to the Likert scale response to questions, experts were also offered the opportunity to raise issues and ideas not already identified in the questionnaire through free text responses. The first round of the Delphi was conducted between 24 November 2015 and 07 December 2015.

In order to address RQ2 the questions of the first Delphi round aimed to gain insight into (1) the experts' understanding and definition of insider threat, (2) what organisational vulnerabilities they believe contribute to insider threat behaviour, and (3) how organisations can better protect themselves from insider threat. See Appendix D for the specific questions of Delphi round one.

Following the submission of the 15 expert responses the results were compiled and analysed. In line with the underlying pragmatic approach to the research, qualitative and quantitative methods were used to analyse results in round one.

3.4.4.2 Delphi Round 2

The round 2 questionnaire was developed based on the results obtained using the qualitative and quantitative analysis described above. The Delphi continued with the three main areas of enquiry as detailed above including targeted questions developed from the opinions of the participants (Skulmoski et al. 2007).

The second round of the Delphi process was conducted between 05 February 2016 and 29 February 2016. The second round was the most demanding of the three Delphi questionnaires. Round 2 included feedback and results in the Annex (see Appendix E) from the initial Delphi questionnaire and presented more open-ended/narrative questions based on the outcomes of the initial round to gain further insights. This iterative process allowed experts the opportunity to validate (or dismiss) the main themes captured by the initial Delphi questionnaire (Catrantzos 2012). The Delphi Round 2 questionnaire can be found in Appendix E.

3.4.4.3 Delphi Round 3

The final round of the Delphi process was conducted between 31 March 2016 and 10 April 2016. Round three of the Delphi allowed the researcher to provide participants with the overall findings of the previous two rounds. Expert panel members were then asked to provide their level of agreement on the outcomes of the three main areas of enquiry (definition, vulnerabilities, and strengths). As such, this round was far more quantitative in approach in that it asked for a level of agreement to the findings. However, free text responses were also included for experts to provide further explanation if they chose. Additional questions that emerged from the Delphi Round 2 were also presented with Likert scale and free text responses. Based on guidance by Skulmoski et al. (2007) only three rounds of the Delphi were conducted as the process sufficiently answered RQ2 through achievement of consensus, satisfactory information exchange, and direction on the variables suitable for inclusion in the inventory. Furthermore, the use of three rounds is considered optimal to ensure results are meaningful whilst also remaining mindful of potential participant fatigue and attrition potential (Trevelyan & Robinson 2015). The round 3 questionnaire can be found at Appendix F.

3.4.5 Delphi Summary

Following the completion of the Delphi process, Delphi experts were provided with an overview of the Delphi findings. This process was considered important to verify and validate the findings as well as provide the opportunity to thank participants for their participation. This summary report, emailed to participants on the 25 May 2016, can be found in Appendix G.

3.4.6 Assessing the reliability and validity of the Delphi Method

3.4.6.1 Validity, Reliability, and Rigour

Face validity is defined as a judgment by experts that the items of the Delphi survey are addressing the construct of intentional insider threat (Neuman 2011). How well the survey addresses the appropriate concept in terms of relevance and presentation are components of face validity. Therefore, in the current research it was important to demonstrate and ensure that each round of the survey was clear and unambiguous (Shariff 2015). The expert panel raised no concern and expressed no confusion throughout the Delphi process contributing to face validity indicators. Further the high level of agreement across the items indicates that the questions presented as part of the Delphi were addressing the construct of intentional insider threat.

Content validity is secured in a Delphi method through involvement of expert participants as well as the use of iterative rounds (Shariff 2015) . Content validity is the assessment of whether a measure is representative of all aspects of the conceptual definition of a construct (Neuman 2011). The comprehensiveness of the Delphi surveys which were informed by published literature, careful analysis of each Delphi round, and inclusion of dimensions contributed by the expert panel members helped to increase content validity. In addition, the confirmation of the content throughout all three rounds and provision of a final summary paper allowed panel experts the opportunity to review outcomes.

Finally, concurrent validity is addressed through the iterative nature of the Delphi process. The use of successive rounds (Hasson et al. 2000) continuing to target concepts related to intentional insider threat, helped to increase concurrent validity.

As already presented above ensuring reliability in the Delphi method was an important consideration. Reliability is defined as the ability of a method to yield consistently similar results (Shariff 2015). One way to address reliability is through the choice of data collection. In the current Delphi study, the use of a 5-point Likert scale contributed to enhance reliability. As Trevelyan and Robinson (2015) discussed following their exploration of Likert scale reliability, the optimal number of Likert categories is between four and seven, as smaller scales have poor reliability and discriminating power and are less favoured by participants.

Diamond et al. (2014) recommended quality indicators for a Delphi study which included reproducible participant criteria, stated number of rounds, and clear criteria for consensus. Further, Hasson et al. (2000) provided guidance on ensuring a successful and credible Delphi study. They suggested that credibility (truthfulness), fittingness (applicability), auditability (consistency) and confirmability all add to the rigour of the study. The advice from Hasson et al. (2000) and Diamond et al. (2014) was clearly addressed in the current study.

The Delphi method reduces or eliminates influences that affect reliability such as group bias, group think, and influence of strong group influencers (Keeney, McKenna & Hasson 2010). The transparency of expert selection criteria, maintaining anonymity of respondents, and ensuring public and private sector representation in the Delphi study further contributed to reliability (Hasson, Keeney & McKenna 2000; Lilja, Laakso & Palomki 2011).

The success of the Delphi method can be enhanced through the organisation and administrative skills of the researcher (Hasson, Keeney & McKenna 2000). With this in mind, the use of a database to track the Delphi process was deemed an important attribute to reliability of the study. The database was developed with the objectives of the study in mind. It included coded details of each expert panel member, the industry and expertise represented, as well as details of the three Delphi rounds; including when emails were sent, when questionnaires were received, and any email reminders required.

In order to further demonstrate the rigour of the entire study, especially the Delphi method, the researcher kept a supervision journal throughout the course of the study (Brady 2015). Among other things this journal documented supervision sessions, methodological considerations, and major research decisions and rules. The journal was able to contribute to the trustworthiness of the study as it detailed contemplations and decisions made over the research journey, including identification of challenges and justification of decisions.

Given the high attention to validity, reliability and rigour indicators in the design and delivery of the Delphi study, these methodological considerations are considered well defensible.

3.5 Phase Three - Organisational Vulnerability to Intentional Insider Threat Inventory (OVIT)

3.5.1 Inventory Design

Based on the findings of both phase one and phase two of the project, the OVIT was developed. The Delphi process was an important component of the research, providing a means to consolidate the literature review findings (RQ1) and gain greater understanding of the most pertinent variables relevant to the construction of an inventory on Organisational Vulnerability to Insider Threat (OVIT). The implementation and validation of the inventory is also an important contributor to the Delphi study providing a means of validation of the Delphi process (Skulmoski et al. 2007).

Under the pragmatic paradigm research methods are chosen to best support the question being investigated. The current research intended to examine concepts in the form of distinct variables which contribute to an organisation's vulnerability to intentional insider threat. As such this phase of the study employed a quantitative cross-sectional approach to the research and the use of a survey as a valid form of enquiry (Creswell 2009, 2014). The exploratory and descriptive nature of the study suits the use of a cross-sectional survey design (administered at a single point in time)

where concerns such as being unable to investigate change or social processes are not pertinent (Creswell 2014).

There are many other advantages to employing a cross-sectional survey for the current research, especially in the online format. These include the ability to collect data in an unobtrusive manner, access to a hard to reach sample, participant anonymity, and reducing the time required to collect valuable information (Alessi & Martin 2010).

3.5.2 Development of the OVIT

The Organisational Vulnerability to Intentional Insider Threat Inventory (OVIT) was developed from the information obtained in phases one and two of the current research. The instrument was designed specifically for the current research. The inventory included both the conceptualisation and operationalisation of relevant dimensions related to intentional insider threat as distilled through consensus during the Delphi process. These dimensions were transformed into question format, and as per the quantitative component of the Delphi study, responses were on a 5-point Likert Scale with anchors of Strongly Agree to Strongly Disagree or Never to Always based on question type (see Sections 3.4.4.1 and 3.4.6.1 for justification of the use of 5-point Likert scales in survey research).

Due to the nature of the construct of organisational vulnerability to intentional insider threat the inventory was constructed to examine the three concepts (individual, organisational, and technical) as elucidated in the literature and Delphi process and in line with the initial conceptualisation presented in the literature review (Chapter 2). As such, the final OVIT Inventory was designed as three embedded instruments; OVIT – Individual, OVIT – Organisational, and OVIT – Technical (see Section 4; see Tables 21, 28, and 35). The initial online survey consisted of 242 questions; eight demographic (optional) questions and 234 questions relating to the three dimension of intentional insider threat (see Appendix I).

The online survey comprised six sections:

- Introductory cover page
- Demographic information
- Section for questions addressing *individual* factors (OVIT – Individual, 70 items); these questions explored the extent to which organisations assess and monitor a variety of known individual risk factors. The questions covered a wide range of individual vulnerabilities from social connections, psychological predispositions, motivation, staff behaviour, and duty-of-care perspectives.
- Section for questions addressing *organisational* factors (OVIT – Organisational, 119 items); questions specifically explored the organisational environment and how this can enable negative insider actions. Questions covered policies, practices, and strategies that may contribute to intentional insider threat.
- Section for questions addressing *technical* factors (OVIT – Technical, 45 items); these questions looked at how organisations may detect, analyse, and identify intentional insider threat potential through technical means. The questions covered areas such as access, monitoring, and technical control strategies.
- A thank you page and contact details.

Prior to conducting the pilot the draft survey in its entirety was distributed to the researcher's primary supervisor and two of the Delphi panel members to test the survey, and for feedback on the process, presentation and content. The feedback received was incorporated into the final pilot survey. In addition, the feedback cycle contributed to the face and content validity of the survey. The survey was then distributed for pilot testing.

3.5.3 Pilot of the OVIT

Pilot testing survey instruments is considered best-practice (Neuman 2011). It provides the researcher with the opportunity to make amendments to the design and

content and identify any potential problems with the survey itself, implementation, or form.

The pilot survey was available online through Questionpro™ (www.questionpro.com). As per the guidance of Johanson and Brooks (2010) samples representative of the population provide the most accuracy of parameter estimates and they suggest that 30 respondents is the reasonable minimum expectation for survey development. Working on this recommendation, the Delphi expert panel members, as detailed above, along with a convenience sample of senior public service risk managers and consultants from professional service companies in Australia were invited via email to complete the survey. The initial invitees were also encouraged to recruit participants (snowball technique). The pilot study was viewed by 79 people, many of whom did not begin the survey. Of the 30 participants that started the survey, 23 completed it. The response rate was 76.67%.

The results from the pilot attempted to improve the OVIT instrument, including validity, reliability and utility. It is acknowledged that a strong survey is able to accurately and consistently measure the constructs under investigation (Neuman 2011). As such, determining the statistical rigour of the survey was of paramount importance.

Due to the lower response rate (23 respondents) to the pilot study the ability to measure the reliability and validity through statistical analysis was compromised. Despite a seemingly low response to the pilot, which did not meet the target of Johanson and Brooks (2010), the number of participants does fall within routine recommendations for pilot and exploratory studies which have recommended between 10 and 30 participants in survey research (Johanson & Brooks 2010). Whilst statistical techniques were not performed, participants extended guidance and feedback on the survey, providing valuable content and face validity, as well as minor corrections to content, clarity, and completeness. The most often cited feedback was that the survey was very long; this was not surprising given the item list was intentionally oversampled, however, it was seen as imperative to reduce the length

of the survey before progressing. Several participants also made comment on the insight they were able to draw from the entirety of the survey and from the specific questions; a valuable outcome of participation and validation of the pragmatic approach whereby application and practice are important value considerations.

3.5.3.1 Improvement to the OVIT

Given the feedback on the length of the inventory it was deemed important to reduce the length. Analysis of the factorability of the pilot sample data aided in survey reduction. However, given the small sample size and the high number of items on each inventory (Individual, Organisational, and Technical), a factor analysis on the entire inventory or its three sub-inventories was not possible and violated guidance on minimum suitability for factor analysis (Hair et al. 2010). Given that statistical analyses were unable to be completed on the pilot OVIT, the researcher returned to qualitative and manual form of survey improvement.

A review of all of the items of the inventory was undertaken by the researcher in order to determine any duplicate or superfluous questions. Reducing the number of items was important from a practical perspective, but also for the future factor analytic process, where reduction of large numbers of variables is encouraged early to aid better factor solutions (MacCallum et al. 1999). To ensure this process was robust, the potential items for removal were confirmed with the researcher's supervisor and one panel expert for consensus. Through this process the inventories were reduced to 56 individual items, 90 organisational items, and 27 technical items.

3.5.4 Inventory administration

Consistent with the administration of the pilot study, the final OVIT was administered in its entirety online using Questionpro™ (www.questionpro.com). Questionpro™ provided the researcher the ability to construct and host the online survey in one destination. Participants were directed to the survey link, initially through email and then through other advertising means, in order to complete the survey. Responses to the survey are automatically coded and the data is stored by Questionpro™. Automatic reporting by Questionpro™ allows for detailed understanding of

responses through indication of views, dropouts, and completed surveys which are easily exported to SPSS for further analysis. An entry level subscription was chosen for this research. This limited some of the services, available through upgrade, but was not considered to negatively affect the current study or its ability to address the relevant research questions. The entry level package provided the ability to collect, store, and export the data relevant to meet the needs of the doctoral project.

There are many benefits to online surveys including the comparative low cost and ability to yield responses in real time and without the influence of researcher bias (Neuman 2011). For the current study the use of an online survey also provided opportunity for geographical distribution and a way to attempt to increase response rates.

3.5.5 Sampling

This study aimed to develop an organisational inventory to assess an organisations vulnerability to intentional insider threat. In its broadest sense all, and any, organisation may benefit from the implementation of the inventory. However, it is not possible to access the full population in the design, validation, or rollout of the survey. As such a sampling strategy is required. Sampling is the process of defining the population under investigation and in a mixed method approach can combine both random and purposeful samples (Creswell 2009).

The sampling strategy for the Delphi process and the pilot study are detailed above. For the deployment of the full OVIT, probability sampling and representation of the full population was not feasible. Instead, non-probability sampling was employed as it is considered the most appropriate method when a sample frame is not available (Sheehan 2002) or when the population is very large (Etikan 2016).

Convenience sampling utilises participants who are easily accessible whilst purposive sampling is the deliberate selection of participants due to their knowledge and experience (Etikan 2016). In the current research, the non-random selection of individuals available to the researcher, through convenience and purposive sampling,

included Delphi experts and other networks. In order to achieve the high number of responses required to undertake relevant statistical analyses, further outreach to a broader non-probability sample included a LinkedIn post requesting participation (https://www.linkedin.com/pulse/people-grudge-agenda-may-cause-crippling-damage-justine-bedford/?trackingId=rM770ON3AeQ87sMwnVkIMA%3D%3D), snowball sampling, direct request to specific organisations and to other Doctoral students, and inclusion of the research opportunity on the Australian Psychological Society website (http://www.psychology.org.au/academic/research_opps/). While non-probability sampling is a valid approach to the quantitative study of difficult to reach populations (Neuman 2011) it is acknowledged to be a limitation of the current study. The sampling method does not determine the depth of knowledge or participants understanding of the survey questions, which may be influenced by factors such as role in the organisation, commitment, and interest in IIT and related work behaviours.

3.5.5.1 Sample size

In order to facilitate the statistical analysis required to demonstrate rigour and meaningfulness a large sample size is required in quantitative research helping to reduce sampling error and provide adequate statistical power (Creswell 2009). The sample size is further determined by the number of elements included in the study (Hair et al. 2010). The purpose of the current study is to develop a set of inventories which assess an organisation's vulnerability to intentional insider threat. As previously stated, it is important that the entire inventory is reliable and valid but also, from a practical perspective, that it is not prohibitive in length. The use of factor analysis not only contributes to reliability and validity indicators but also contributes to data reduction through the identification of superfluous questions (Hair et al. 2010).

When it comes to determining the appropriate sample size to undertake a factor analysis there is considerable disagreement. This has led to confusion and overall has not served researchers well. Determination of an adequate sample size has included advice on absolute sample sizes, sample to variable ratios, and post-hoc

determinations discovered at the completion of data analysis. From an absolute sample size perspective, 100 cases is considered *poor* by some (Comrey & Lee 2013) but, under some conditions, adequate for others (Hair et al. 2010). According to several authors, a sample of 300 is considered a good size for any factor analysis (Comrey & Lee 2013; Tabachnick & Fidell 2013; Yong & Pearce 2013). Hair et al. (2010) state that in a factor analysis a sample of fewer than 50 is inadequate and that at least a sample size of 100 is preferred. Further, Kline (2005) recommends that as long as factor loadings are greater than 0.6, a sample size in excess of 200 is acceptable. Worthington and Whittaker (2006) demonstrated that absolute sample sizes endorsed in publications ranged between 84 and 411.

There are complex dynamics to be considered when conducting factor analysis and some researchers have argued that a minimum threshold for sample size does not exist and invariant across studies (Costello & Osborne 2005; de Winter et al. 2009; MacCallum et al. 1999). Whilst others recommend that adequate sample size is best discovered at the completion of data analysis (Cabrera-Nguyen 2010). Those suggesting that minimal sample size is not absolute instead look to alternative determinations including sample to variable ratio (recommendations range from 3:1 through to 20:1, although studies with as low as 2:1 have been reported; Costello & Osborne 2005), the factorability of the correlation matrix, measures of sampling adequacy, high communalities, high correlations and loadings, and items per factor (Cabrera-Nguyen 2010; de Winter et al. 2009; Guadagnoli & Velicer 1988; MacCallum et al. 1999; Williams et al. 2010).

Given that the current research is part of a doctoral study, time to collect data is not unlimited and this restricted the researcher's capacity to achieve a very large sample. In addition, it is well reported (and accepted) that low response rates are not uncommon when targeting mid-high level management participation or experts within a particular field (Cycyota & Harrison 2006) as is the case with the current study. Taking into consideration the above guidelines, noting caution in determining an absolute a priori threshold for factor analysis (MacCallum et al. 1999), the aim was to achieve 200 valid responses to all three inventories, satisfying various approaches

to determining minimum sample size, assuming that tests for sampling adequacy, communalities, and adequate factor loadings were also achieved.

3.6 Data Analysis Strategy

As already discussed, the primary purpose of the current research is to develop a diagnostic inventory assessing organisational vulnerability to intentional insider threat. In order to determine the best inventory questions and the validity and reliability of each of the inventories (Individual, Organisational, Technical), statistical analysis is required. The statistical analysis software, IBM SPSS version 25, was used to analyse the data of phase three of the current study. The following section describes the process of data extraction, preparation, and analysis.

3.6.1 Extracting the data

Responses to the final OVIT were collected online through Questionpro™. This online survey data management system was able to collect all data electronically which was then downloaded directly as an Excel file and exported to SPSS. Once available in SPSS the process of investigation followed the recommendations of Hair et al. (2010) and Creswell (2009), beginning with a check for inconsistencies in the data and examination for any missing data, followed by testing the assumptions of multivariate analysis (see Data analysis and interpretation Chapter 4).

3.6.2 Summary statistics

Descriptive statistics that summarise the demographic characteristics of the participants was extracted and collated. The purpose of this was two-fold. Firstly, it afforded an ability to identify suitability for further multivariate analysis (Hair et al. 2010) and secondly, it provided the researcher with an overview of the data set. Serving as a precursor to the EFA, calculations of the correlations between variables were also performed. This helped determine the potential for the EFA and provided an initial view of the relationships between variables. Results can be found in Chapter 4.

3.6.3 Exploratory Factor Analysis (EFA)

Factor analysis is a multivariate statistical approach which can be used in the construction, refinement, and evaluation of surveys (Williams et al. 2010). Whilst factor analysis has many promising uses, in relation to the current study it aided the construction of three inventories to measure intentional insider threat, reduction of a large number of questions into a smaller set, and provided construct validity evidence (Field 2013; Hair et al. 2010; Williams et al. 2010).

There are two types of factor analysis; confirmatory and exploratory. Due to the exploratory nature of the current study, including its progression into unchartered territory, the Exploratory Factor Analysis (EFA) was considered the most appropriate. This is in part due to the fact that the current research is not a test of theory and has no significant assumptions or expectations that are required of a confirmatory factor analysis (CFA; Williams et al. 2010).

As already elucidated above, the aim of the current study is to develop a diagnostic inventory to assess organisational vulnerability to intentional insider threat. Given the current state of research and practice in the area, this research is exploratory in nature. The research problem well suits the use of exploratory factor analysis, where the statistical technique can provide a way to summarise and condense a large number of inventory questions in to a smaller set and to best define constructs which underlie the original question sets (Hair et al. 2010; Hooper 2012; Williams et al. 2010).

From a data summary perspective, the EFA provides structure to the data. Through EFA individual variables are grouped together to represent a collective expression of a concept (Hair et al. 2010). In data reduction, the EFA helps to reduce the large number of inventory questions, in to a smaller and more manageable question set, whilst still retaining the nature and meaning of the original questions (Hair et al. 2010; Hooper 2012).

As factor analysis is an interdependence technique it is driven by both statistical assumptions and its underlying conceptual assumptions (Hair et al. 2010). As such, this multivariate technique is complementary to the pragmatic paradigm underpinning the current research. Consideration on the choice of variables is based on both statistical qualities and researcher judgement.

To support the current research an EFA is determined as the most suitable statistical analysis. Whilst EFA has been described as "a complex procedure with few absolute guidelines and many options" (Costello & Osborne 2005, p. 1) decisions must be made in an attempt to yield the best outcomes. Following exploration of the various extraction methods available, the Maximum Likelihood (ML) has been recommended as yielding the best results when data are relatively normally distributed (Costello & Osborne 2005). Therefore the current study used the ML.

"The goal of rotation is to simplify and clarify the data structure" (Costello & Osborne 2005, p. 3). Some authors discuss that in the social sciences the use of orthogonal rotation may be flawed as it is highly probable that units of interest are correlated (Costello & Osborne 2005; Hooper 2012). They determine that orthogonal rotation will not effectively and accurately produce a solution. Instead, the same authors recommend oblique rotation to reduce the loss of valuable information especially where factors are correlated. Oblique rotation (Promax) is chosen for the current research due to the assumption that factors are allowed to correlate (Costello & Osborne 2005; Field 2013; Hooper 2012).

As the OVIT consists of three embedded inventories, each was factor analysed separately. This is consistent with the advice of MacCallum et al. (1999) that it is "preferable" to analyse smaller inventories where variables adequately represent content of the domain.

3.6.4 Assessing the reliability and validity of the OVIT

When developing an empirically based survey instrument it is paramount that the inventory is valid and reliable and can therefore lead to meaningful results and

interpretation (Creswell 2009, 2014). *Reliability* is determined when an inventory is internally consistent, stable over time, and there is no change to administration and scoring (Creswell 2014). In contrast, *validity* is determined by the inventory's ability to provide meaningful and useful inferences (Creswell 2014). Neuman (2011) discusses that achieving perfect reliability and validity is not possible but that measures should be taken to achieve the most statistically sound instrument.

As the OVIT is a newly developed set of three inventories, specifically for this research, there is no previous assessment of validity or reliability. As such, this section will provide an overview of the design of the OVIT and its ability to connect measurement to constructs.

As previously discussed, the pragmatic paradigm underpins the current study. As such discussion of validity and reliability of the survey will be presented from the pragmatic worldview and with relevance to the current research. It is acknowledged there are some forms of validity which are not able to be addressed due to the limitations of the current research. For example, criterion validity and its subtypes which aim to measure the validity of an instrument through comparison and external verification sources (Neuman 2011). Concurrent validity relies on the ability to measure validity against a pre-existing measure of the construct (Neuman 2011). As the OVIT is a unique contribution to the study of insider threat, concurrent validity is unable to be assessed due to a lack of pre-existing and accepted measure of insider threat. Further, predictive validity relies on a future event or behaviour to verify the construct (Neuman 2011). The cross-sectional nature of the study prohibits assessment of predictive validity, which is a limitation of the current research. However, future longitudinal research will enable a better overview of concurrent validity. Further, case studies and organisationally specific research can assist in the assessment of the validity of the OVIT. The discussion below captures the most relevant reliability and validity indicators for the current research.

3.6.4.1 Face and content validity

Face validity is defined as a judgment by experts that the items of a survey are able to measure the construct (Neuman 2011). It has been argued that face validity is a weak form of validity due to its reliance on subjective criteria (Jones 1999). It has therefore been commented that face validity does not contribute significantly to the validity assessment and should be disregarded (Engel & Schutt 2009; Royal 2016). However, other authors consider that face validity has a role, especially in the development of new surveys, and provides a precursory assessment of validity prior to consideration of more effective and robust validity checks (Engel & Schutt 2009). Content validity is the assessment of whether a measure is representative of all aspects of the conceptual definition of a construct (Neuman 2011). As such, content validity is considered a valuable asset to survey design and is a highly recommended inclusion (Engel & Schutt 2009).

Both face and content validity were assessed in parallel during the current research. Face and content validity was established through reference to peer-reviewed literature in establishing items for the survey. Further the Delphi method provided a means for subject matter experts to determine insider threat items of high pertinence. Establishing consensus of the most relevant items through the Delphi process contributed equally to face and content validity. The review of the draft survey, for content and form, by experienced researchers and experts in the field provided additional support for the validity of the content. Finally, the implementation of a pilot survey also contributed to the measurement validity of the study. Whilst factor analysis was conducted during the pilot phase, the three inventories of the OVIT were subjected to factor analysis providing further support for face validity (see Section 4.4.3).

3.6.4.2 Convergent validity

Convergent validity is established when multiple measures of the same construct are associated with one another (Neuman 2011). Convergent validity is achieved when a high statistical correlation is found to exist between the items measuring their intended concepts (Hair et al. 2010). Convergent validity is established through factor

analysis. Again, due to the low response rate in the pilot study factor analysis was not possible. However, factor analysis of the three inventories of the final OVIT was found to be at an adequate level (see Data analysis and interpretation for EFA results). As such, the variables under the three concepts (individual, organisational, and technical) helped to better understand the distinct differences and aided diagnosis of organisational vulnerability to intentional insider threat.

The use of triangulation is also a component of the current study. Triangulation "seeks convergence, corroboration, and correspondence of results from different methods" (Creswell 2011, p. 62). The three phases of the current study, especially the Delphi process, pilot study, and final inventory, provide a means to determine the representativeness of items across different methods. These different methods allowed for corroboration of findings as well as helping to validate each separate phase of the research process.

3.6.4.3 Reliability

As previously stated it is not possible to achieve perfect validity and reliability. However, it is important to ensure that both validity and reliability are ably demonstrated. Interestingly, a reliable research study can be achieved without achieving validity. However, the reverse is not true; in order for research to be valid it must also be reliable (Engel & Schutt 2009). Therefore, reliability must be indicated in order for validity to follow. Neuman (2011) discussed three types of reliability: 1) measurement reliability, the consistency or dependability of the measure of a variable; 2) stability reliability, a measure of reliability across time and demonstrating consistency; and 3) representative reliability, a measure that yields consistent results across different groups.

Reliability of a measure can be enhanced through the clear conceptualisation of all constructs, increasing the level of measurement, using multiple indicators of a variable, and implementation of a pilot study. With respect to the current survey, all four of these potential improvements to reliability were considered (see Table 2).

Table 2: Reliability indicators of the study.

Conceptualisation	Review of current definitions, models and frameworks. Development of an intentional insider threat definition by Delphi experts.
Increasing measurement	The use of a 5-point Likert scale rather than a dichotomous response or 2-4 point Likert scale.
Multiple indicators	Several items in the OVIT addressing the one item of consensus by the Delphi panel
Pilot study	Implementation of peer, supervisor, and expert review of the draft survey as well as a pilot survey to Delphi experts (and beyond)

Source: Developed for this study.

Reliability of a survey may be determined by the internal consistency of a scale using the reliability coefficient (Hair et al. 2010). Hair et al. (2010) discusses the use of the Cronbach's alpha to be the most widely used and accepted measure of reliability. The outcomes of the Cronbach's alpha analyses indicated the entire OVIT (α = .98) and the three separate OVIT inventories (Individual α = .96; Organisational α = .96; Technical α = .95) to be reliable instruments as were the underlying Factors (see Data Analysis and Interpretation sections 4.4.3.4, 4.4.3.8, and 4.4.3.12, for further information).

Two other common measures of reliability include inter-rater reliability and test-retest reliability (Neuman 2011). Both of these types of reliability were not considered applicable to the current research due to the type of data collected and the use of a cross-sectional survey design. As with the predictive validity above, future use of the survey may provide opportunity to assess the instrument through a longitudinal design and achieve test-retest reliability; however, due to the parameters of the doctoral research, this was not achieved for the current study.

3.7 Limitations

Significant effort was made to ensure that the current study was able to balance statistical requirements and methodological rigour with practical utility. Under the pragmatic paradigm the research questions are considered central to the investigation and methods to extract valuable insight. All three phases of the current

research (literature review, Delphi method, and survey) were able to provide a positive contribution, academically and practically. Although the research was based on an exploratory and mixed method design, the main purpose was to develop a set of inventories to assess an organisation's vulnerability to intentional insider threat, hence greater emphasis on quantitative research.

Insider threat is a relatively new field of research. Certainly it has gained momentum, especially in the past decade and with the increasing focus on cyber security. However, the overall study of insider threat lacks theoretical underpinnings and direction. As such, the current research is not theoretically driven and without theoretical underpinning to inform interpretation of results, there is a level of subjectivity as determined by the researcher. However, this concern is partially mitigated by the chosen philosophical approach, the pragmatic worldview. The pragmatic paradigm does not require theory for application as it holds the research problem itself as the central consideration from which data collection and analysis is chosen (Mackenzie & Knipe 2006).

The use of mixed methods in the research design contributes to the depth and breadth of research outcomes. However, the results are still limited by the exploratory and cross-sectional design. Applying the OVIT to real case studies and determining its utility in demonstrating vulnerabilities is an avenue for future research and can assist to build on reliability and validity indicators of the OVIT. The ability to generalise findings and assert causality is restricted and only overcome by capacity for future longitudinal research (Creswell 2014) which is beyond the scope of the current doctoral studies, however the strongest validation would be for the OVIT to predict actual insider exploits that can only be determined by a longitudinal study (Greitzer et al. 2013). The resultant EFA outcomes are exploratory and further future studies will help to sharpen the outcomes.

As already discussed there are statistical limitations relevant to the methodology. Not all types of validity and reliability are able to be determined in the current research and will require further future exploration. The sample size in the pilot, whilst

meeting recommendations by several researchers (Johanson & Brooks 2010), allowed for pragmatic survey input including content, comprehension, and presentation. However, the pilot sample was not sufficient to satisfy minimum requirements for statistical analyses. Also, the capacity to achieve the desired 200 participants for the final OVIT analyses is potentially contentious given the difficulty in recruiting management and time poor responders.

Further, the EFA is largely criticised for its subjectivity, whereby results of the analysis are determined by the researcher (Williams et al. 2010). Further, Tabachnick and Fidell (2007) noted that the process of the EFA, including the choice of rotation and factors to retain, are not theoretically underpinned, but rather pragmatic and therefore rely on the judgment of the researcher. In order to reduce such bias, review processes were used throughout the study to ensure ongoing expert, colleague, and supervisor input. Finally, a limitation for the EFA is that the use of oblique rotation methods can present risk of being sample specific and lacking generalisability, especially when there is small sample size and/or low cases-to-variable ratio (Hair et al. 2010).

From a practical perspective the OVIT is able to provide organisations with education, understanding, and a baseline measure of overall vulnerability to intentional insider threat. It is hypothesised that the implementation of appropriate countermeasures to address areas of vulnerability should reduce an organisation's overall level of vulnerability. Again this assumption is not able to be tested within the restraints of the current project. It is, however, recommended that organisations may track progress through re-administration of the OVIT and that over time, predictive utility of the survey as well as risk parameters (such as what constitutes a low, moderate, or high level of vulnerability) can be determined.

A common concern of survey instruments is their reliance on self-report data. It is accepted that respondents to the OVIT may present bias including impression management and/or self-deception (Paulhus 1998). The OVIT was not designed to include measures of undesirable response styles. However, the survey result

outcomes were triangulated against the Delphi results and extant literature to establish a level of reliability. The absence of a measure of undesirable responding is a limitation that may be controlled by ensuring multiple members of an organisation, across various disciplines, participate in the completion of the OVIT. Having three separate inventories may be of significant benefit as staff can respond to the inventory specific to their role and/or level of organisational knowledge. Further, from a practical and academic perspective, additional qualitative measures and 360° feedback questionnaires may provide a way to further address this limitation.

The current study was designed to address a considerable limitation in the extant literature on insider threat, namely the absence of significant Australian contribution. As such the Delphi method was aimed at gathering Australian expert opinion on insider threat. It is possible that Australian expert opinion and experience differs from that of experts in other countries. Given this, it would be unwise to suggest the findings could be generalised internationally.

Finally, as discussed earlier, the study of insider threat is relatively new. A search of the available literature on insider threat especially that which relates to organisational vulnerability reveals it has received limited and narrow focus. However, this does not necessarily determine that research on the topic is not being conducted; only that it is not available through public means. There are several possible reasons for a lack of publication and presentation of research and experience; including potential damage to reputation (Sarkar 2010) or sensitive and classified material. Certainly the limited and redacted reporting on Project Slammer (Director of Central Intelligence 1990) suggests that further classified knowledge may be available but inaccessible. There was an attempt to overcome this problem through an extensive literature review, anonymous participation in the Delphi method and survey, and purposive sampling techniques. However it is possible that the items of the OVIT might have omitted or not factored in all dimensions of insider threat.

3.8 Ethical Considerations

In conducting research it is asserted that researchers consider and anticipate ethical issues that may arise throughout the research journey (Creswell 2009, 2011, 2014). According to Neuman (2011) a commitment to ethical conduct in research helps to preserve the integrity of the research process as well as the researcher and participants. To retain ethical integrity, University of Southern Queensland (USQ) places a strong emphasis on the promotion of ethical conduct. The ethical guidelines of the USQ are monitored by the Human Research Ethics Committee (HREC) and before the conduct of any research ethics approval must be granted. Human Ethics Research Approval was applied for and granted on 08 October 2015 and was valid until expiry on 08 October 2018 (see Appendix H). The HREC also requires the submission of Ethics Progress Reports at regular intervals.

Daft (2007, p. 374) defined ethics as "the code of moral principles and values that governs the behaviours of a person or group with respect to what is right and wrong". History, society and the environment has an effect on an individual's ethical values, along with organisational influence and professional standards (Daft 2007). In the workplace managerial ethics is defined as "[s]tandards of conduct and moral judgment used by managers of organisations in carrying out their business" (Bartol et al. 2008, p. 112).

As an Organisational Psychologist the researcher is expected to follow the Australian Psychological Society Code of Ethics (The Australian Psychological Society 2007, p. 6) which "articulates and promotes ethical principles, and sets specific standards to guide both psychologists and members of the public to a clear understanding and expectation of what is considered ethical professional conduct by psychologists". The code itself is built around three general ethical principles: Respect for the rights and dignity, propriety, and integrity of people. The APS Code of Ethics requires that when psychologists undertake research they also observe specific principles. In support of the APS Code of Ethics there are also Ethical Guidelines which aid ethical decision making, along with an ethical decision-making model (see Appendix J) to assist with working through ethical dilemmas.

The current research project falls under the definition of human research by the National Statement on Ethical Conduct in Human Research (The National Health and Medical Research Council 2007 (updated March 2014)) given that it involves participants taking part in surveys and the Delphi method. Taking into consideration the kind of harm, level of harm, and likelihood of harm to participants, the current research is considered to be low risk (The National Health and Medical Research Council 2007 (updated March 2014)). Still, the research requires anticipation of any relevant ethical dimensions (Creswell 2009). Possible ethical dilemmas, hurdles, and other considerations for the current research are addressed in Appendix K.

3.9 Summary

Chapter 3 provided an overview of the research design, paradigm, and strategy for the current study. Through detailing the research methodology, data collection, and methods of statistical analysis the rigour of the study was elucidated. Whilst the research is underpinned by a robust approach to investigation, it is not without limitations, which are acknowledged. Finally the ethical considerations of the study have been identified.

4 Data Analysis and Interpretation

4.1 Introduction

Chapter 3 provided an overview of the research design, strategy and methods adopted by the study to achieve the aims and objectives of the research as well as answering the research questions. It also described the strengths and limitations of the mixed method approach to the study and focused on a critical justification of the research analysis techniques. This chapter reports on the results of the three phases of the research project.

4.2 Phase One: The Literature Review

Phase one included a thematic analysis of the extant literature as a basis for determining the pertinent aspects of IIT as they relate to the aims of the study and the research questions. Based on the exhaustive review of literature available on IIT 141 items were determined relevant for inclusion in the phase two of the study. These were themes in the literature, focal areas of discussion, and directions in past research regarding where future research could be of benefit. To address the research aims, objectives and questions, the review looked at words and themes that related to the definition of IIT, (see Table 3), factors/variables considered to increase or decrease IIT (see Table 4), as well as organisational conditions thought to mitigate and moderate IIT (see Table 5). Italicised items are those that reached consensus in the following Delphi study phase.

4.2.1 The definition

As previously discussed, there are several definitions of insider threat available in the literature. However, in the absence of a widely accepted definition a more precise description for Australia may provide assistance to alleviate the fragmented conceptions which exist. As such the current study looked at current definitions, and presented the most used words to a panel of Australian experts for further consensus and clarification. The words from the literature are presented in

Table 3. An Australian definition of intentional insider threat is provided in Section 4.3.1.

Table 3: Definition of intentional insider threat: Words from the literature.

▪ Action ▪ Contractor/Consultant ▪ *Critical Information* ▪ *Employee* ▪ Inaction ▪ *Intent* ▪ *Knowledge*	▪ *Legitimate Access* ▪ *Loss* ▪ *Person of Trust* ▪ *Protected Information* ▪ *Sensitive Information* ▪ *Unauthorised* ▪ *Values Assets*

4.2.2 Increasing and decreasing intentional insider threat

The tables below outline key areas identified in the literature that have potential to affect organisational vulnerability to intentional insider threat. Table 4 provides the variables that were derived from the content analysis that decrease and increase potential for IIT. As can be determined in the table below there are a vast number of factors which affect IIT.

Table 4: Factors that increase or decrease IIT based on literature review.

Factors considered to decrease IIT	
▪ Ability to accept and integrate feedback ▪ *Aligned values* ▪ *Behavioural monitoring* ▪ Benchmarking ▪ *Computer monitoring* ▪ *Conscientiousness* ▪ *Control of physical security environment* ▪ Cultural understanding ▪ Employee assistance programs ▪ Extracurricular involvement ▪ Help-seeking ▪ *Impeded access/access controls* ▪ *Loyalty* ▪ *Minimum privileges* ▪ Ongoing education ▪ Positive economic position ▪ Positive IT subculture ▪ *Positive organisational culture* ▪ Positive reputation	▪ *Positive support networks* ▪ *Random auditing* ▪ *Relevant IT policies and procedures* ▪ *Relevant security policies and procedures* ▪ *Resilience* ▪ *Security awareness training* ▪ *Self-awareness* ▪ Sharing knowledge of insider risks outside the organisation ▪ Sophistication/knowledge of IT staff ▪ *Sound and reliable behaviour outside of work* ▪ *Sound judgment* ▪ Sound work history ▪ *Strict exit controls on staff leaving the organisation* ▪ Strict use of probation ▪ *Strong leadership* ▪ *Vetting and background checks*
Factors considered to increase IIT	
▪ *Criminal associations* ▪ Disparate values	▪ *Disgruntlement* ▪ *Ego/sense of entitlement*

▪ *Ethical flexibility* ▪ Foreign attachments ▪ *History of security violations* ▪ Increased market competition ▪ IT job market/skills shortage ▪ *Lack of leadership* ▪ *Limited authentication procedures* ▪ Mental health concerns ▪ *Moles* ▪ *Negative/stressful life events* ▪ *Old IT policies and procedures* ▪ Outsourcing work ▪ Personal computer behaviour; addiction, delinquency, etc. ▪ Planting: logic bombs, key logging ▪ Poor reputation ▪ *Poor sophistication of IT systems* ▪ Social networking ▪ *Targeted by competitors/foreigners* ▪ Use of contractors/transient workforce ▪ Use of personal technology devices	▪ *Financial pressures* ▪ High IT staff turnover ▪ Increase in number of cyber adversaries ▪ Ineffective/lack of collaboration with others ▪ *Lack of electronic access controls* ▪ Lack of social connectedness ▪ *Limited hardware controls* ▪ Mobile workforce ▪ *Motivation* ▪ *No/limited auditing and monitoring* ▪ *Organisational change* ▪ Overseas/remote/ satellite locations ▪ *Personality vulnerability/disorder* ▪ *Poor organisational culture* ▪ *Poor security culture* ▪ Reduced budget/economic position ▪ Speed of developing technologies ▪ Unsecured networks

4.2.3 Organisational conditions related to intentional insider threat

The research also presents variables extracted from content analysis regarding organisational conditions thought to moderate, and potentially mitigate IIT. These variables include organisational policies, processes, and other actions to reduce IIT. Table 5 provides the list of variables related to organisational conditions thought to moderate/mitigate organisational susceptibility to insider threat.

Table 5: Organisational variables that may mitigate or moderate IIT based on literature review.

Variables thought to moderate or mitigate insider threat	
▪ *Access* ▪ Background updates/re-evaluations ▪ Bag checks ▪ Collaboration with government or other businesses ▪ Cyber vetting ▪ Drug and alcohol testing ▪ *Electronic access controls* ▪ Employee assistance programs/ Staff counselling ▪ *Employee engagement* ▪ *Employee monitoring* ▪ *Employee screening and selection* ▪ *Impeded access* ▪ *Increase in staff counterproductive workplace behaviour* ▪ *IT monitoring of employees* ▪ *IT/Cyber security functions* ▪ *Leadership* ▪ *Management* ▪ *Organisational behaviour monitoring* ▪ *Organisational culture* ▪ Organisational economic pressures ▪ Organisational values ▪ Outsourcing ▪ Overseas locations ▪ Performance evaluations	▪ *Physical access controls* ▪ *Policy and procedures* ▪ *Polygraph* ▪ Psychological assessment ▪ Random auditing ▪ Recruitment ▪ Psychological assessment ▪ *Random auditing* ▪ Recruitment ▪ Referee checks ▪ Regulatory oversight ▪ Rotation of duties ▪ *Security awareness/education* ▪ *Security culture* ▪ *Security governance* ▪ *Security reporting* ▪ *Separation of duties* ▪ *Size of the organisation* ▪ Social engineering ▪ Specific insider threat training ▪ Staff morale ▪ Team members reporting ▪ Trust ▪ *Undue secrecy* ▪ Use of probation ▪ Vetting ▪ Video/CCTV

4.2.4 Working model of organisational vulnerability to intentional insider threat based on literature.

The conceptual model below (Figure 13) provides a synthesis of the literature review and content analysis in visual form. This model demonstrates the simple set relationship between the three concepts of organisational vulnerability to intentional insider threat. It is conceptually determined that organisational vulnerability to intentional insider threat is at *greatest* risk where the individual, organisational, and technical factors intersect.

Figure 13: A conceptual model of insider threat

Source: Developed for this study.

The current research proposes that increasing vulnerability is experienced when there are weaknesses across any or all of the three risk areas; organisational, individual, and technical. As such, the overlapping sections of any two factors represent an increasing organisational vulnerability to IIT and present opportunity for mitigation against IIT. However, it is only when all three are present that an actual IIT event is possible.

4.3 Phase Two: The Delphi Method

This section introduces the results of the Delphi study. The aim of the Delphi study was to generate, validate, and determine pertinent items of intentional insider threat to form a diagnostic inventory. The Delphi study was conducted over three consecutive rounds. Whilst the overall aim of the Delphi process was to determine relevant variables for inclusion in a diagnostic inventory of intentional insider threat, each round of the Delphi had its own individual aim.

The sections below provide a summary of the Delphi results as they relate to the research questions and support the development of a diagnostic inventory to assess organisational vulnerability to intentional insider threat.

4.3.1 An Australian definition of intentional insider threat

Generally there was a strong agreement on the key words associated with defining intentional insider threat. Results from Round 1 of the Delphi identified only three words from the literature in the definition not resonating well with the panel of experts and did not reach consensus. These terms included action, inaction, and contractor/consultant. The other 12 terms identified in the literature reached consensus (see Table 3).

Textual analysis of the overall input from panel experts through open-ended questions during the Delphi process assisted to uncover common themes. The words in Figure 14 appear in alphabetical order, however, their size relates to the frequency of appearance in panel expert responses through the Delphi process. Therefore, it is clear that the word organisation appears the most in the definition. The terms threat, employee, information, and intentional are also high ranking terms.

Figure 14: Text cloud showing frequency of words in summary of definition.

Based on the words achieving consensus and the strength of terms offered by the panel members, a definition of intentional insider threat was constructed and presented to the panel.

> *Intentional insider threat is when a person of trust (employee, contractor, consultant, vendor) who has/had legitimate access to an organisation attempts to cause harm through counterproductive behaviour intended to result in the loss, disclosure, or damage to that organisation's information, resources, or assets.*

Panel feedback and refinement resulted in the addition of the word *reputation*. All panel members agreed on the final definition:

> *Intentional insider threat is when a person of trust (employee, contractor, consultant, vendor) who has/had legitimate access to an organisation attempts to cause harm through counterproductive behaviour intended to result in the loss, disclosure, or damage to that organisation's information, resources, assets, or reputation.*

4.3.2 Delphi outcomes

4.3.2.1 Individual Influences

Individual vulnerabilities from the content analysis of the literature were presented to the panel. The panel were asked to rate to what extent they agree or disagree that the presented vulnerabilities contribute to an *increased* risk of intentional insider threat. Consensus was achieved on ten of the items presented. The panel also achieved consensus on eight of the items suggested to *decrease* risk of intentional insider threat (see Table 6 for variables achieving consensus).

Table 6: Individual variables that increase or decrease risk of intentional insider threat.

Individual variables from the literature which gained consensus	
Increase IIT	**Decrease IIT**
▪ Criminal associations ▪ Disgruntlement ▪ Ego/sense of entitlement ▪ Ethical flexibility ▪ Financial pressures ▪ History of security violations ▪ Motivation ▪ Negative/stressful life events ▪ Personality vulnerability/disorder ▪ Targeted by competitors/foreigners	▪ Aligned values ▪ Conscientiousness ▪ Loyalty ▪ Positive support networks ▪ Resilience ▪ Self-awareness ▪ Sound and reliable behaviour outside of work ▪ Sound judgment

Through open ended questions the panel was able to provide additional items, related to the individual that may be critical to increasing or decreasing intentional insider threat. These were collated and presented to the panel experts in subsequent rounds. The individual vulnerabilities identified by the panel and gaining overall consensus are presented in Table 7. As can be seen by the table, only variables thought to increase IIT was offered, or gained consensus, by the panel. There were

no individual variables offered or which gained consensus to assist in the reduction of IIT.

Table 7: Individual variables that increase individual vulnerabilities to intentional insider threat.

Individual variables thought to increase IIT offered by the panel
▪ Addictions (particularly gambling) ▪ Affiliations (religious, criminal) ▪ Concerns with moral development ▪ Financial concerns that could lead to embarrassment (i.e. gambling, poor investments) ▪ Lack of individual coping mechanisms/resources ▪ Workplace deviance

4.3.2.2 Organisational Influences

As per the individual analysis above, organisational variables from the content analysis of the literature were presented to the panel. The panel was asked to rate to what extent they agreed or disagreed that the presented items had an effect on intentional insider threat. As can be seen in Table 8 consensus was achieved on a large number of the organisational variables. The panel arrived at consensus on 18 items thought to increase IIT and 17 were considered to decrease risk of IIT.

Table 8: Organisational variables that increase and decrease insider threat.

Organisational variables from the literature which gained consensus	
Increase IIT	**Decrease IIT**
▪ Access ▪ Employee engagement ▪ Employee monitoring ▪ Employee screening and selection ▪ Increase in staff counterproductive workplace behaviour ▪ IT monitoring of employees ▪ Lack of leadership ▪ Leadership ▪ Management ▪ Moles ▪ Old IT policies and procedures ▪ Organisational behaviour monitoring ▪ Organisational change ▪ Organisational culture ▪ Poor organisational culture ▪ Poor security culture ▪ Poor sophistication of IT systems ▪ Undue secrecy	▪ Behavioural monitoring ▪ Control of physical security environment ▪ Physical access controls ▪ Policy and procedures ▪ Polygraph ▪ Positive organisational culture ▪ Relevant IT policies and procedures ▪ Relevant security policies and procedures ▪ Security awareness training ▪ Security awareness/education ▪ Security culture ▪ Security governance ▪ Security reporting ▪ Size of the organisation ▪ Strict exit controls on staff leaving the organisation ▪ Strong leadership ▪ Vetting and background checks

The panel was provided the opportunity to contribute further to organisational conditions that are critical in increasing or decreasing risk of IIT. Unlike the individual variables above, the panel offered a number of organisational items (21) that achieved consensus on increasing (11) and decreasing (10) IIT (see Table 9).

Table 9: Organisational variables that increase and decrease IIT.

Organisational variables from the panel	
Increase IIT	**Decrease IIT**
▪ Lack of consistency of policies and expectations across all levels of the organisation ▪ Lack of monitoring and enforcing policies ▪ Lack of oversight of senior managers ▪ Perception that managers do not value staff ▪ Complacency ▪ Lack of connection to employee issues ▪ Lack of management of issues at the emerging stages ▪ Poor application of security ▪ Poor organisational communication ▪ Poor security practices of leadership ▪ Witnessing other staff get away with poor security behaviour with no consequence	▪ Compliance and risk management education ▪ Improving research on how offenders "evaluate an opportunity" ▪ Leadership that is connected and supportive of staff ▪ Organisational resilience ▪ Positive leadership and change management ▪ Staff consultation ▪ Whistleblower protection policies ▪ Better communication across organisations ▪ Clear organisational goals and objectives ▪ Identifying red flags

4.3.2.3 Technical Influences

The same process was followed for the technical variables. The outcomes of the content analysis were presented to the Delphi experts. Items were rated on an agreement based Likert scale. As can be seen in Table 10 consensus was achieved across a number of technical items. The panel determined that nine of the items exposed from the content analysis were of significance to the study of IIT. The panel members further agreed on six items which may decrease risk of IIT.

Table 10: Technical variables that increase and decrease IIT.

Technical variables from the literature which gained consensus	
Increase IIT	**Decrease IIT**
▪ Electronic access controls ▪ Impeded access ▪ IT monitoring of employees ▪ IT/Cyber security functions ▪ Lack of electronic access controls ▪ Limited authentication procedures ▪ Limited hardware controls ▪ No/limited auditing and monitoring ▪ Poor sophistication of IT systems	▪ Computer monitoring ▪ Impeded access/access controls ▪ Minimum privileges ▪ Random auditing ▪ Separation of duties

The panel was offered the opportunity to provide further technical variables which they thought critical to increase, decrease, moderate, or mitigate IIT. The only additional technical variable that was offered by the Delphi panel experts and gained consensus was the inclusion of *obvious and declared security controls*.

4.3.3 Summary

The findings from the Delphi study were foundational for the development of a diagnostic inventory designed to determine an organisation's vulnerability to intentional insider threat. The individual, organisational, and technical items identified by the Delphi panel experts to be of pertinence in the study of IIT underpin the development of the inventory. Items of significance were determined based on consensus. That is, a) at least 70% of panel members agreed on its importance, and b) there was no abnormal distribution of responses for that item. Inventory questions were developed to represent each of the items which gained consensus through the Delphi process. The design of the OVIT is presented in Section 3.5. The results of phase three of the study are presented below.

4.4 Phase Three. The Organisational Vulnerability to Intentional Insider Threat Inventory (OVIT)

Data analysis is the process of "examining, categorizing, tabulating, or otherwise recombining the evidence, to address the initial propositions of a study" (Yin 1984). In order to achieve the aim of developing a diagnostic inventory to assess

organisational vulnerability to intentional insider threat an Exploratory Factor Analysis (EFA) was undertaken.

4.4.1 Data Preparation: Cleaning and Screening

Hair et al. (2010) discussed that it is important for researchers to assess and overcome potential pitfalls resulting from the design of the research and/or the data collection practices. In order to achieve this, cleaning and screening of the data is required. The process of investigation followed the recommendations of Hair et al. (2010) and Creswell (2009), beginning with a check for inconsistencies in the data and examination for any missing data.

4.4.1.1 Response rates

For the purpose of the current research the survey was administered according to the method outlined in Chapter 3. The sampling strategy also described in the previous chapter included convenience, purposive and nonprobability techniques. This effort of sampling resulted in 602 views of the online survey. Of the 602 views, only 161 (26.74%) commenced the survey. Following data preparation a total of 141 cases were retained for further analysis. Twenty cases were removed as they did not meet predetermined criteria for missing data (see 4.4.1.2). The sample size of 141 did not reach the a priori threshold of 200 valid cases. However, as demonstrated below the sample size presented no concerns for sampling adequacy, resulted in high communalities, provided a degree of over determination (where each factor is represented by a sufficient number of variables), and/or converged to a proper solution, all of which have been shown to provide quality factor solutions with relatively smaller sample sizes (MacCallum et al. 1999). Therefore the post-hoc judgment is that the sample size is adequate and sufficient to achieve the exploratory objectives of the study.

4.4.1.2 Missing data

As Hair et al. (2010) discussed there are both practical and substantive impacts of missing data, including reduction of sample size and possible bias in results. They

suggested a four-step process for identifying and remedying missing data before undertaking further statistical analysis. The steps include (1) identifying the type of missing data, (2) determining the extent of missing data, (3) diagnosing the randomness of missing data, and (4) choosing the imputation method.

Missing data can result from errors in data collection, data entry, or from the omission of answers on the part of respondents (Hair et al. 2010). To reduce the potential for missing data the survey was administered online with a setting loaded to ensure that participants completed all questions (not including demographic questions) before progressing to subsequent pages of the survey. As such there was no missing or inconsistent data for participants who completed the entire survey (n=141).

Following the process expressed by Hair et al. (2010) the survey set included missing data which could not be ignored. These missing data were easily identifiable to the researcher and were not random, mainly a result of failing to complete the survey (step one). Due to attrition, the extent of the missing data was extensive and not considered low enough to not affect the results (step two). Tabachnick and Fidell (2013) argued that appropriate treatment depends on the pattern of missing values. The most efficient method of remedy was to delete these non-random individual cases (Hair et al. 2010). This was considered appropriate especially as the design of the survey presented concepts of intentional insider threat in a specified order and grouping of questions (i.e., individual, organisational, and then technical). As such, failure to complete the entire survey often meant failure to address all three concepts of insider threat. Following this decision, it was not necessary to continue to steps three and four; applying empirical examination of the missing data and imputation.

Following this process the remaining number of cases with no missing data was 141 and sufficient to complete the selected analysis technique as described below. To ensure no data transfer concerns between the online survey tool and SPSS, a missing value analysis was conducted which determined no missing values in the data for the 141 respondents.

4.4.1.3 Outliers

Outliers can be defined as extreme responses which can unduly influence the outcome of EFA (Hair et al. 2010). Not all outliers are necessarily negative and instead should be reviewed within the context of the study and the statistical analysis of choice. Hair et al. (2010) recommend that where outliers have the potential to distort the multivariate analysis outcomes they should be handled appropriately. Based on methods for detecting outliers, no outliers were identified in the current data set for deletion.

The process for assessing potential outliers was undertaken using univariate analysis. The univariate analysis is used to identify any observations that are unique or extreme. According to Hair et al. (2010) cases falling outside the range of 2.5 to four standard deviations from the mean indicates the detection of an outlier. A review of the standard deviations suggested no univariate outliers (STD between 0.88 and 1.99).

4.4.1.4 Normality

Normality is the most fundamental assumption in multivariate analysis (Hair et al. 2010). Normality is defined as the "degree to which the distribution of the sample data corresponds to a normal distribution" (Hair et al. 2010, p. 36). Normality can be assessed in a number of ways and for the current study included both graphical and statistical assessment. Non-normality in data distribution can have random effects on analysis (Hall & Wang 2005). As such, normality was assessed using measures of kurtosis and skewness to determine any possible impacts due to the shape of the distribution.

Graphical analysis of normality was assessed through use of a normal probability plot. Normal P-P Plot, using Blom's proportion estimation formula, identified no significant concerns regarding the distribution of the data. Statistical analysis of normality can also be assessed using the skewness and kurtosis results of the descriptive statistics. West et al. (1995) proposed a reference of substantial departure from normality as an absolute skew value > 2.1. In addition, the same authors proposed a reference of

substantial departure from normality as an absolute kurtosis (proper) value > 7.1. Tabachnick and Fidell (2013) further suggested that an absolute z-score above 3.29 for either skewness or kurtosis raised concern of non-normal distribution. Based on these criteria the skewness and kurtosis results do not represent a departure from normality that would require a remedy for non-normality (see Appendix L for results).

4.4.1.5 Summary

The data preparation, cleaning, and screening provided critical insights into the characteristics of the data. Importantly, undertaking these steps ensured that the data analysis met the demands, assumptions, and requirements of multivariate techniques. Due to the survey strategy missing data was easily managed. Further graphical and statistical measures of outliers and non-normality suggested no significant violations to require remedy. As a result, 141 qualifying responses were included in the exploratory multivariate analysis.

4.4.2 Data Summary

4.4.2.1 Respondent profiles summary

Descriptive statistics that summarised the demographic characteristics of the participants were extracted and collated. The purpose of this was two-fold. Firstly, it provided an ability to identify suitability for further multivariate analysis (Hair et al. 2010) and secondly, allowed the researcher to understand the sample in greater depth.

In total, 141 qualifying respondents were included in the analyses. The demographic information in the online survey covered gender, age, level of education, job level, industry, size of organisation, and level of expertise on insider threat issues. Whilst missing values were not accepted for the questions related to the content of the inventory, missing data for the descriptive questions was accepted. Missing values ranged between 0.7% and 4.3% for the demographic questions. Tables 11, 12, 13, and 14 provide an overview of respondent characteristics.

Table 11: Frequencies of respondent profiles: Location.

		Frequency	Percent	Valid Percent
Location	Australia	138	97.87	97.87
	Other	3	2.13	2.13
	Total	141	100	100.0

Location: The OVIT survey was open to anyone with access to the Internet. However, sampling technique including non-random selection of individuals available to the researcher, through convenience and purposive sampling as well as broader non-probability techniques, resulted in a highly homogenous sample. As a result the majority of participants were located in Australia (97.87%).

Table 12: Frequencies of respondent profiles: Gender and age.

		Frequency	Percent	Valid Percent
Gender	Female	75	53.2	53.6
	Male	65	46.1	46.4
	Total	140	99.3	100.0
	Missing	1	0.7	
Age	18-24yrs	4	2.8	2.9
	25-34yrs	11	7.8	7.9
	35-44yrs	68	48.2	48.9
	45-54yrs	34	24.1	24.5
	55-64yrs	16	11.3	11.5
	65-74yrs	6	4.3	4.3
	Total	139	98.6	100.0
	Missing	2	1.4	

Age and Gender: The study did not purposefully target for age or gender. In summary the sample consisted of and almost equal balance 53.6% females and 46.4% males. With respect to age, the majority of respondents (48.9%) were between 35-44 years old with those aged between 45-54 years old accounting for a further 24.5%. As such the majority of participants were over 35 years of age and in the middle to advanced stages of their careers.

Education, Job Level, and Industry: As can been seen in Table 14, 64.8% of respondents were middle management and above. Specialist staff (11.5%) and Contractors/Consultants (13.7%) were also strongly represented in the sample.

Respondents with a tertiary education were strongly represented in this sample (77.1%). Of the 141 participants, 42.1% had a postgraduate qualification at or above the Master level. Overall, the sample can be regarded as predominantly having a tertiary level education with a minimal representation of those that have not pursued further vocational or tertiary qualifications (12.9%).

Table 13: Frequencies of respondent profiles: Education, Job level, Industry.

		Frequency	Percent	Valid Percent
Education	Less than Year 12	5	3.5	3.6
	Year 12 or equivalent	13	9.2	9.3
	Vocational/Trade Qualification	11	7.8	7.9
	Bachelor Degree	49	34.8	35.0
	Master Degree	50	35.5	35.7
	Doctoral Degree/PhD	9	6.4	6.4
	Other	3	2.1	2.1
	Total	140	99.3	100.0
	Missing	1	0.7	
Job level	CEO	15	10.6	10.8
	Senior Manager	29	20.6	20.9
	Middle manager	46	32.6	33.1
	General Staff	14	9.9	10.1
	Specialist Staff	16	11.3	11.5
	Contractor/Consultant	19	13.5	13.7
	Total	139	98.6	100.0
	Missing	2	1.4	
Industry	Government	74	52.5	53.2
	Private	50	35.5	36.0
	Not for Profit	10	7.1	7.2
	Other	5	3.5	3.6
	Total	139	98.6	100.0
	Missing	2	1.4	
APS Industry	Communication, Arts, Recreation	3	2.1	2.2
	Defence, Security, Intelligence, Law Enforcement	52	36.9	38.5
	Education, Employment	12	8.5	8.9
	Environment, Energy	4	2.8	3.0
	Health, Human, Social Services	16	11.3	11.9
	Industry, Science	9	6.4	6.7
	Not Applicable	19	13.5	14.1
	Other	19	13.5	14.1
	Fire and Emergency	1	0.7	0.7
	Total	135	95.7	100.0
	Missing	6	4.3	

With respect to Industry, there was a strong representation from Government (53.2%) and many respondents working in Defence, Security, Intelligence or Law Enforcement (38.5%). This is not an unexpected result given that the researcher primarily targeted participants from this population through purposeful and convenience sampling.

Table 14: Frequencies of respondent profiles: Insider threat expertise.

		Frequency	Percent	Valid Percent
Level of expertise on insider threat issues	Not advanced	28	19.9	20.4
	Somewhat advanced	24	17.0	17.5
	Moderately advanced	22	15.6	16.1
	Advanced	55	39.0	40.1
	Very advanced	8	5.7	5.8
	Total	137	97.2	100.0
	Missing	4	2.8	

Expertise: The level of insider threat expertise of the sample was considered an important demographic characteristic to capture. It was postulated that participants experience and exposure to insider threat issues would make completion of the inventory more straightforward. The inventory covered a depth and breadth of questions that were considered more accessible to respondents with insider threat experience as well as those in positions of management (with an overview of organisational functions). The fact that 79.6% of respondents had some level of experience with insider threat issues is a positive indication of ability to respond to the content of the inventories. Further, 62% of the sample was moderately to very advanced, suggesting that majority of the sample understood the context and nuances of IIT. Whilst 20.4% of participants did not have an advanced level of insider threat expertise they were able to complete the inventory.

Based on the frequency information available on the participants a high level of homogeneity in the sample was achieved. Respondent profiles demonstrate just close to parity outcomes on gender (53.6% female and 46.4% male), job level (approximately 30% for Senior Management, Middle Management, and general/specialist staff), industry sector (53.2% public versus 46.8% other) and a predominantly Australian sample (over 97%). The generally even distributions across a number of descriptive questions assisted in improving the internal validity of the results.

4.4.2.2 OVIT profiles summary

Appendix M is a representation of the distributed inventory questions in a descriptive format. The tables include the questions of the inventory, the valid percentage of responses, as well as the median response. As per the data preparation process described above, all 173 questions of the inventory are completed by the sample. For ease, the summaries below are separated to address each of the three dimensions considered to influence Organisational Vulnerability to Intentional Insider Threat, in line with the three separate OVIT inventories.

Individual:

Descriptive statistics from the individual inventory questions revealed that the organisations represented by the respondents could certainly do more to assess for individual vulnerabilities which have been associated with intentional insider threat. Over 40% of respondents indicated that their organisations *never* test for illegal drug use, past substance use/abuse, problematic gambling behaviour, or financial, credit, and bankruptcy history. Organisations also seem reluctant to identify increasing financial pressures on their employees. There seems to be some level of reliance on criminal record checks with 66.7% of organisations *often* or *always* checking the criminal history of potential staff with many of these (29.8%) also evaluating risk-related criminal associations. Despite this, a similar percentage (31.2%) does not review criminal associations. It seems surprising that 13.5% of organisations *never* checked criminal records as part of their organisational processes.

Positive conduct of employees appears to be valued with a very high representation of good conduct policy uptake (74.1%). Performance reviews remain a strongly endorsed employee management intervention. Perhaps an organisations ability to identify and manage potential for disgruntlement assists in very high commitment (58.9%), high ethical standards (68%), and integrity and honesty (66%) of staff. However, it is acknowledged that better management of workplace deviance may be warranted.

When it comes to psychological characteristics there is great variability of endorsement across the Likert scales. Questions associated with assessment of individuals, especially conscientiousness, sound judgment, self-awareness, resilience, and ego/sense of entitlement are not consistently applied. The variability in responses across the scale of these questions is a concern given the link between personality and character and potential to act as a malicious insider. There is possibly a link between the lack of strength in positive endorsement of these assessment methods and the perceived complacency of organisations when it comes to insider threat. More than half of the respondents indicated their organisations do not employ trained professionals to identify and manage employees vulnerable to become an insider threat. Therefore, it is not unsurprising that almost 55% of organisations do not regularly undertake personality testing to identify individuals with the potential to become an insider threat. Consistent with this, many organisations also do not identify employees susceptible to manipulation and coercion which may increase risk of insider threat action.

Organisational:

At an organisational level it appears there is a level of complacency when it comes to insider threat. Based on the results of the inventory there is a large variability in the utilisation of insider threat initiatives. Many respondents (41.8%) suggested that their organisations were not fostering an environment conducive to the success of insider threat initiatives. Almost 35% of the respondents indicated that their organisations do not have specialised or multidisciplinary teams for the evaluation of insider threat risk. As well, 34% of respondents indicated their organisations do not have a senior management position dedicated to security. Further, a high percentage (73%) is less than occasionally making efforts to integrate insider threat mitigation as part of their broader enterprise risk management strategy. Despite this there was a surprising level of positive response to organisations conducting research on insider threat (63.2% indicating at least occasional engagement).

While many organisations do not appear to be focusing specifically on insider threat intervention, respondents indicated a commitment to improving security (70.2%),

especially through exit strategies, including the disabling of access privileges and signing of non-disclosure statements. However, further protection through random reviews of exiting staff computer activities is warranted. A high percentage of respondents indicated their organisations *never* (22%), *rarely* (22%), or *occasionally* (28.4%) reviewed staff computer activities leading up to their final date. On-boarding processes suggested that there is a high level utilisation of evidence-based recruitment methods as well as subjecting staff to relevant vetting processes for their roles (58.2% often or always).

Physical security controls were common place through review of access anomalies and relevant policies of protection. Respondents also indicated a high uptake of policies and practices to protect organisational assets and prevent unauthorised disclosure of sensitive information. Certainly a high percentage (67.3%) of participants agreed that staff in their organisations were aware of critical assets worth protecting. There were quite a number of respondents indicating that their organisations did not have a whistle-blower policy (20.6%). Respondents also indicated a high level of variability across the Likert scale when it came to organisational policy, practice, principles, and measurement of counterproductive behaviour in the workplace.

With regard to organisational culture, climate, and staff engagement, respondents indicated a high level of adoption of annual and/or pulse surveys, assessment of organisational and job fit, and a strong level of collegiality. Further, respondents described their organisations as resilient and able to learn from failures and mistakes. Questions on security culture showed over 30% of organisations are *rarely* or *never* assessing security culture. This may be due to positive experiences of security culture within organisations. From this survey a significant portion of respondents disagreed that their organisation had a poor security culture (60.3%). Over half of the respondents agreed that security reporting is encouraged.

When it comes to management, respondents to this inventory indicated there may be room for improvement. There was strong capacity for management to

communicate plans and objectives, be accountable and responsible to others, and occasional utilisation of a variety of staff consultation methods to understand viewpoints. Further there was general support that management treated staff fairly (59.6%). However, 30% of respondents indicated that there was a perception that management did not value staff.

Technical:

A review of the 27 technical questions in the inventory revealed a substantial amount of variability in respondent answers resulting in a median of 3 (*occasionally*) for two-thirds (66.67%) of the questions. It is not clear whether participants were unable to respond to questions with conviction or whether the median response is indicative of an opportunity for greater response to technical vulnerabilities. Certainly, high numbers of managerial respondents indicated they should have some oversight of the technical capabilities of their organisations.

The two strongest positive actions of organisations, represented by the respondents include the existence of guidelines to ensure that staff only have access to data, systems, and information required to perform their duties (70.9%) and having back-up and recovery processes in place to avoid disruption (73%). The median results suggest that respondents felt their organisations were at least *occasionally* and often more regularly attending to potential technical vulnerabilities and implementing technical safeguards. Authentication processes in the respondent organisations were occasionally multi-factorial (79.4%) and increasingly advanced with greater access to critical data (79.4%). Further, monitoring for access anomalies of sensitive systems (80.8%) and collecting and monitoring network traffic and security log anomalies (75.9%) suggested a high level of attention of the organisations represented by this sample.

Whilst there were no questions with a median below 3 there were several questions in never and rarely categories such as: Organisations could make more use of advanced analytic tools to analyse and report on insider threat (38.3%), implementing auditing as part of performance reviews (46.8%), and using modern

technologies to assist insider threat detection, deterrence, prevention and reporting (31.2%). It is acknowledged that the uptake of these technical mitigations is influenced by the organisations complacency when it comes to insider threat focus and the value of insider threat specific intervention.

4.4.2.3 Summary: Descriptive Statistics

In summary, the current sample was represented by close to equal numbers of male and female respondents. The majority of the sample was highly educated, in the middle to advanced stage of career, and in positions of middle management or above. There was nearly equal representation of Government and Non-Government organisations and a high proportion of the sample expressed some level of insider threat expertise.

When considering the three dimensions of IIT the descriptive statistics demonstrated potential organisational vulnerabilities as well as strengths.

For the individual dimension, organisations could benefit more from checking for potential problematic behaviour, abuses, and personality characteristics associated with insider threat including workplace deviance. However, there is a strong sense of organisations attempting to manage staff behaviour through positive performance and conduct policy and strategies.

From an organisational perspective, complacency was a striking outcome. Organisations can clearly benefit from greater focus on intentional insider threat. A specialised/multidisciplinary team and dedication to security risk management can assist in improvements and uptake of IIT initiatives. Improvement in assessment of security culture and leadership and management, as well as relevant policy, process, and practice could prove beneficial. Based on this sample, organisations appear more focused on physical and technical security matters.

Technical safeguarding is well represented in this sample but could be further enhanced through use of modern technologies and advanced analytic tools designed to detect, deter, prevent, and report on IIT.

4.4.3 Exploratory Factor Analysis (EFA)

As presented earlier, an EFA was the chosen multivariate statistical approach to aid the development of the OVIT. An EFA is appropriate in exploratory studies and allows for the construction, refinement, and evaluation of statistical validity of surveys. The EFA is a statistical technique which is able to summarise and condense the large OVIT question set into a smaller question set and also define the underlying factor structure which may exist.

An EFA was conducted on each of the dimensions of IIT as represented by the sub-inventories of the OVIT, beginning with the OVIT-Individual and followed by the OVIT-Organisational and OVIT-Technical. The following section more explicitly discusses the process of obtaining results for the OVIT-Individual, the OVIT-Organisational and OVIT-Technical.

4.4.3.1 OVIT – Individual: Testing the assumptions

Hooper (2012) recommended that prior to interpreting an EFA output the first step is to explore the Correlation Matrix. The Pearson Bivariate Correlation was chosen to ensure there were correlation coefficients that exceeded 0.30 among the variables of the three inventories. Examination of the correlation matrix determined there were many coefficients greater than 0.30.

A highlighting condition was set in SPSS to easily determine correlations above 0.9, noting that correlations above 0.9 may indicate multi-collinearity (Hair et al. 2010; Yong & Pearce 2013). There was evidence of multi-collinearity with two items correlating above 0.9 (I5 – does the organisation assess past substance use and I6 – does the organisation assess for problematic gambling behaviour) in the OVIT – Individual. It was decided, based on researcher judgment, to maintain both of these questions in this exploratory stage of the research noting that each question is

conceptually different. Due to the size of the correlation matrices, the nature of the exploratory study, and in line with recommendations of Jackson et al. (2009), they have not been included in this thesis. The correlation matrices are available from the author on request.

In order to assess the overall significance of the correlation matrix, the Bartlett test of sphericity was performed (Field 2013). This a statistical test to determine suitability for EFA and is an indication that there exits correlations among variables (Hair et al. 2010). The Bartlett's test of sphericity was significant for the OVIT-Individual (see Table 15) at 0.94 sampling adequacy.

The measure of sampling adequacy (MSA) measures the degree of inter-correlations among variables and should be greater than 0.5 to proceed with an EFA (Hair et al. 2010). According to Tabachnick and Fidell (2013) using the Kaiser-Meyer-Olkin's (KMO) test of sampling adequacy a value greater than 0.60 provides evidence for factorability. Further Williams et al. (2010) noted the importance of this index, especially where case to variable ratios are low (as is the case in this research). The KMO measure of sampling adequacy for the OVIT-Individual is well above the recommended 0.60 (see Table 15).

Table 15: OVIT-Individual KMO and Bartlett's Test.

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		0.941
Bartlett's Test of Sphericity	Approx. Chi-Square	3347.240
	df	300
	Sig.	0.000

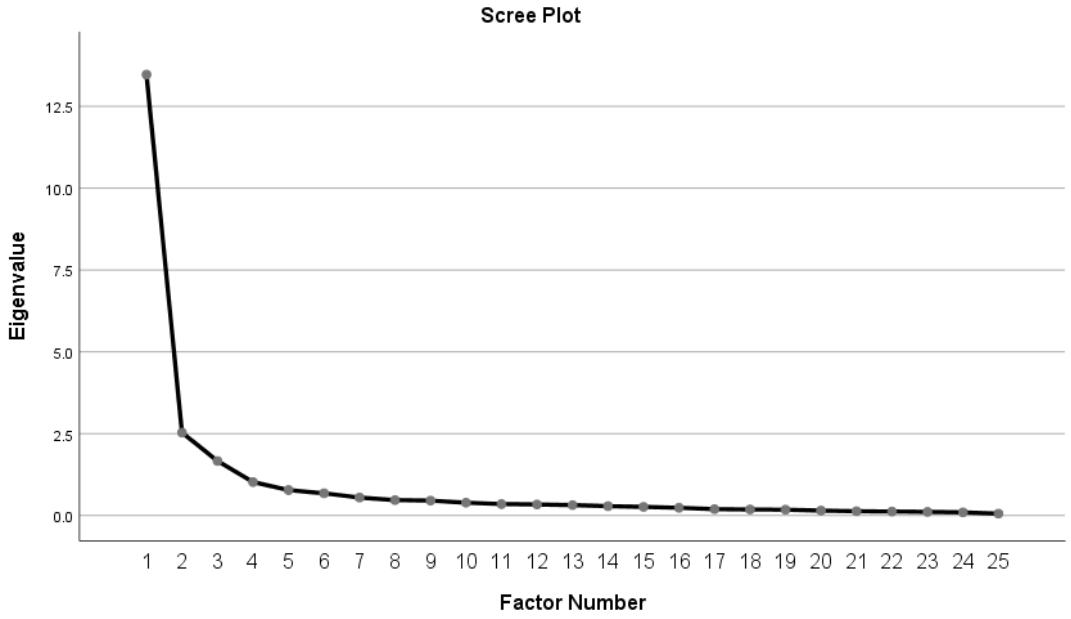
4.4.3.2 OVIT – Individual: Extraction of factors

Costello and Osborne (2005) warned there is danger in over-and under-extraction of factors and careful consideration of factor retention should be applied. Hair et al. (2010) encourage researchers to combine a conceptual and evidence based approach

to factor reduction and suggest that researchers consider how many factors should be in the structure and how many factors can be reasonably supported.

A number of selection criteria were utilised to determine factor extraction. First, a scree test was viewed to determine the optimum number of factors to be extracted. The point at which the scree curve begins to straighten out determines the maximum number of factors to extract. Given that the initial scree test results showed clustering of data points near the bend, multiple factor analyses were performed to improve factor extraction (Costello & Osborne 2005). The final scree test for the EFA are presented in Figure 15.

Figure 15: The Final OVIT-Individual Scree Plot.



The combination of the scree test and eigenvalues is recommended to determine the number of factors to retain (Yong & Pearce 2013). It is recommended that Eigenvalues should be greater than one when applied as a factor extraction method (Field 2013; Hair et al. 2010; Hooper 2012; Yong & Pearce 2013). As such, the Eigenvalues were utilised to assist factor extraction (using both the scree test and variance explained). The final Eigenvalue outcome is presented below in Table 16.

Table 16: The Final OVIT–Individual Eigenvalues.

Total Variance Explained

Factor	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings[a]
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total
1	13.470	53.881	53.881	12.918	51.673	51.673	11.812
2	2.532	10.128	64.009	2.269	9.078	60.751	10.398
3	1.665	6.661	70.670	1.445	5.781	66.532	9.215
4	1.021	4.083	74.753	0.957	3.827	70.360	2.126
5	0.776	3.105	77.858				
6	0.677	2.709	80.567				
7	0.547	2.189	82.756				
8	0.470	1.882	84.638				
9	0.453	1.811	86.450				
10	0.390	1.559	88.009				
11	0.349	1.394	89.403				
12	0.337	1.349	90.752				
13	0.317	1.270	92.022				
14	0.285	1.139	93.160				
15	0.264	1.054	94.215				
16	0.235	0.942	95.157				
17	0.192	0.768	95.925				
18	0.183	0.732	96.657				
19	0.177	0.707	97.364				
20	0.149	0.596	97.959				
21	0.128	0.513	98.473				
22	0.121	0.485	98.958				
23	0.108	0.434	99.392				
24	0.095	0.379	99.771				
25	0.057	0.229	100.000				

Extraction Method: Maximum Likelihood.

a. When factors are correlated, sums of squared loadings cannot be added to obtain a total variance.

Additionally, the percentage of variance also aided factor extraction. Hair et al. (2010) discussed that, in the social sciences, solutions are satisfactory if they account for more than 60% of the total variance. As can be seen in Table 16 the percentage of variance explained in the final EFA for the OVIT-Individual is well above this recommendation (70.36%).

Utilising these three approaches to factor extraction, along with researcher judgment consistent with the conceptual and theoretical underpinnings of the research, the final OVIT – Individual factor solution included four individual factors.

4.4.3.3 OVIT – Individual: Factor rotation and interpretation

The Maximum Likelihood procedure was used to extract factors from the variables of the OVIT-Individual. Hair et al. (2010) underlined the importance of factor rotation in interpreting factors. For the current research the *Promax* oblique rotation was chosen in the quest to achieve a simple and meaningful factor structure outcome (Pett et al. 2003). Costello and Osborne (2005) suggest that the use of the default kappa (4) is appropriate when using the Promax oblique rotation and this was maintained for the current study.

Following the guidance of Field (2013) the factor loadings and communalities were explored first. In search for the best factor solution, item loadings above 0.30, with the least crossloadings, and factors with at least three items are considered "best-fit" (Costello & Osborne 2005). However, according to Hair et al. (2010) factor loadings above ±0.3 meet minimal level, with loadings ±0.5 considered practically significant and loadings exceeding ±0.7 indicating a well-defined structure (Hair et al. 2010). Further, Hooper (2012) suggest that loadings less than .40 may indicate that it is unreliable and a candidate for deletion.

Following these guidelines, low-loading items (less than 0.40) were dismissed unless there was a determination, based on theoretical or conceptual reasoning and in line with the underpinning pragmatic paradigm that the item should remain in this exploratory phase. According to Costello and Osborne (2005) researcher judgment is important as the removal of some items can compromise the integrity of the data. Further, any items below 0.40 that were retained did not breach the minimum loading of an item of at least 0.32 (Tabachnick & Fidell 2007). Next, Communalities were explored to determine factor items that may be candidates for deletion. It is commonly accepted that communalities above 0.3 are stable (Hooper 2012). However, Costello and Osborne (2005) argued that in the social sciences

communalities between 0.40 and 0.70 are appropriate and that anything below 0.40 should be considered for removal. Consideration of the communalities along with the item loadings was undertaken in conjunction. Communalities for the OVIT –Individual can be found in Table 17.

Table 17: The Final OVIT–Individual Communalities.

Communalities[a]

	Initial	Extraction
I5. does the organisation assess past substance use/abuse	0.910	0.908
I6. does the organisation assess for problematic gambling behaviour	0.901	0.920
I17. does the organisation monitor foreign contacts of staff	0.779	0.764
I9. does the organisation have methods to identify financial pressures of employees	0.826	0.760
I8. does the organisation assess financial, credit, and bankruptcy history	0.808	0.735
I14. does the organisation evaluate risk-related criminal associations	0.736	0.684
I16. does the organisation identify employees susceptible to social engineering (manipulation of people to get them to perform actions that do harm)	0.747	0.699
I38. does the organisation employ trained professionals to identify and manage employees vulnerable to becoming an insider threat	0.720	0.671
I44. the organisation has methods to assess for addictions	0.704	0.658
I4. does the organisation test for illegal drug use	0.692	0.624
I32. does the organisation utilise methods to assess for employee resilience	0.729	0.720
I36. does the organisation conduct mental health testing/assessment	0.820	0.800
I37. does the organisation conduct personality testing to determine an employee's vulnerability to become an insider threat	0.820	0.802
I34. does the organisation utilise methods to assess for employee sound judgment	0.735	0.631
I35. does the organisation utilise methods to assess for employee conscientiousness	0.730	0.631
I39. does the organisation utilise methods to assess for employee self-awareness	0.721	0.675
I31. does the organisation utilise methods during recruitment processes to assess for ego/sense of entitlement	0.646	0.588
I3. does the organisation have policy and processes to manage staff with a history of security violations	0.732	0.806
I10. does the organisation undertake a formal risk assessment of high risk employees/positions	0.734	0.712
I11. does the organisation have a means by which employees can report suspicious contacts from other employees or outsiders	0.588	0.590
I1. does the organisation check civil records	0.599	0.527
I2. does the organisation have methods to assess sound and reliable behaviour of staff	0.654	0.576
I15. does the organisation check criminal records	0.533	0.354
I55. people in the organisation maintain high ethical standards	0.796	0.972
I56. people in the organisation demonstrate high integrity & honesty	0.785	0.783

Extraction Method: Maximum Likelihood.

a. One or more communality estimates greater than 1 were encountered during iterations. The resulting solution should be interpreted with caution.

The communality table presents a caution of a Heywood case. An Heywood case is represented by a communality equal to or greater than 1 (Harris 2001). With the respecifying of the factor model the extracted communality of question I55 continued to rise. According to the current table, the communality estimate has become greater than 1. It is explained that the Maximum Likelihood method is susceptible to Heywood cases and there is debate about whether a Heywood case alone invalidates the solution. At this stage the variable has been maintained as it did not produce problematic communality estimates in earlier EFA solutions and the final solution has a maximum communality (0.972) below one (Harris 2001). de Winter et al. (2009) reported that Heywood cases reduce as *p* increases, and therefore, it is considered possible that the Heywood case may be improved in future analyses once greater sample size is achieved. Further, there is evidence of other published exploratory studies with similar communality estimates (e.g. Turner 2015).

The tables below show the factor loadings after rotation using a significant factor criterion of 0.40. One item (I15. does the organisation check criminal records) fell below 0.4, represented in italics in Table 18 below, was maintained based on theoretical, conceptual, or researcher judgement. As described by Pett et al. (2003) some weak-loading items can be significant contributors to the content of a scale and therefore should not be eliminated. Further, this item remained within the minimum guidelines of 0.3 presented by other authors (Hair et al. 2010; Tabachnick & Fidell 2007).

Table 18: The Final OVIT – Individual Pattern Matrix.

Pattern Matrix[a]

	Factor			
	1	2	3	4
I6. does the organisation assess for problematic gambling behaviour	1.046			
I5. does the organisation assess past substance use/abuse	0.959			
I8. does the organisation assess financial, credit, and bankruptcy history	0.958			
I9. does the organisation have methods to identify financial pressures of employees	0.823			
I17. does the organisation monitor foreign contacts of staff	0.794			
I4. does the organisation test for illegal drug use	0.570			
I16. does the organisation identify employees susceptible to social engineering (manipulation of people to get them to perform actions that do harm)	0.501			
I14. does the organisation evaluate risk-related criminal associations	0.478			
I44. the organisation has methods to assess for addictions	0.473			
I38. does the organisation employ trained professionals to identify and manage employees vulnerable to becoming an insider threat	0.449			
I15. does the organisation check criminal records	*0.359*			
I34. does the organisation utilise methods to assess for employee sound judgment		0.854		
I39. does the organisation utilise methods to assess for employee self-awareness		0.829		
I35. does the organisation utilise methods to assess for employee conscientiousness		0.812		
I31. does the organisation utilise methods during recruitment processes to assess for ego/sense of entitlement		0.780		
I32. does the organisation utilise methods to assess for employee resilience		0.775		
I37. does the organisation conduct personality testing to determine an employee's vulnerability to become an insider threat	0.482	0.659		
I36. does the organisation conduct mental health testing/assessment	0.431	0.619		
I3. does the organisation have policy and processes to manage staff with a history of security violations			0.920	
I11. does the organisation have a means by which employees can report suspicious contacts from other employees or outsiders			0.690	
I1. does the organisation check civil records			0.653	
I10. does the organisation undertake a formal risk assessment of high risk employees/positions			0.642	
I2. does the organisation have methods to assess sound and reliable behaviour of staff			0.498	
I55. people in the organisation maintain high ethical standards				1.007
I56. people in the organisation demonstrate high integrity & honesty				0.859

Extraction Method: Maximum Likelihood.
Rotation Method: Promax with Kaiser Normalization.[a]
a. Rotation converged in 6 iterations.

Note: Factor loadings < 0.4 are suppressed to assist in determining cross-loading and high loading items

Hooper (2012) recommended that before interpreting factor analysis a check for cross-loadings on the pattern matrix is required. Cross-loading items may require further consideration as these too raise questions regarding the reliability of the item (Hooper 2012). According to Costello and Osborne (2005, p. 4) "[a] "crossloading" item is an item that loads at 0.32 or higher on two or more factors". However, Hooper (2012) was more strict with a criteria of 0.4.

As can be seen from the pattern matrices, there are two cross-loading items evident (I36 and I37). Despite the suggestion of Hooper (2012) to remove cross-loading items, other authors have argued that correlating factors are not a high level concern in exploratory stages of research (Brown 2009; Pett et al. 2003). Based on the exploratory nature of the study, these cross-loading items were retained based on the researcher's judgment and underlying theory (Costello & Osborne 2005; Field 2013; Pett et al. 2003) and in line with the underlying pragmatic paradigm which balances practical utility with scientific outcomes. Yong and Pearce (2013) articulate that items that are crossloading may be retained if theoretical interpretation fits. Whilst the pattern of loadings demonstrated in this study is clear there is complexity in the factor structures as demonstrated by the cross-loadings (Brown 2009).

There appears to be debate in the literature about whether the pattern or structure matrix, or both, should be the basis for interpretation in an EFA. According to Hair et al. (2010) many interpret the pattern matrix as it usually presents a more simple demonstration of the relationships between factors. Many researchers recommend the pattern matrix for interpretation (Costello & Osborne 2005; Field 2013; Hooper 2012), especially where factors are highly correlated (Field 2013). It is acknowledged that with an oblique rotation a difference in the pattern and structure matrix exists. It has been argued that the structure matrix best accounts for the bi-directional quality of the relationships between variables and factors and therefore the structure matrix should be the basis for interpretation (Comrey & Lee 2013; Graham et al. 2003). Following the guidance of several researchers, the pattern and structure matrices were both examined (Gorusch 1983; Graham et al. 2003; Hair et al. 2010).

Table 19: The Final OVIT – Individual Structure Matrix.

Structure Matrix

	Factor			
	1	2	3	4
I5. does the organisation assess past substance use/abuse	**0.951**	0.642	0.678	
I6. does the organisation assess for problematic gambling behaviour	**0.951**	0.587	0.663	
I17. does the organisation monitor foreign contacts of staff	**0.870**	0.629	0.662	
I9. does the organisation have methods to identify financial pressures of employees	**0.868**	0.637	0.640	
I8. does the organisation assess financial, credit, and bankruptcy history	**0.854**	0.570	0.556	
I14. does the organisation evaluate risk-related criminal associations	**0.783**	0.648	0.724	
I16. does the organisation identify employees susceptible to social engineering (manipulation of people to get them to perform actions that do harm)	**0.782**	0.707	0.699	
I38. does the organisation employ trained professionals to identify and manage employees vulnerable to becoming an insider threat	**0.773**	0.725	0.584	
I44. the organisation has methods to assess for addictions	**0.765**	0.728	0.600	
I4. does the organisation test for illegal drug use	**0.761**	0.540	0.572	
I32. does the organisation utilise methods to assess for employee resilience	0.613	**0.845**	0.551	
I37. does the organisation conduct personality testing to determine an employee's vulnerability to become an insider threat	0.771	**0.834**	0.465	
I36. does the organisation conduct mental health testing/assessment	0.793	**0.827**	0.527	
I39. does the organisation utilise methods to assess for employee self-awareness	0.577	**0.820**	0.516	
I35. does the organisation utilise methods to assess for employee conscientiousness	0.506	**0.786**	0.454	
I34. does the organisation utilise methods to assess for employee sound judgment	0.454	**0.777**	0.491	
I31. does the organisation utilise methods during recruitment processes to assess for ego/sense of entitlement	0.524	**0.766**	0.482	
I3. does the organisation have policy and processes to manage staff with a history of security violations	0.630	0.529	**0.891**	
I10. does the organisation undertake a formal risk assessment of high risk employees/positions	0.704	0.561	**0.822**	
I11. does the organisation have a means by which employees can report suspicious contacts from other employees or outsiders	0.549	0.560	**0.756**	
I1. does the organisation check civil records	0.564	0.402	**0.712**	
I2. does the organisation have methods to assess sound and reliable behaviour of staff	0.547	0.617	**0.705**	
I15. does the organisation check criminal records	0.527	0.426	**0.542**	
I55. people in the organisation maintain high ethical standards				**0.984**
I56. people in the organisation demonstrate high integrity & honesty				**0.883**

Extraction Method: Maximum Likelihood.
Rotation Method: Promax with Kaiser Normalization.

As Hair et al. (2010) expressed the structure matrix output is more complicated and it is not uncommon that variables will load highly on more than one factor. Hence, they argue a preference for interpreting the pattern matrix, which presents the unique, rather than shared, contribution of a variable to a factor. Based on review of the pattern (see Table 18) and structure matrices (see Table 19) there were limited differences for the OVIT-Individual factors as a whole. Certainly the order of the dimensions, and therefore strength of the loading on each factor, changed but generally resulted in the same outcomes. One of the variables (I15 - does the organisation check criminal records) moved from Factor 1 (in the pattern matrix) to Factor 3 in the structure matrix. From initial impressions it appears to fit more closely with the variables of Factor 1. Pett et al. (2003) recommend placing cross-loading items with the factor that is most closely related conceptually. However, for consistency and in this initial exploratory phase, results of the factors are taken from the structure matrix, which on the whole shares the same simple structure as the pattern matrix (Pett et al. 2003). Finally, a closer examination of both the pattern and structure matrices appears to reveal no evidence of variables acting as suppressors (Graham et al. 2003).

It is noted that in the OVIT-Individual, Factor 4 has only two items (I55 – people in the organisation maintain high ethical standards and I56 – people in the organisation demonstrate high integrity and honesty). Costello and Osborne (2005) recommended that a factor may be weak and unstable with less than three items. However, Yong and Pearce (2013) suggested two variables could be valid if the variables were highly correlated ($r > 0.7$) to each other but uncorrelated with other variables as is the case with these two variables. Based on this recommendation the factor is maintained for this exploratory stage.

Finally, the Factor Correlation Matrix (Table 20) was examined which presents the correlation coefficients between factors (Hair et al. 2010). The output suggests that for the OVIT-Individual there are relationships between factors and therefore independence cannot be assumed. This outcome also supports the use of the oblique (Promax) rather than orthogonal rotation (Hair et al. 2010). Clearly the correlations

between factors 1, 2, and 3, are strong. Factor 4 has a weak relationship with all the other factors. It is not clear, from this exploratory phase, why Factor 4's correlation with the other factors is low and negative in regards to Factor 1.

Table 20: The Final OVIT-Individual Factor Correlation Matrix.

Factor Correlation Matrix

Factor	1	2	3	4
1	1.000	.702	.690	-.133
2	.702	1.000	.606	.132
3	.690	.606	1.000	.129
4	-.133	.132	.129	1.000

Extraction Method: Maximum Likelihood.

Rotation Method: Promax with Kaiser Normalization.

4.4.3.4 Summary of EFA outcomes for the OVIT – Individual

Fifty-six OVIT-Individual items were subjected to the Maximum Likelihood extraction method with Oblique (Promax) rotation. The final EFA solution was achieved in 12 iterations of the full EFA process (i.e. checking KMO, Bartlett's test of sphericity, goodness of fit, communalities, variance explained, factor loadings, removal of items etc.) in order to determine the EFA of 'best-fit'. Four factors were extracted explaining 70.36% of the variance and 25 questions were retained. Reliability analyses of the full OVIT was sound ($\alpha = 0.98$). Based on the recommendation of Hair et al. (2010) reliability analysis on the OVIT-Individual and its four factors was also completed. Using the Cronbach's alpha the OVIT-Individual was determined to be internally consistent and reliable ($\alpha = 0.96$; see Table 21 and Figure 16).

Table 21: The OVIT-Individual Inventory.

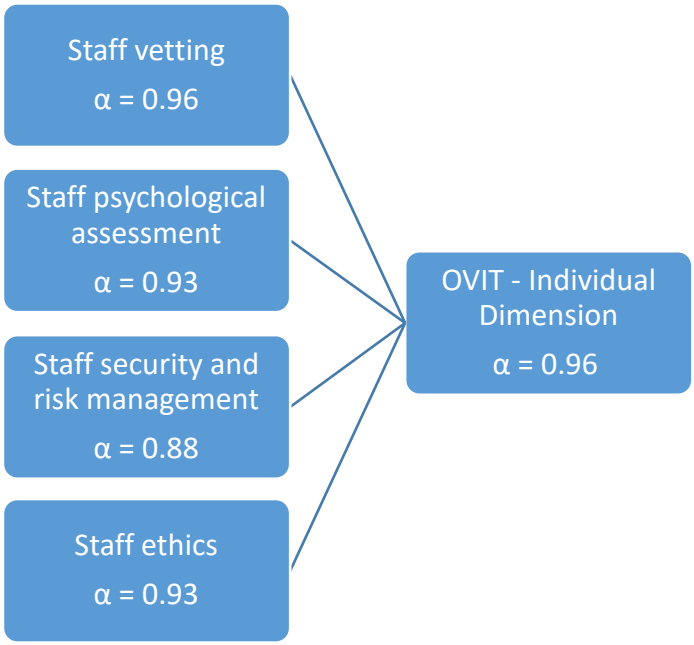
The OVIT (α = 0.98)
OVIT – INDIVIDUAL (α = 0.96)
Factor 1 – *Staff vetting (α = 0.96)*
1. does the organisation assess past substance use/abuse 2. does the organisation assess for problematic gambling behaviour 3. does the organisation monitor foreign contacts of staff 4. does the organisation have methods to identify financial pressures of employees 5. does the organisation assess financial, credit, and bankruptcy history 6. does the organisation evaluate risk-related criminal associations 7. does the organisation identify employees susceptible to social engineering (manipulation of people to get them to perform actions that do harm) 8. does the organisation employ trained professionals to identify and manage employees vulnerable to becoming an insider threat 9. the organisation has methods to assess for addictions 10. does the organisation test for illegal drug use
Factor 2 – *Staff psychological assessment (α = 0.93)*
11. does the organisation utilise methods to assess for employee resilience 12. does the organisation conduct personality testing to determine an employee's vulnerability to become an insider threat 13. does the organisation conduct mental health testing/assessment 14. does the organisation utilise methods to assess for employee self-awareness 15. does the organisation utilise methods to assess for employee conscientiousness 16. does the organisation utilise methods to assess for employee sound judgment 17. does the organisation utilise methods during recruitment processes to assess for ego/sense of entitlement
Factor 3 – *Staff security and risk management (α = 0.88)*
18. does the organisation have policy and processes to manage staff with a history of security violations 19. does the organisation undertake a formal risk assessment of high risk employees/positions 20. does the organisation have a means by which employees can report suspicious contacts from other employees or outsiders 21. does the organisation check civil records 22. does the organisation have methods to assess sound and reliable behaviour of staff 23. does the organisation check criminal records (on structure but factor 1 on pattern matrix)
Factor 4 – *Staff ethics (α = 0.93)*
24. people in the organisation maintain high ethical standards 25. people in the organisation demonstrate high integrity & honesty

Labelling of factors is subjective but should reflect the conceptual intent (Hooper 2012; Williams et al. 2010; Yong & Pearce 2013). Pett et al. (2003) recommended that the structure matrix is useful for naming factors. According to Field (2013) more important variables have greater loadings, and should be given more importance in the naming of factors. Given the subjective nature of labelling factors the final descriptors were discussed with one Delphi panel expert and the principal research

supervisor. This ensured conceptual, academic, and practical application of the factors in each of the OVIT sub-inventories. The four factors are named:

1. Staff vetting
2. Staff psychological assessment
3. Staff security and risk management
4. Staff ethics.

Figure 16: OVIT - Individual Dimension Factor Structure



Source: Developed for this study

4.4.3.5 OVIT – Organisational: Testing the assumptions

As per the OVIT-Individual, the OVIT-Organisational was subjected to the same testing of assumptions, beginning with a review of the Pearson Bivariate Correlation matrix. Again the correlation matrix determined coefficients above 0.30. A check for multi-collinearity indicated there were no correlations above 0.90 (as recommended by Yong & Pearce 2013).

The Bartlett's test of sphericity was significant (χ^2 (300) = 3347.24, p<0.000). The KMO test for sampling adequacy was 0.918 which is greater than the recommended 0.60 indicating the strength of the relationships as high (see Table 22).

Table 22: OVIT-Organisational KMO and Bartlett's Test.

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		0.918
Bartlett's Test of Sphericity	Approx. Chi-Square	7344.441
	df	1275
	Sig.	0.000

4.4.3.6 OVIT – Organisational: Extraction of factors

As previously explained this study combined a conceptual and evidence based approach to factor reduction based on review of the scree test, eigenvalues, and total variance explained. As can be seen by the final factor analysis results, the eigenvalues of the factors are above one (See Figure 17 and Table 23).

Figure 17: The Final OVIT-Organisational Scree Plot

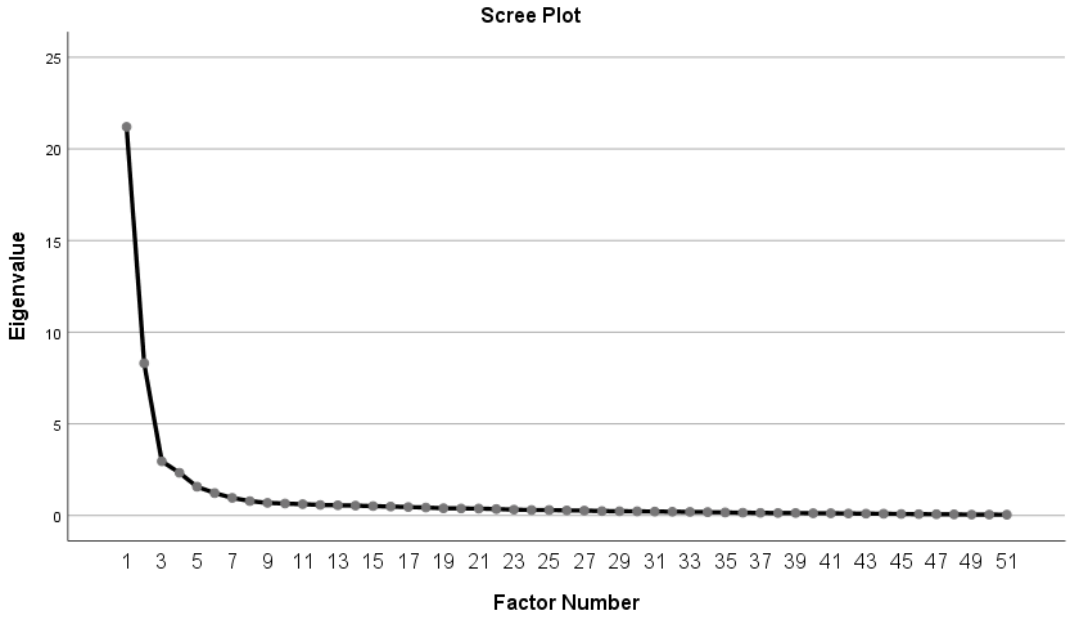


Table 23 shows that the total variance explained is 70.25% much greater than the recommended 60% (Hair et al. 2010).

Table 23: The Final OVIT–Organisational Eigenvalues.

Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings[a]
Factor	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total
1	21.204	41.576	41.576	20.860	40.902	40.902	16.137
2	8.306	16.286	57.862	8.066	15.815	56.717	14.311
3	2.955	5.793	63.655	2.672	5.240	61.957	10.129
4	2.333	4.574	68.229	2.040	4.000	65.957	4.679
5	1.570	3.078	71.307	1.264	2.479	68.437	14.968
6	1.221	2.393	73.701	0.926	1.815	70.251	9.029
7	0.960	1.883	75.584				
8	0.785	1.538	77.122				
9	0.686	1.345	78.467				
10	0.651	1.276	79.743				
11	0.620	1.216	80.958				
12	0.574	1.125	82.084				
13	0.557	1.092	83.176				
14	0.537	1.053	84.229				
15	0.511	1.001	85.230				
16	0.488	0.957	86.187				
17	0.461	0.903	87.091				
18	0.433	0.850	87.940				
19	0.395	0.774	88.714				
20	0.382	0.749	89.463				
21	0.375	0.736	90.199				
22	0.350	0.686	90.885				
23	0.319	0.625	91.510				
24	0.298	0.584	92.095				
25	0.296	0.581	92.676				
26	0.276	0.541	93.217				
27	0.267	0.523	93.740				
28	0.238	0.467	94.207				
29	0.230	0.451	94.658				
30	0.226	0.443	95.101				
31	0.215	0.421	95.522				
32	0.206	0.404	95.925				
33	0.198	0.388	96.313				
34	0.183	0.359	96.673				
35	0.166	0.325	96.997				
36	0.152	0.299	97.296				
37	0.142	0.279	97.575				
38	0.137	0.269	97.844				

39	0.135	0.265	98.110				
40	0.122	0.240	98.350				
41	0.120	0.236	98.585				
42	0.108	0.211	98.797				
43	0.097	0.191	98.988				
44	0.096	0.188	99.175				
45	0.079	0.156	99.331				
46	0.075	0.146	99.477				
47	0.070	0.137	99.614				
48	0.060	0.118	99.732				
49	0.049	0.097	99.828				
50	0.044	0.087	99.915				
51	0.043	0.085	100.000				

Extraction Method: Maximum Likelihood.

a. When factors are correlated, sums of squared loadings cannot be added to obtain a total variance.

Utilising three approaches to factor extraction (review of scree test, eigenvalues, and total variance explained) along with researcher judgment consistent with the conceptual underpinnings of the research, the final OVIT – Organisational factor solution resulted in six individual factors.

4.4.3.7 OVIT – Organisational: Factor rotation and interpretation

The Maximum Likelihood estimation procedure with oblique rotation (Promax) was utilised and the factor loadings, commonalties, and a check for cross-loading items in the pattern matrix was undertaken. Communalities below 0.40 were removed for the OVIT-Organisational. Item loadings below the recommended 0.40 were also removed.

Table 24: The Final OVIT–Organisational Communalities.

Communalities

	Initial	Extraction
O76. the organisation is open and honest with its employees	0.914	0.852
O52. management in the organisation do not hesitate to provide the leadership that is needed	0.877	0.798
O57. management in the organisation take care to be informed about how others think and feel about things	0.885	0.791
O56. management in the organisation provide the support and resources needed to help staff meet their goals	0.854	0.767
O58. management in the organisation encourage staff to speak up about employee issues	0.865	0.738
O62. the organisation has a positive organisational culture	0.843	0.765
O60. staff in the organisation are treated fairly by management in the organisation	0.841	0.734
O30. does the organisation structure allow for open and efficient communication across all levels	0.841	0.723
O17. does the organisation have strong and positive leadership	0.844	0.700
O63. both overt and covert messages are corrected to create a positive organisational culture	0.843	0.711
O77. management in the organisation encourage staff to participate in important decisions	0.796	0.750
O50. management in the organisation are accountable and responsible to others	0.805	0.665
O18. does management in the organisation communicate clear plans & objectives for the organisation	0.845	0.680
O48. the organisation is able to learn from failures and mistakes	0.816	0.721
O51. management in the organisation lead by example when it comes to security practice	0.827	0.712
O55. the values of the organisation are made explicit and help to build a strong security culture	0.756	0.641
O78. policies and expectations are consistent across all levels of the organisation	0.736	0.630
O74. the organisation balances trust with the application of consistent employee monitoring	0.807	0.676
O26. does the organisation commit to the prevention, detection, deterrence, and response to insider threats	0.884	0.809
O45. the organisation keeps abreast of best practice when it comes to insider threat	0.879	0.770
O25. does the organisation management integrate insider threat mitigation as part of the broader enterprise risk mitigation strategy	0.831	0.760
O14. does the organisation have an established insider threat contingency management plan	0.820	0.760
O12. does the organisation promote integrated approaches to insider threat management	0.842	0.745
O4. does the organisation have a specialised and multidisciplinary team to evaluate the risk of insider threat	0.832	0.761
O11. does the organisation have policies and processes to attempt to identify moles	0.835	0.725
O38. does the organisation regularly review and update insider threat and security policy and procedures	0.844	0.716
O1. does the organisation offer specific training and education programs addressing policy and practice areas relevant to insider threat	0.780	0.715

O2. does the organisation structure security awareness training and education efforts appropriately to the needs of different employees groups	0.751	0.634
O46. the organisation is good at addressing underlying systemic issues that may be linked to increased risk of insider threat	0.814	0.661
O39. does the organisation have policy to conduct random reviews of exiting staff computer activities leading up the final date	0.734	0.473
O13. does the organisation have a senior management position dedicated to security who answers to a Board member	0.749	0.564
O36. does the organisation have policies that protect the security of organisational information and IT resources	0.833	0.750
O42. does the organisation have policies protecting the physical security of facilities	0.791	0.663
O40. are policies and processes in place to ensure that the privileges and accesses of staff leaving the organisation are disabled	0.825	0.637
O37. does the organisation implement security practices to prevent unauthorised disclosure of sensitive information	0.811	0.669
O43. does the organisation review physical access anomalies and denials	0.783	0.672
O54. the organisation has a poor security culture	0.723	0.738
O66. when it comes to insider threat the organisation is complacent	0.805	0.760
O59. that, overall, staff of the organisation engage in poor security behaviour	0.653	0.646
O69. there is a lack of management of insider threat issues at the emerging stages	0.777	0.735
O80. staff are aware of the security controls utilised by the organisation	0.799	0.697
O79. security reporting is encouraged in the organisation	0.831	0.663
O84. security controls of the organisation are adequate and applied whenever necessary	0.787	0.658
O86. the organisation has a proactive and risk-based approach to mitigating emerging insider threats	0.833	0.730
O87. security awareness is high among staff	0.835	0.734
O85. staff in the organisation can identify and report on red flags	0.764	0.637
O83. the organisation is committed to improving security in order to protect its information and resources	0.816	0.663
O67. the organisation is aware of its risk tolerance level/risk appetite	0.691	0.561
O35. does the organisation have a whistle-blower protection policy	0.832	0.768
O34. does the organisation have confidential reporting so that employees can report suspicious events without fear of repercussion	0.795	0.690
O81. the organisation has a whistle-blower policy that has the confidence of all staff	0.756	0.612

Extraction Method: Maximum Likelihood.

A review of the communalities table reveals high communality results for the organisational variables. There is also no evidence of any Heywood cases.

The pattern matrix in Table 25 demonstrates a clean Pattern Matrix with six distinct factors and no suggestion of complex variables (items that crossload on to two or more factors).

Table 25: The Final OVIT – Organisational Pattern Matrix.

Pattern Matrix[a]

	Factor					
	1	2	3	4	5	6
O76. the organisation is open and honest with its employees	1.018					
O57. management in the organisation take care to be informed about how others think and feel about things	0.987					
O60. staff in the organisation are treated fairly by management in the organisation	0.927					
O52. management in the organisation do not hesitate to provide the leadership that is needed	0.908					
O30. does the organisation structure allow for open and efficient communication across all levels	0.886					
O58. management in the organisation encourage staff to speak up about employee issues	0.884					
O62. the organisation has a positive organisational culture	0.874					
O56. management in the organisation provide the support and resources needed to help staff meet their goals	0.864					
O50. management in the organisation are accountable and responsible to others	0.847					
O17. does the organisation have strong and positive leadership	0.812					
O63. both overt and covert messages are corrected to create a positive organisational culture	0.801					
O77. management in the organisation encourage staff to participate in important decisions	0.762					
O18. does management in the organisation communicate clear plans & objectives for the organisation	0.743					
O48. the organisation is able to learn from failures and mistakes	0.694					
O78. policies and expectations are consistent across all levels of the organisation	0.675					
O51. management in the organisation lead by example when it comes to security practice	0.631					
O74. the organisation balances trust with the application of consistent employee monitoring	0.625					
O55. the values of the organisation are made explicit and help to build a strong security culture	0.501					
O11. does the organisation have policies and processes to attempt to identify moles		0.996				
O4. does the organisation have a specialised and multidisciplinary team to evaluate the risk of insider threat		0.936				
O12. does the organisation promote integrated approaches to insider threat management		0.895				

O14. does the organisation have an established insider threat contingency management plan		0.850				
O1. does the organisation offer specific training and education programs addressing policy and practice areas relevant to insider threat		0.840				
O45. the organisation keeps abreast of best practice when it comes to insider threat		0.824				
O25. does the organisation management integrate insider threat mitigation as part of the broader enterprise risk mitigation strategy		0.814				
O26. does the organisation commit to the prevention, detection, deterrence, and response to insider threats		0.795				
O2. does the organisation structure security awareness training and education efforts appropriately to the needs of different employees groups		0.661				
O13. does the organisation have a senior management position dedicated to security who answers to a Board member		0.655				
O38. does the organisation regularly review and update insider threat and security policy and procedures		0.609				
O46. the organisation is good at addressing underlying systemic issues that may be linked to increased risk of insider threat		0.591				
O39. does the organisation have policy to conduct random reviews of exiting staff computer activities leading up the final date		0.499				
O36. does the organisation have policies that protect the security of organisational information and IT resources			0.749			
O42. does the organisation have policies protecting the physical security of facilities			0.729			
O40. are policies and processes in place to ensure that the privileges and accesses of staff leaving the organisation are disabled			0.687			
O37. does the organisation implement security practices to prevent unauthorised disclosure of sensitive information			0.666			
O43. does the organisation review physical access anomalies and denials			0.580			
O54. the organisation has a poor security culture				0.835		
O59. that, overall, staff of the organisation engage in poor security behaviour				0.782		
O69. there is a lack of management of insider threat issues at the emerging stages				0.752		
O66. when it comes to insider threat the organisation is complacent				0.728		
O80. staff are aware of the security controls utilised by the organisation					0.775	
O84. security controls of the organisation are adequate and applied whenever necessary					0.675	
O87. security awareness is high among staff					0.624	

O85. staff in the organisation can identify and report on red flags					0.620	
O83. the organisation is committed to improving security in order to protect its information and resources					0.605	
O86. the organisation has a proactive and risk-based approach to mitigating emerging insider threats					0.593	
O79. security reporting is encouraged in the organisation					0.554	
O67. the organisation is aware of its risk tolerance level/risk appetite					0.434	
O35. does the organisation have a whistle-blower protection policy						0.834
O81. the organisation has a whistle-blower policy that has the confidence of all staff						0.626
O34. does the organisation have confidential reporting so that employees can report suspicious events without fear of repercussion						0.571

Extraction Method: Maximum Likelihood.
Rotation Method: Promax with Kaiser Normalization.
a. Rotation converged in 7 iterations.

Note: Factor loadings < 0.4 are suppressed to assist in determining crossloading and high loading items

The structure matrix (Table 26) was contrasted and compared with the pattern matrix (Table 25). Limited differences were observed in these matrices. There was some change in the hierarchy of the items of each factor, but all of the items remained the same between both matrices. There was also no evidence of suppressor variables.

Table 26: The Final OVIT – Organisational Structure Matrix.

Structure Matrix

	Factor					
	1	2	3	4	5	6
O76. the organisation is open and honest with its employees	**0.900**	0.070	0.218	-0.192	0.379	0.296
O52. management in the organisation do not hesitate to provide the leadership that is needed	**0.886**	0.233	0.411	-0.211	0.492	0.304
O57. management in the organisation take care to be informed about how others think and feel about things	**0.879**	0.162	0.285	-0.118	0.407	0.303
O56. management in the organisation provide the support and resources needed to help staff meet their goals	**0.863**	0.163	0.436	-0.158	0.468	0.283
O58. management in the organisation encourage staff to speak up about employee issues	**0.849**	0.140	0.296	-0.238	0.456	0.261

O62. the organisation has a positive organisational culture	**0.847**	0.087	0.162	-0.134	0.460	0.343
O60. staff in the organisation are treated fairly by management in the organisation	**0.845**	0.152	0.232	-0.110	0.407	0.342
O30. does the organisation structure allow for open and efficient communication across all levels	**0.833**	0.184	0.414	-0.123	0.428	0.240
O17. does the organisation have strong and positive leadership	**0.830**	0.174	0.396	-0.178	0.453	0.343
O63. both overt and covert messages are corrected to create a positive organisational culture	**0.830**	0.312	0.312	-0.199	0.517	0.453
O77. management in the organisation encourage staff to participate in important decisions	**0.825**	0.132	0.194	-0.091	0.550	0.383
O18. does management in the organisation communicate clear plans & objectives for the organisation	**0.812**	0.223	0.441	-0.150	0.500	0.372
O50. management in the organisation are accountable and responsible to others	**0.805**	0.193	0.364	-0.208	0.399	0.305
O48. the organisation is able to learn from failures and mistakes	**0.796**	0.294	0.580	-0.159	0.543	0.306
O51. management in the organisation lead by example when it comes to security practice	**0.789**	0.351	0.545	-0.251	0.623	0.334
O78. policies and expectations are consistent across all levels of the organisation	**0.761**	0.265	0.220	-0.181	0.567	0.398
O74. the organisation balances trust with the application of consistent employee monitoring	**0.753**	0.385	0.226	-0.228	0.605	0.528
O55. the values of the organisation are made explicit and help to build a strong security culture	**0.714**	0.378	0.565	-0.256	0.629	0.344
O26. does the organisation commit to the prevention, detection, deterrence, and response to insider threats	0.272	**0.888**	0.472	-0.319	0.576	0.497
O45. the organisation keeps abreast of best practice when it comes to insider threat	0.303	**0.871**	0.399	-0.276	0.573	0.487
O25. does the organisation management integrate insider threat mitigation as part of the broader enterprise risk mitigation strategy	0.217	**0.867**	0.379	-0.246	0.512	0.525
O14. does the organisation have an established insider threat contingency management plan	0.200	**0.866**	0.402	-0.307	0.478	0.462
O12. does the organisation promote integrated approaches to insider threat management	0.113	**0.854**	0.348	-0.199	0.468	0.382
O4. does the organisation have a specialised and multidisciplinary team to evaluate the risk of insider threat	0.080	**0.851**	0.384	-0.204	0.401	0.350
O11. does the organisation have policies and processes to attempt to identify moles	0.166	**0.833**	0.300	-0.195	0.375	0.345

O38. does the organisation regularly review and update insider threat and security policy and procedures	0.306	**0.808**	0.418	-0.321	0.551	0.624
O1. does the organisation offer specific training and education programs addressing policy and practice areas relevant to insider threat	0.151	**0.803**	0.161	-0.091	0.500	0.442
O46. the organisation is good at addressing underlying systemic issues that may be linked to increased risk of insider threat	0.478	**0.739**	0.338	-0.296	0.585	0.584
O2. does the organisation structure security awareness training and education efforts appropriately to the needs of different employees groups	0.248	**0.739**	0.206	-0.105	0.581	0.466
O13. does the organisation have a senior management position dedicated to security who answers to a Board member	0.150	**0.719**	0.445	-0.246	0.465	0.311
O39. does the organisation have policy to conduct random reviews of exiting staff computer activities leading up the final date	0.295	**0.639**	0.455	-0.137	0.489	0.421
O36. does the organisation have policies that protect the security of organisational information and IT resources	0.429	0.386	**0.824**	-0.068	0.546	0.423
O42. does the organisation have policies protecting the physical security of facilities	0.298	0.448	**0.787**	-0.047	0.474	0.330
O40. are policies and processes in place to ensure that the privileges and accesses of staff leaving the organisation are disabled	0.445	0.388	**0.780**	-0.127	0.486	0.295
O37. does the organisation implement security practices to prevent unauthorised disclosure of sensitive information	0.365	0.499	**0.773**	-0.223	0.539	0.413
O43. does the organisation review physical access anomalies and denials	0.326	0.603	**0.737**	-0.216	0.565	0.423
O54. the organisation has a poor security culture	-0.238	-0.180	-0.175	**0.833**	-0.340	-0.192
O66. when it comes to insider threat the organisation is complacent	-0.071	-0.469	0.039	**0.788**	-0.193	-0.312
O69. there is a lack of management of insider threat issues at the emerging stages	-0.120	-0.315	0.136	**0.783**	-0.142	-0.334
O59. that, overall, staff of the organisation engage in poor security behaviour	-0.254	-0.030	-0.214	**0.742**	-0.241	-0.102
O80. staff are aware of the security controls utilised by the organisation	0.413	0.543	0.493	-0.258	**0.822**	0.428
O79. security reporting is encouraged in the organisation	0.557	0.560	0.472	-0.227	**0.788**	0.497
O86. the organisation has a proactive and risk-based approach to mitigating emerging insider threats	0.405	0.710	0.333	-0.316	**0.783**	0.532
O84. security controls of the organisation are adequate and applied whenever necessary	0.473	0.460	0.577	-0.243	**0.779**	0.359
O85. staff in the organisation can identify and report on red flags	0.444	0.574	0.494	-0.255	**0.775**	0.410
O87. security awareness is high among staff	0.361	0.658	0.505	-0.376	**0.769**	0.299

O83. the organisation is committed to improving security in order to protect its information and resources	0.492	0.476	0.615	-0.198	**0.760**	0.304
O67. the organisation is aware of its risk tolerance level/risk appetite	0.524	0.525	0.497	-0.199	**0.705**	0.400
O35. does the organisation have a whistle-blower protection policy	0.289	0.513	0.431	-0.255	0.382	**0.820**
O81. the organisation has a whistle-blower policy that has the confidence of all staff	0.439	0.478	0.390	-0.277	0.515	**0.742**
O34. does the organisation have confidential reporting so that employees can report suspicious events without fear of repercussion	0.497	0.505	0.556	-0.168	0.571	**0.722**

Extraction Method: Maximum Likelihood. Rotation Method: Promax with Kaiser Normalization.

The results of the Factor Correlation Matrix (Table 27) suggest that there are moderate relationships between factors and therefore independence cannot be assumed. This outcome again supports the use of the oblique (Promax) rather than orthogonal rotation (Hair et al. 2010).

Table 27: The Final OVIT-Organisational Factor Correlation Matrix.

Factor Correlation Matrix

Factor	1	2	3	4	5	6
1	1.000	.240	.395	-.206	.574	.406
2	.240	1.000	.399	-.295	.579	.537
3	.395	.399	1.000	-.134	.498	.243
4	-.206	-.295	-.134	1.000	-.266	-.238
5	.574	.579	.498	-.266	1.000	.502
6	.406	.537	.243	-.238	.502	1.000

Extraction Method: Maximum Likelihood.

Rotation Method: Promax with Kaiser Normalization.

4.4.3.8 Summary of EFA outcomes for the OVIT – Organisational

Ninety OVIT-Organisational items were subjected to the Maximum Likelihood extraction method with Oblique (Promax) rotation in order to determine the EFA of 'best-fit'. The final EFA solution was achieved in nine iterations of the full EFA process (i.e. checking KMO, Bartlett's test of sphericity, goodness of fit, communalities, variance explained, factor loadings, removal of items etc.). The best result for this preliminary stage was achieved when the factor analysis was forced to six factors. These six factors explained 70.25% of the variance and a total of 51 questions were

retained. Before completing reliability analysis on the OVIT-Organisational, four questions required reverse scoring in SPSS (whereby a response on the Likert scale of 1 became a 5, 2 became a 4, 3 remained the same, 4 became a 2, and 5 became a 1). The following questions were reverse scored:

- O54. the organisation has a poor security culture
- O59. that, overall, staff of the organisation engage in poor security behaviour
- O66. when it comes to insider threat the organisation is complacent
- O69. there is a lack of management of insider threat issues at the emerging stages

Reliability analyses on the full OVIT-Organisational and its six factors were then completed. Using the Cronbach's alpha the OVIT-Organisational inventory was determined to be internally consistent and reliable with an alpha of 0.98 which is well above the recommended 0.60 benchmark (see Table 28 and Figure 18).

Table 28: The OVIT-Organisational Inventory.

The OVIT (α = 0.98)
OVIT – ORGANISATIONAL (α = 0.98)
Factor 1 – *Organisational culture and leadership (α = 0.97)*
1. the organisation is open and honest with its employees 2. management in the organisation do not hesitate to provide the leadership that is needed 3. management in the organisation take care to be informed about how others think and feel about things 4. management in the organisation provide the support and resources needed to help staff meet their goals 5. management in the organisation encourage staff to speak up about employee issues 6. the organisation has a positive organisational culture 7. staff in the organisation are treated fairly by management in the organisation 8. does the organisation structure allow for open and efficient communication across all levels 9. does the organisation have strong and positive leadership 10. both overt and covert messages are corrected to create a positive organisational culture 11. management in the organisation encourage staff to participate in important decisions 12. does management in the organisation communicate clear plans & objectives for the organisation 13. management in the organisation are accountable and responsible to others 14. the organisation is able to learn from failures and mistakes 15. management in the organisation lead by example when it comes to security practice 16. policies and expectations are consistent across all levels of the organisation 17. the organisation balances trust with the application of consistent employee monitoring 18. the values of the organisation are made explicit and help to build a strong security culture
Factor 2 – *Insider threat initiatives (α = 0.96)*
19. does the organisation commit to the prevention, detection, deterrence, and response to insider threats

20. the organisation keeps abreast of best practice when it comes to insider threat
21. does the organisation management integrate insider threat mitigation as part of the broader enterprise risk mitigation strategy
22. does the organisation have an established insider threat contingency management plan
23. does the organisation promote integrated approaches to insider threat management
24. does the organisation have a specialised and multidisciplinary team to evaluate the risk of insider threat
25. does the organisation have policies and processes to attempt to identify moles
26. does the organisation regularly review and update insider threat and security policy and procedures
27. does the organisation offer specific training and education programs addressing policy and practice areas relevant to insider threat
28. the organisation is good at addressing underlying systemic issues that may be linked to increased risk of insider threat
29. does the organisation structure security awareness training and education efforts appropriately to the needs of different employees groups
30. does the organisation have policy to conduct random reviews of exiting staff computer activities leading up the final date (check loading as not showing on pattern matrix)
31. does the organisation have a senior management position dedicated to security who answers to a Board member

Factor 3 – *Organisational protection (α = 0.91)*

32. does the organisation have policies that protect the security of organisational information and IT resources
33. does the organisation have policies protecting the physical security of facilities
34. are policies and processes in place to ensure that the privileges and accesses of staff leaving the organisation are disabled
35. does the organisation implement security practices to prevent unauthorised disclosure of sensitive information
36. does the organisation review physical access anomalies and denials

Factor 4 – *Organisational complacency (α = 0.85)*

37. the organisation has a poor security culture
38. when it comes to insider threat the organisation is complacent
39. there is a lack of management of insider threat issues at the emerging stages
40. that, overall, staff of the organisation engage in poor security behaviour

Factor 5 – *Organisational security awareness (α = 0.93)*

41. staff are aware of the security controls utilised by the organisation
42. security reporting is encouraged in the organisation
43. the organisation has a proactive and risk-based approach to mitigating emerging insider threats
44. security controls of the organisation are adequate and applied whenever necessary
45. staff in the organisation can identify and report on red flags
46. security awareness is high among staff
47. the organisation is committed to improving security in order to protect its information and resources
48. the organisation is aware of its risk tolerance level/risk appetite (check value as dropped off pattern matrix but is showing)

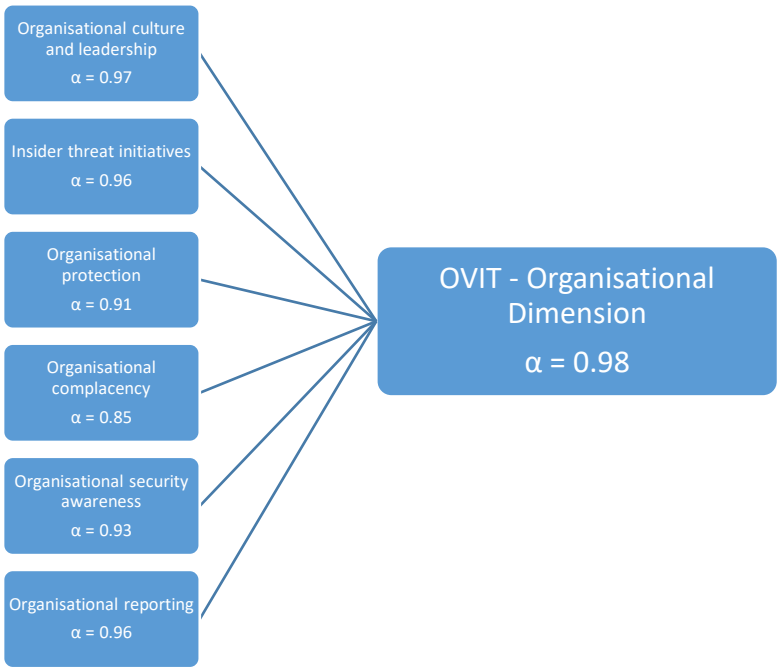
Factor 6 – *Organisational reporting (α = 0.96)*

49. does the organisation have a whistle-blower protection policy
50. the organisation has a whistle-blower policy that has the confidence of all staff
51. does the organisation have confidential reporting exist so that employees can report suspicious events without fear of repercussion

The factors were labelled and the final descriptors were discussed with the research supervisor to reduce subjectivity. The factors were named as:

1. Organisational culture and leadership
2. Insider threat initiatives
3. Organisational protection
4. Organisational complacency
5. Organisational security awareness
6. Organisational reporting.

Figure 18: OVIT – Organisational Dimension Factor Structure



Source: Developed for this study

4.4.3.9 OVIT – Technical: Testing the assumptions

The OVIT-Technical was subjected to the same test of assumptions as the OVIT-Individual and the OVIT-Organisational. The Pearson Bivariate Correlation matrix was above 0.30 and below 0.90.

The Bartlett's test of sphericity was significant (χ^2 (190) = 2617.91, p<0.000). The KMO test for sampling adequacy was 0.908 which is greater than the recommended 0.60 (see Table 29).

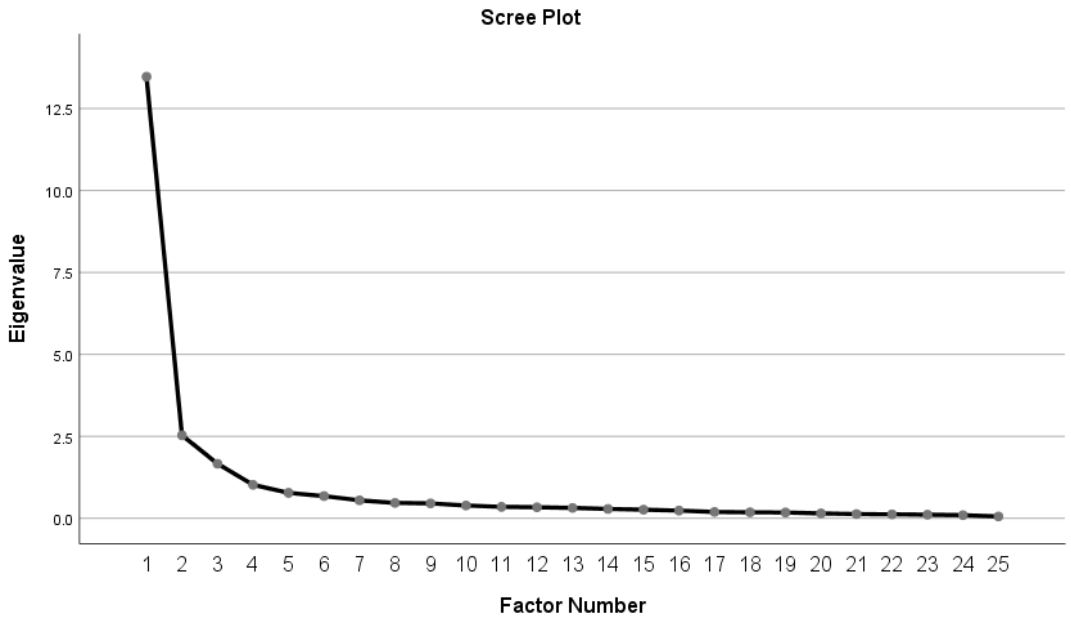
Table 29: The OVIT-Technical KMO and Bartlett's Test.

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		0.908
Bartlett's Test of Sphericity	Approx. Chi-Square	2617.911
	df	190
	Sig.	0.000

4.4.3.10 OVIT – Technical: Extraction of factors

As previously explained this study combined a conceptual and evidence based approach to factor reduction based on review of the scree test (see Figure 19), eigenvalues, and total variance explained (see Table 30). The eigenvalues of the factors were above 1 and the total variance explained was 68.22%, much greater than the recommended 60% (Hair et al. 2010).

Figure 19: The Final OVIT-Technical Scree Plot



Utilising these three approaches to factor extraction, along with researcher judgment consistent with the theoretical and conceptual underpinnings of the research, the final OVIT – Technical factor solution resulted in three individual factors.

Table 30: The Final OVIT–Technical Eigenvalues.

Total Variance Explained

Factor	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings[a]
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total
1	11.093	55.465	55.465	10.725	53.623	53.623	9.666
2	2.150	10.751	66.215	1.854	9.272	62.895	9.079
3	1.350	6.752	72.967	1.065	5.326	68.221	5.389
4	0.780	3.898	76.865				
5	0.660	3.301	80.166				
6	0.548	2.742	82.908				
7	0.535	2.673	85.581				
8	0.427	2.134	87.715				
9	0.413	2.064	89.779				
10	0.353	1.765	91.544				
11	0.280	1.402	92.946				
12	0.264	1.322	94.268				
13	0.200	1.001	95.269				
14	0.190	0.949	96.218				
15	0.177	0.885	97.102				
16	0.158	0.789	97.892				
17	0.146	0.731	98.623				
18	0.107	0.533	99.155				
19	0.091	0.455	99.610				
20	0.078	0.390	100.000				

Extraction Method: Maximum Likelihood.

a. When factors are correlated, sums of squared loadings cannot be added to obtain a total variance.

4.4.3.11 OVIT – Technical: Factor rotation and interpretation

The Maximum Likelihood estimation procedure with oblique rotation (Promax) was applied to OVIT-Technical. Communalities below 0.40 were removed. Item loadings below the recommended 0.40 were also removed.

Table 31: The Final OVIT–Technical Communalities.

Communalities

	Initial	Extraction
T12. does the organisation monitor common data exfiltration methods (e-mail, removable media) to identify anomalous behaviour	0.836	0.826
T13. does the organisation collect and monitor network traffic and security logs for anomalies	0.837	0.833
T14. does the organisation monitor key databases, data access and movement	0.821	0.819
T16. does the organisation have means to monitor trends in IT policy breaches to inform corrective action	0.833	0.785
T10. does the organisation implement random auditing of IT use implemented	0.783	0.711
T15. does the organisation use modern technologies to assist insider threat detection, deterrence, prevention and reporting	0.779	0.690
T9. does the organisation use advanced analytics tools to analyse and report on insider threat	0.779	0.683
T21. does the organisation use regular penetration testing to strengthen defences	0.732	0.595
T7. does the organisation restrict administrators from controlling auditing functions	0.768	0.752
T8. does the organisation conduct routine auditing of privileged functions	0.833	0.761
T6. does the organisation require multiple users to action all modifications to critical systems, network, applications, and data	0.709	0.709
T5. does the organisation ensure access to sensitive systems and areas enforced by authentication procedures are monitored for anomalies	0.792	0.692
T4. does the organisation ensure authentication procedures become more advanced with increasing access to critical information/data	0.709	0.627
T2. does the organisation have guidelines to ensure that staff only have access to data, systems, and information required to perform their duties	0.633	0.543
T3. does the organisation implement multi-factor authentication	0.603	0.489
T22. does the organisation hire technically sophisticated system administrators or programmers	0.657	0.471
T27. does the organisation employ special authentication procedures employed for database administrators	0.742	0.739
T25. does the organisation review access request denials	0.712	0.699
T24. does the organisation have a clear list of access privileges for all roles	0.694	0.655
T26. does the organisation ensure computing equipment connected to the corporate network of the organisation reside in an area that has electronic access controls in place (i.e.- requires a swipe card to access)	0.675	0.566

Extraction Method: Maximum Likelihood.

A review of the communalities in Table 31 reveals high communality results for the technical variables. There is also no evidence of any Heywood cases.

A check for cross-loading items in the pattern matrix was then undertaken. The pattern matrix in Table 32 demonstrates a clean Pattern Matrix with three distinct factors and no suggestion of complex variables. One item fell just below 0.4 at 0.395

(T22 - does the organisation hire technically sophisticated system administrators or programmers), but was retained based on theoretical considerations at this exploratory stage. This item was also within the minimum guidelines of 0.3 (Hair et al. 2010; Tabachnick & Fidell 2007).

Table 32: The Final OVIT – Technical Pattern Matrix.

Pattern Matrix[a]

	Factor		
	1	2	3
T13. does the organisation collect and monitor network traffic and security logs for anomalies	1.016		
T12. does the organisation monitor common data exfiltration methods (e-mail, removable media) to identify anomalous behaviour	1.000		
T14. does the organisation monitor key databases, data access and movement	0.952		
T10. does the organisation implement random auditing of IT use implemented	0.774		
T16. does the organisation have means to monitor trends in IT policy breaches to inform corrective action	0.722		
T15. does the organisation use modern technologies to assist insider threat detection, deterrence, prevention and reporting	0.690		
T9. does the organisation use advanced analytics tools to analyse and report on insider threat	0.677		
T21. does the organisation use regular penetration testing to strengthen defences	0.529		
T7. does the organisation restrict administrators from controlling auditing functions		0.884	
T6. does the organisation require multiple users to action all modifications to critical systems, network, applications, and data		0.883	
T2. does the organisation have guidelines to ensure that staff only have access to data, systems, and information required to perform their duties		0.828	
T4. does the organisation ensure authentication procedures become more advanced with increasing access to critical information/data		0.707	
8. does the organisation conduct routine auditing of privileged functions		0.613	
T3. does the organisation implement multi-factor authentication		0.524	
T5. does the organisation ensure access to sensitive systems and areas enforced by authentication procedures are monitored for anomalies		0.523	
T22. does the organisation hire technically sophisticated system administrators or programmers	*0.395*		
T27. does the organisation employ special authentication procedures employed for database administrators			0.881
T25. does the organisation review access request denials			0.856
T24. does the organisation have a clear list of access privileges for all roles			0.821
T26. does the organisation ensure computing equipment connected to the corporate network of the organisation reside in an area that has electronic access controls in place (i.e.- requires a swipe card to access)			0.617

Extraction Method: Maximum Likelihood.
Rotation Method: Promax with Kaiser Normalization.[a]
a. Rotation converged in 6 iterations.

Note: Factor loadings < 0.4 are suppressed to assist in determining crossloading and high loading items

The structure matrix (Table 33) of the OVIT-Technical was contrasted and compared with the pattern matrix (Table 32). Based on review of these matrices there were limited differences observed. There was some change in the hierarchy of the items of each factor, but all the same items remained the same between both matrices. There was also no evidence of suppressor variables.

Table 33: The Final OVIT – Technical Structure Matrix.

Structure Matrix

	Factor		
	1	2	3
T12. does the organisation monitor common data exfiltration methods (e-mail, removable media) to identify anomalous behaviour	**0.905**	0.623	0.381
T13. does the organisation collect and monitor network traffic and security logs for anomalies	**0.904**	0.598	0.449
T14. does the organisation monitor key databases, data access and movement	**0.901**	0.635	0.453
T16. does the organisation have means to monitor trends in IT policy breaches to inform corrective action	**0.874**	0.748	0.409
T10. does the organisation implement random auditing of IT use implemented	**0.839**	0.671	0.373
T15. does the organisation use modern technologies to assist insider threat detection, deterrence, prevention and reporting	**0.819**	0.696	0.367
T9. does the organisation use advanced analytics tools to analyse and report on insider threat	**0.813**	0.697	0.359
T21. does the organisation use regular penetration testing to strengthen defences	**0.748**	0.680	0.433
T7. does the organisation restrict administrators from controlling auditing functions	0.647	**0.865**	0.377
T8. does the organisation conduct routine auditing of privileged functions	0.777	**0.842**	0.401
T6. does the organisation require multiple users to action all modifications to critical systems, network, applications, and data	0.601	**0.841**	0.415
T5. does the organisation ensure access to sensitive systems and areas enforced by authentication procedures are monitored for anomalies	0.745	**0.799**	0.480
T4. does the organisation ensure authentication procedures become more advanced with increasing access to critical information/data	0.633	**0.789**	0.413
T2. does the organisation have guidelines to ensure that staff only have access to data, systems, and information required to perform their duties	0.485	**0.731**	0.359
T3. does the organisation implement multi-factor authentication	0.597	**0.686**	0.397
T22. does the organisation hire technically sophisticated system administrators or programmers	0.531	**0.618**	0.559
T27. does the organisation employ special authentication procedures employed for database administrators	0.370	0.394	**0.859**
T25. does the organisation review access request denials	0.376	0.373	**0.835**
T24. does the organisation have a clear list of access privileges for all roles	0.314	0.398	**0.804**
T26. does the organisation ensure computing equipment connected to the corporate network of the organisation reside in an area that has electronic access controls in place (i.e.- requires a swipe card to access)	0.519	0.474	**0.724**

Extraction Method: Maximum Likelihood. Rotation Method: Promax with Kaiser Normalization.

The Factor Correlation Matrix was examined (Table 34). The results indicated moderate to high relationships between factors and therefore independence cannot be assumed. This outcome supports the use of the oblique (Promax) rather than orthogonal rotation (Hair et al. 2010).

Table 34: The Final OVIT-Technical Factor Correlation Matrix.

Factor Correlation Matrix

Factor	1	2	3
1	1.000	.746	.467
2	.746	1.000	.493
3	.467	.493	1.000

Extraction Method: Maximum Likelihood.
Rotation Method: Promax with Kaiser Normalization.

4.4.3.12 Summary of EFA outcomes for the OVIT - Technical

Twenty-seven OVIT-Technical items were subjected to the Maximum Likelihood extraction method with Oblique (Promax) rotation. In order to determine the EFA of 'best-fit, 'final EFA solution was achieved in seven iterations of the full EFA process (i.e. checking KMO, Bartlett's test of sphericity, goodness of fit, communalities, variance explained, factor loadings, removal of items etc.). Three factors were extracted explaining 68.22% of the variance and 20 questions were retained in the OVIT - Technical. Reliability analyses on the full OVIT-Technical and its three factors were completed. Using the Cronbach's alpha the OVIT-Technical was determined to be internally consistent and reliable ($\alpha = 0.95$, see Table 35 and Figure 20).

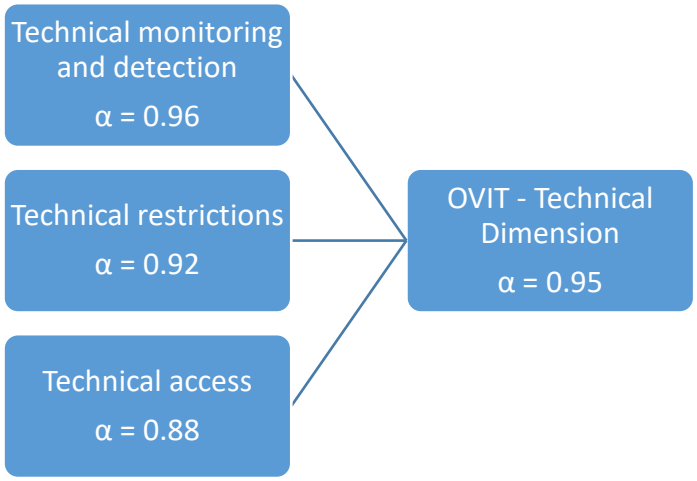
Table 35: The OVIT-Technical Inventory.

The OVIT (α = 0.98)
OVIT – TECHNICAL (α = 0.95)
Factor 1 – *Technical monitoring and detection (α = 0.96)*
1. does the organisation monitor common data exfiltration methods (e-mail, removable media) to identify anomalous behaviour 2. does the organisation collect and monitor network traffic and security logs for anomalies 3. does the organisation monitor key databases, data access and movement 4. does the organisation have means to monitor trends in IT policy breaches to inform corrective action 5. does the organisation implement random auditing of IT use implemented 6. does the organisation use modern technologies to assist insider threat detection, deterrence, prevention and reporting 7. does the organisation use advanced analytics tools to analyse and report on insider threat 8. does the organisation use regular penetration testing to strengthen defences
Factor 2 – *Technical restrictions (α = 0.92)*
9. does the organisation restrict administrators from controlling auditing functions 10. does the organisation conduct routine auditing of privileged functions 11. does the organisation require multiple users to action all modifications to critical systems, network, applications, and data 12. does the organisation ensure access to sensitive systems and areas enforced by authentication procedures are monitored for anomalies 13. does the organisation ensure authentication procedures become more advanced with increasing access to critical information/data 14. does the organisation have guidelines to ensure that staff only have access to data, systems, and information required to perform their duties 15. does the organisation implement multi-factor authentication 16. does the organisation hire technically sophisticated system administrators or programmers
Factor 3 – *Technical access (α = 0.88)*
17. does the organisation employ special authentication procedures employed for database administrators 18. does the organisation review access request denials 19. does the organisation have a clear list of access privileges for all roles 20. does the organisation ensure computing equipment connected to the corporate network of the organisation reside in an area that has electronic access controls in place (i.e.- requires a swipe card to access)

The technical factors were labelled and the final descriptors were discussed with the research supervisor to reduce subjectivity. The factors were names as:

1. Technical monitoring and detection
2. Technical restrictions
3. Technical access.

Figure 20: OVIT – Technical Dimension Factor Structure



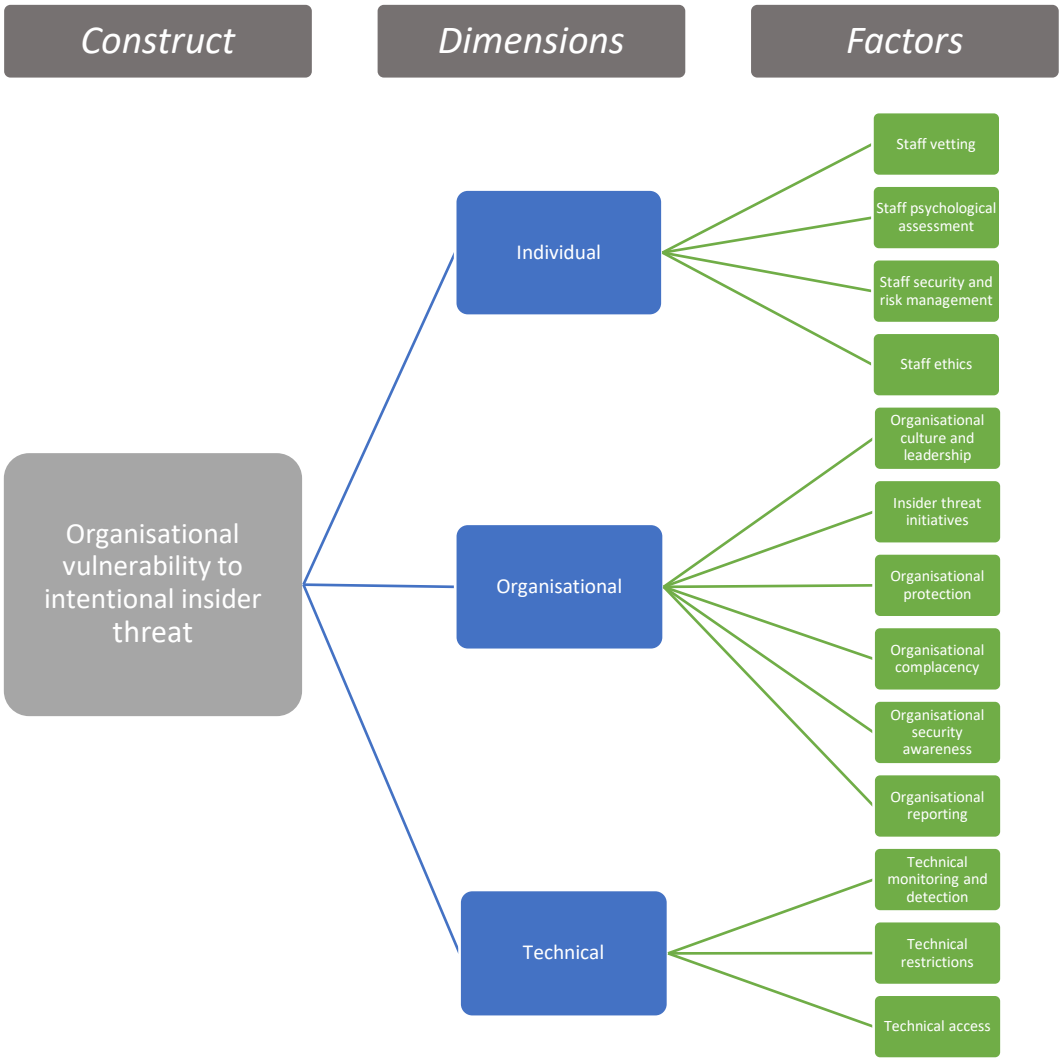
Source: Developed for this study

4.5 Operationalising Organisational Vulnerability to Intentional Insider Threat

The EFA process determined that the OVIT and its sub-inventories are statistically robust. From the outcomes of the EFA a framework for understanding organisational vulnerability to IIT has been determined. The construct of IIT is represented by the three dimensions; individual, organisational, and technical. These dimensions breakdown further in to 13 factors (see Figure 21).

The development of the OVIT framework is significant especially in terms of the gaps identified in the literature review surrounding insider threat (see Chapter 1). Band et al. (2006) encouraged a more rigorous focus on organisational predispositions and vulnerabilities. The OVIT framework addresses the importance of individual and technical factors, but also the organisational factors of influence which have been largely ignored or undervalued. The OVIT framework reflects where organisations may improve the organisational environment, thereby reducing inappropriate insider action and exploitation.

Figure 21: The OVIT Framework and factor structure of individual, organisational, and technical dimensions



Source: Developed for this research.

The OVIT framework compliments the existing models and frameworks on insider threat. However, it also presents a completely original model to the theory. Unlike previous models the OVIT challenges the 'attack-focus', prominence of insider attributes and actions, and prediction and detection. Instead, the OVIT framework identifies multi-dimensional areas where organisations can reduce vulnerability to IIT in a way that is not cumbersome or challenging for practitioners to use. From an applied perspective the potential for the OVIT framework to provide predictive or protective outcomes also addresses the limitation in current practice towards

reactive and detection focused solutions (Greitzer & Hohimer 2011; Greitzer et al. 2009).

4.6 Summary

The focus of the current thesis is to operationalise the key constructs of organisational vulnerability to IIT. This was achieved through three research phases ultimately attempting to define, describe, and validate the construct of organisational vulnerability to IIT.

Part One – Defining IIT

The definition of organisational vulnerability to IIT was built around a thematic analysis of the extant literature which aided the determination of pertinent aspects of IIT. The literature review provided an understanding of the many factors associated with the construct of IIT vulnerability. A significant number of items were identified to increase, decrease, and mitigate or moderate IIT based on the extant literature. A synthesis of the literature review and content analysis revealed a simple set relationship between three dimensions of IIT being individual, organisational, and technical dimensions.

Through a Delphi study expert panel members were presented with factors and variables of intentional insider threat from the literature. The Delphi panel also provided additional critical items relevant to IIT. As such the Delphi process was able to build upon the literature review and determine an Australian definition of IIT (see below) as well as demonstrate the most pertinent measures of IIT; those critical to increasing, decreasing, and moderating IIT (see Tables 7, 8, 9, and 10 above).

> *Intentional insider threat is when a person of trust (employee, contractor, consultant, vendor) who has/had legitimate access to an organisation attempts to cause harm through counterproductive behaviour intended to result in the loss, disclosure, or damage to that organisation's information, resources, assets, or reputation.*

Part Two – Describing IIT

Following the literature review and Delphi process, pertinent items of IIT were transformed into questions for the development of a diagnostic inventory of organisational vulnerability to IIT (the OVIT). The valid completion of the online inventory by 141 respondents provided a means for describing IIT. The high level of homogeneity of the sample providing a basis for robust outcomes. Analysis of the descriptive statistics highlighted: (1) that organisations could benefit more from checking for potential problematic behaviour, abuses, and personality characteristics associated with insider threat; (2) organisational complacency, when it comes to IIT focus and implementation of initiatives, was a salient outcome; and (3) technical safeguarding is a positive organisational practice although could be enhanced though use of modern technologies and advanced analytic tools designed to detect, deter, prevent, and report on IIT.

Through exploratory factor analysis (EFA) a further understanding of the construct was achieved. The EFA was able to reduce the number of items designed to measure the individual, organisational, and technical dimensions of organisational vulnerability to IIT.

Phase Three – Validating IIT

The validation of the construct was achieved through an EFA of the OVIT. Following assumption testing, the conduct of EFA on the inventories designed to measure the three dimensions of IIT (individual, organisational, technical) was performed. Assumption testing revealed no significant concerns for exploratory research. Maximum Likelihood procedure was used to extract factors from the variables of the OVIT sub-inventories and the Promax oblique rotation was chosen to provide simple and meaningful factor structures. The overall outcomes demonstrated that the full OVIT (96 questions) and its three sub-inventories - OVIT-Individual (25 questions), OVIT-Organisational (51 questions), and OVIT-Technical (20 questions) - are valid and reliable measures of the dimensions and construct.

This chapter described the data analysis undertaken in this exploratory research study. The chapter highlighted the three main phases of data collection and analysis highlighting the results of the literature review, the Delphi process, and the Exploratory Factor Analyses. The multivariate analysis process included data preparation, cleaning and screening, generating descriptive statistics, and conducting three EFA. Whilst an EFA of the entire inventory was not possible, the EFA of the three separate inventories produced preliminary factor solutions which operationalised the construct of organisational vulnerability to intentional insider threat.

The results of this study has contributed new insights to IIT such as the development of an IIT definition. It has extended conceptual and theoretical understanding through demonstrated exploratory evidence of the validity and reliability of the construct of IIT, including the relevance of its three dimensions; individual, organisational, and technical. A working framework on organisational vulnerability to intentional insider threat is presented. The underlying factors associated with the dimensions of IIT is an original contribution which extends current understanding of IIT. The elucidation of underlying IIT factors provides a means for organisations to understand vulnerability to intentional insider threat and target specific areas to mitigate IIT.

The interpretation, implications, and limitations of these results are discussed in the following chapter.

5 Discussion and Conclusions

5.1 Introduction

The current thesis began in Chapter 1 by introducing the researcher and providing an introduction and overview to the research. The influence of the scientist-practitioner model along with policies of the Australian Government was introduced. A background to the motivation for completing the research, the scope of the project, an outline of the anticipated contributions, as well as the aims of the research and thesis structure was presented.

In order to achieve the aims of the research, Chapter 2 presented an extensive literature review that explored insider threat and risk management. Various approaches to the study of insider threat were introduced. Further, prominent models and frameworks of insider threat were examined. Positioning the study in a risk management framework was also undertaken. The limitations of the available research were expressed to justify the importance of further exploration of organisational vulnerability to intentional insider threat and benefit of developing the OVIT.

Chapter 3 outlined the research design adopted in the study and detailed major methodologies used. The current research was underpinned by the Pragmatist worldview and a sequential mixed method typology chosen for the design. This research aimed to develop a greater understanding of IIT through three distinct research phases: review of current literature, a Delphi study, and the operationalisation of organisational vulnerability to IIT through multivariate analysis. Finally, ethical considerations for the research was examined.

Chapter 4 provided the data analysis and interpretation. Results of the three phases of the research design were presented in detail. The outcomes of the exploratory factor analyses were presented culminating in the presentation of the OVIT

Framework and factor structures for the individual, organisational, and technical dimensions.

Chapter 5 now reports on the findings that have emerged throughout the research process. This chapter first explores the conclusions reached with regard to the three research questions. Additional contributions to the field from a theoretical, practical, and personal perspective are also discussed. Finally, limitations of the study and recommendations for future research are explored.

5.2 Research Outcomes

Intentional insider threat is one of the many risks that organisations are confronted with. The ability to reduce vulnerability to IIT is critical to organisations achieving strategic and competitive advantage (Vashisth & Kumar 2013). It also provides organisational protection reducing potential financial loss, damage to reputation, and loss of valuable intellectual property. This thesis focused on organisational vulnerability to IIT, addressed some of the inadequacies in existing research, especially related to organisational influence, risk management, and the multidimensional aspects of the problem. It also provided a brief futures perspective in order to suggest how IIT may evolve looking ahead.

The study developed a diagnostic inventory (OVIT) to assess organisational vulnerability to IIT and, based on these findings presented a preliminary model of organisational vulnerability to IIT with both practical and academic utility. The research adopted a multipronged approach proposing a comprehensive way to mitigate vulnerability to IIT. The thematic analysis determined pertinent dimensions of IIT and provided a greater understanding of the multidimensional (individual, organisational, and technical) considerations of IIT.

A modified Delphi study and expert opinion and consensus provided relevant and purposeful information on insider threat (Catrantzos 2012) and the most relevant factors and variables were incorporated in the final operationalisation of IIT and development and validation of the OVIT. The outcome of this exploratory research is

a comprehensive, expertly informed, valid, and reliable tool for the assessment of organisational vulnerability to IIT as well as a working framework which clearly demonstrates the relationship between the construct and its dimensions and factors.

5.3 Research Findings

5.3.1 Phase One – Research Question 1

Research Question 1: *What are the main organisational influences on intentional insider threat (IIT) based on available literature?*

Research question one proposed that the literature content has explored the foundational concepts and variables related to IIT. It was deemed critical to the study to comprehensively identify the relevant influences of IIT expressed in the available literature. Through phase one, 141 item variables (see Section 3.4.1) were extracted from extant literature addressing pertinent aspects of IIT. These included coverage of the individual, organisational, and technical aspects of the problem. There were 35 variables of influence considered to potentially decrease IIT, 42 thought to increase IIT, and 51 generalised potential methods and conditions to mitigate insider threat.

The distillation of themes from the literature review not only contributed to potential variables of interest that were included in phase two of the study, but also culminated in a simple conceptual model of organisational vulnerability to IIT (see Figures 9 and 13). This is a unique contribution of the study and provides a simple diagrammatic overview of the concepts of IIT, how they are related, and how they affect organisations.

An evaluation of the available research and extant literature demonstrated that whilst researchers and organisations did recognise IIT as a potential organisational risk, there was a greater emphasis on addressing external and technological risk (Cyber Security Division 2009). Further, consistent with the findings of Festa (2012b) and Catrantzos (2012) there was a clear and prominent focus on individual, societal,

and technological influence, with less focus on organisational factors and determinants.

Prior to the current study, *there was a persistent concern identified in the literature regarding the narrow and predetermined focus given to insider threat*. This thesis contributes to, and enhances, the importance and application of organisational factors in the management of IIT. Based on this exploratory study it was determined that the construct of organisational vulnerability to IIT can be represented by three dimensions (individual, technical, organisational) and 13 factors (see 20 and phase 3, RQ2). The more specific OVIT-Organisational Inventory resulted in 90 items representing the organisational dimension within the construct of broader organisational vulnerability.

Seeking a level of robustness in the OVIT-Individual, demographical, motivational, and psychological components were incorporated. Addressing specific individual concerns was not within the aims of the current study. However, ensuring that organisations considered a layer of protection in determining individual vulnerability was important. The OVIT and related working model identifies four specific factors under the *individual* dimension supporting a focus on understanding people working for and within any organisation.

Likewise, technical factors have been incorporated in to the OVIT. It is clear from the literature that IT and cyber influence is important. Therefore a comprehensive approach to determining organisational vulnerability requires consideration of some of the technical factors within an organisation's control. The span of influence of the technical factors is narrower than the organisational component, with 20 questions retained for the OVIT-Technical Inventory.

5.3.2 Phase One – Other Outcomes

Whilst RQ1 was very specific, the undertaking of phase one presented additional findings which are considered important for presentation. The current thesis was able to extend the literature and understanding of IIT in various ways, advancing the

study of IIT. Specifically this study was able to address the clear lack of representation of Australian contribution to IIT literature as well as couch its findings in a manner relevant to the Australian context while also contributing original insights to IIT literature of global relevance.

Risk Management and IIT

The Australian Government mandates a risk management approach to addressing insider threat, however, a review of the literature exposed limited research which specifically utilises risk management methodology to underpin investigations. In fact, there was also an underwhelming representation from Australia on the topic.

Even so, the extensive and exhaustive review of the extant literature determined that organisational vulnerabilities and strengths could be distilled and identified for greater investigation. The coverage of demographical, psychological, motivational, organisational, and technological research, as it relates it IIT, demonstrates the multifactorial influence as well as the need for multidimensional response.

The addition of reflecting on IIT through a risk management perspective also exposed new insights determining organisational influence on IIT. As such, this thesis presents a unique contribution to the study of IIT which integrates the research on insider threat with the AS/NZ ISO 31000:2009 risk management standards (see Sections 2.2.8, 2.2.9, and 2.2.10).

Given the above exercise, the current thesis has also made a contribution to the risk management field. Until now, there has been limited expression of insider threat through use of a risk management methodology as defined the Australian Standards (AS/NZ ISO 31000:2009). This is a unique contribution of the current thesis. In Chapter 2, Section 2.2.5 integrates risk management standards, including security risk management, with research/publications on insider threat, under rigorous research conditions. Further, ensuring an alignment between risk management methodology, assessment, and practice has provided a diagnostic tool with potential for a standardised approach to the identification, assessment, and evaluation of IIT.

Implementation of the OVIT allows for comparisons within and across organisations, enhancing shared understanding and facilitating decision making and judgment (Homeland Security 2011).

The OVIT Framework

When it comes to current and prominent models of insider threat, individual and technical dimensions are well covered. However, to varying extent, the current models undermine or underrepresent the importance of organisational influence in both positive and negative representations. Even though the current research aimed to strengthen the importance of organisational representation in the literature, the resultant OVIT appears capable of aligning with the most commonly cited models of insider threat (see Table 36). Further the assimilation of all three dimensions into a diagnostic instrument is original and makes a significant contribution to IIT practice.

From the current thesis a working model of organisational vulnerability to IIT has been presented along with three inventories designed as a diagnostic tool to aid organisations in appropriate risk management. The model presented is an academic contribution, but it does not stand alone. In fact, the presenting model works with the existing frameworks and models in insider threat study. Many of the existing models already acknowledge insider attributes and actions as well as the complex interaction between individuals and their environments (Legg et al. 2013). The set of inventories produced from this research are able to support the various models of insider threat that exist in the literature (see Table 36) and advances the contribution to knowledge of IIT and practice by proposing a diagnostic tool aimed at identifying and mitigating vulnerability in a holistic approach.

Table 36: OVIT Support for Existing Insider Threat Models.

Model	OVIT support
Critical pathway model	Personal predispositions Personal stressors Concerning individual behaviours Organisational responses
Management and Education of the Risk of Insider Threat (MERIT) models (Cappelli et al. 2012)	Personal predispositions Disgruntlement Behaviour Behavioural monitoring Technical monitoring Positive organisational intervention
Legg et al. (2013)	*Enterprise* – elements that constitute the enterprise on an operational level *People* – elements describing an insider, his motivations and his behaviour within the enterprise *Technology and Information* – elements relating to hardware and software in the enterprise and the digital activities that can be recorded *Physical* – elements that capture physical components (e.g. locations) that exist within the enterprise
'A Grounded Framework' by Nurse et al. (2014a)	Technical and behavioural indicators Human factors and motivations

The Blick Review

In Australia, a review by Blick (Williams 2000) recommended Australian Government reduce potential for insider threat through various means of protection. These covered psychological assessment, staff checking, physical and personnel security practices, and security programs. These broad areas of countermeasure were consistently identified in the literature review process. In addition, the outcomes of this thesis resulted in a working model of organisational vulnerability to IIT, along with specific items in the OVIT, which captures the factors of staff vetting, staff psychological assessment, and staff security and risk management, under the *individual* dimension. As well there are factors of the *organisational* dimension - organisational initiatives and organisational protections – which fit well with the means of protection offered by Blick. This provides support for the recommendations Blick provided to Government. However, the recommendations (as exposed through open source publication) do not appear to address the full gamut of protection available to organisations, critically avoiding broader organisational influence and control.

Contrasting Outcomes

The research review process identified a number of potential insider threat concerns which were not identified as pertinent in this study. For example, Shaw et al. (1998) indicated that high demand for IT services and high rates of turnover in IT roles should be explored as having potential to reduce loyalty to organisations and result in increased insider threat risk. Further, globalisation and foreign allegiance, as discussed by Cappelli et al. (2012) and Herbig (2008), were concepts considered to affect loyalty and therefore insider threat potential. However, throughout this research, questions addressing the risk related to high turnover and allegiance did not survive beyond the Delphi study (that is, did not reach consensus).

In addition, Colwill (2010) argued that outsourcing could result in the dilution of protection controls and increase risk of insider threat. However, Munshi et al. (2012) determined that empirical evidence at the current time does not appear to suggest that outsourcing and use of contractors are significant factors in insider threat. Outsourcing as an IIT diagnostic concern did not reach consensus through the Delphi panel phase and appears to support the current position of Munshi et al. (2012).

While there were some factors which did not survive from the literature review through to the final OVIT, there were many areas which were clear strengths consistently addressing the construct under investigation. Personality vulnerabilities and predispositions affecting judgment are clear examples. So too, organisationally specific considerations such as the way in which organisations recruit, train, and manage staff. Positive organisational leadership, culture, and conditions are consistently expressed as having the potential to strengthen defence (CPNI & PA Consulting Group 2012; Shaw & Fischer 2005; Shaw et al. 2009; Shaw & Stock 2011; Tang et al. 2016). Based on the outcomes of this current research there is a clear representation by several questions addressing the *organisational* dimension, especially the factor of *organisational culture and leadership*.

From an IT perspective detection, analysis, and misuse are clear priorities in the research effort (Neumann 2010). This, overall, is consistent with the findings of the current thesis, where the *technical* dimension has resulted in three factors of

technical monitoring and detection, technical access, and technical restrictions. When it comes to cyber-security and insider threat, the research literature suggests that IT sabotage often occurs following termination or during suspension from duties (Cappelli et al. 2012; Catrantzos 2012). It is therefore positive to note the survival of variables of the OVIT addressing termination and exit processes from the individual, organisational, and technical perspectives (e.g. does the organisation have policy to conduct random reviews of exiting staff computer activities leading up the final date *and* are policies and processes in place to ensure that the privileges and accesses of staff leaving the organisation are disabled).

Foresight and Futures Studies

The current status of IIT research and the way in which this thesis contributes and extends the current position has been clearly presented in this thesis. However, it is worthy to note that IIT study and practice cannot be static. To this end, attention to foresight and futures studies was introduced as a complimentary perspective in Phase One of the study. The current research has successfully contributed to this narrative throughout the entire research project and the foresight and futures studies perspective is presented here even though it transcends all three research phases.

Clearly this thesis has contributed to foresight and futures studies through addressing the initial phase of the foresight process and makes initial insights into Phase 2 of the foresight process. Horton (1999) acknowledges that third parties are useful contributors to phase one, helping organisations unfamiliar with the subject matter and/or preventing narrow sightedness. The future availability of the thesis presents a gathering of relevant source material on the current status of insider threat, providing a sound basis for greater understanding of the future of insider threat. Whilst the foresight process is most commonly applied to organisations specifically, it can be argued that the process of engagement in foresight methodology may still be relevant in broader applications such as in the conduct of research (van der Laan 2010). For example, consider the application of the foresight process to insider threat through conduct of the current research. Certainly the means of undertaking the

current thesis has achieved against the first two phases of the foresight process and provides some wisdom required for appropriate action.

The collection of information and review of literature, discussion with colleagues and business networks, appraisal of government reports, and supervision with university staff, satisfies the collection component of phase one of the foresight process. Not to mention the Delphi study (RQ2) which was conducted as part of the methodology. Delphi studies are a common research method adopted in futures studies (van der Laan 2010) and assist with Phase 2 interpretation of the foresight process. The collation component of phase two requires that collected information is given greater structure and form through reduction in volume and deciphering what is most relevant (Horton 1999). The result is a summarisation of all information in a relevant form, perhaps akin to the current research literature review. In phase two, translation has been achieved through the plain language writing of the research thesis as well as the three inventories. Finally, interpretation is achieved via the results and discussion of the current research thesis. As Horton (1999) described the application of meaning to the data and the ability to use it to product actionable outcomes to prepare for possible future scenarios is what is most important. It is therefore recommended that future research adopt the findings of this thesis for the Phase 3 completion of the foresight process.

Assimilation and commitment are the pillars of phase three of the foresight process. The current research has achieved this through presentation of new insights, actions, and tangible outcomes. Not only the production of three inventories to assist organisations to better understand their vulnerability to insider threat, but also the discussion of new insights and presentation of new foresights following the data collection through both the Delphi method and survey outcomes.

Here, the OVIT demonstrates its utility in providing a means of evaluating organisational vulnerability to IIT regardless of the organisation's (or staff) expertise in the area or any bias in assumptions (such as the insider threat only being of

technical concern). Further the implementation of the OVIT can provide an organisation's real-time understanding of vulnerability to IIT.

5.3.3 Phase One – Contributions

Theory
▪ Enhanced understanding and knowledge of organisational vulnerability to intentional insider threat ▪ Comprehensively identified the relevant influences of IIT expressed in the available literature ▪ Conceptualisation of a simple model of organisational vulnerability to IIT based on the consolidation of extant literature ▪ Integrating the research on insider threat with the AS/NZ ISO 31000:2009 risk management standards ▪ Contributing foresight and building on futures studies research as it relates to insider threat
Practice
▪ Enhancing the narrative and emphasising the importance of organisational factors in the study (and application) of IIT ▪ Demonstrating the multifactorial influence as well as the need for multidimensional response ▪ Informing future practice through distilling emerging trends related to insider threat
Self
▪ Enhanced theoretical knowledge by developing greater understanding of risk management and insider threat ▪ Enhanced professional knowledge, tolerance for ambiguity and critical judgement by increasing understanding of insider threat through use of high level research skills

5.3.4 Phase Two – Research Question 2

Research Question 2: *What are the main organisational influences on IIT based on expert opinion?*

The Delphi study was a vital contributor to the overall research. Whilst the literature review provided the current positioning of IIT, the Delphi process sought to gain insight and feedback from experts to identify key gaps and critical additions to variables of influence. Through utilisation of the Delphi method, deep insights from Australian experts provided a greater understanding of the construct of IIT. Having extracted the pertinent variables in the literature review, the Delphi study contributed to, and informed, this real world study by determining which items were of greatest relevance and priority. The Delphi process also exposed a number of variables, considered critical to the diagnostic potential of IIT, and either missing (or missed) from the literature review process or where panel experts considered their relevance as underrepresented or underemphasised.

Given the Delphi study was part-based on the literature it is not surprising that there is a strong level of consistency between the Delphi outcomes and the extant research. The Delphi results are presented in Section 4.3 as variables which underpin the initial OVIT. These variables have been summarised as broad organisational considerations and themes for the detection and prevention of IIT. Table 37 demonstrates that these broad Delphi outcomes are consistent with the literature and, in the majority, also support the operationalisation of organisational vulnerability to IIT as proposed by the OVIT Framework and working model presented as part of this thesis.

Table 37: Mapping of outcomes from the research with existing literature.

Summarised Delphi Outcomes	**Operationalised Thesis Factors**	**Examples of Supporting Literature**
Regular staff education and training; including security awareness, compliance, and risk management	Staff Security and Risk Management Insider Threat Initiatives	Sarkar (2010) Williams (2008) Kraemer et al. (2009) Hunker and Probst (2011)
Leadership training, education, and management aimed at producing strong and supportive leaders and managers	Organisational Culture and Leadership Staff Ethics Organisational Complacency	Greitzer and Hohimer (2011) Kraemer et al. (2009) Hunker and Probst (2011) Gelles (2016)
Appropriate employee monitoring and assessment through all stages of the employee cycle – especially as it relates to disgruntlement and ego/sense of entitlement.	Staff Vetting Staff Psychological Assessment Organisational Complacency	Probst et al. (2010b) Greitzer et al. (2013) (Festa 2012a) Shaw and Stock (2011) Huth (2013)
Providing avenues for staff engagement and input, including performance reviews, staff surveys, etc.	Staff Security and Risk Management Organisational Reporting	Probst et al. (2010b) Huth (2013)
Provision of an EAP/Staff counselling service	Not applicable – did not survive the EFA	Greitzer and Hohimer (2011) Probst et al. (2010b)
Relevant, endorsed, and monitored security policies and procedures; including whistle-blower protection policies, how to identify, report and manage concerning behaviour/security issues	Staff Security and Risk Management Insider Threat Initiatives Organisational Protection Organisational Security Awareness Organisational Reporting	Greitzer and Hohimer (2011) Williams (2008) Kraemer et al. (2009) Hunker and Probst (2011) Probst et al. (2010b) Huth (2013)
Relevant, endorsed, and monitored IT policies and procedures	Organisational Protection Organisational Security Awareness	Sarkar (2010) Huth (2013)
Aiming for consistency across all organisational policies and processes	Organisational Protection Organisational Security Awareness	Pfleeger et al. (2010) Hunker and Probst (2011) Shaw and Stock (2011) Huth (2013)

Obvious and declared security controls	Organisational Protection Organisational Security Awareness	Probst et al. (2010b) Huth (2013)
Random auditing and computer monitoring	Technical Monitoring and Detection Insider Threat Initiatives	Sarkar (2010) Kraemer et al. (2009)
Impeded access controls, including minimum privilege access, physical access controls, etc.	Technical Restrictions Technical Monitoring and Detection Technical Access	Sarkar (2010) Kraemer et al. (2009)
Open source monitoring	Organisational Protection Technical Monitoring and Detection	Sarkar (2010) (Festa 2012a)
Ongoing and evolving focus on risk assessment and management, including development of an Insider Threat response plan	Staff Security and Risk Management Insider Threat Initiatives Organisational Complacency	Hunker and Probst (2011) Huth (2013) Gelles (2016)
Developing a resilient organisation with a strong organisational and security culture	Organisational Culture and Leadership	Pfleeger et al. (2010) Williams (2008) Hunker and Probst (2011) Probst et al. (2010b) Gelles (2016) Catrantzos (2012)
Focus on research including how offenders evaluate opportunity, how to develop a security culture, etc.	Not applicable to the diagnostic requirements of the OVIT. But does support: Insider threat initiatives Organisational reporting	Most research and publication recommends future research and opportunity.

5.3.5 Phase Two – Other Outcomes

Aside from the consistencies, as they relate to operationalisation of IIT, determined through the Delphi study and literature review, there are several additional contributions borne out of the Delphi process. These are not directly related to RQ2 or the determination of the OVIT and operationalisation of organisational vulnerability to IIT. Still they are important contributions ascertained from the three rounds of the Delphi study (phase two).

An Australian Definition

As Hunker and Probst (2011) expressed there is no uniform or widely accepted definition of insider threat and certainly a review of the literature also revealed a similar fate for the definition of IIT. The absence of an Australian definition of IIT has been addressed in the current research. Whilst a specific definition for the Australian context may not be a necessity, a more precise definition for Australia may provide

assistance to alleviate the fragmented conceptions which exist. In the current study the development of an Australian definition on IIT assisted understanding in the scope of exploration as well as the parameters of the development of the OVIT. Further, the development of an Australian definition enhanced the conceptualisation of the construct under investigation and therefore worked to enhance the reliability of the study (see Table 2, page 124).

Gelles (2016) discussed the critical importance of defining insider threat within an organisation as it can help inform an insider threat strategy, including its structure, size, and scope. Whilst the definition produced from this thesis is not organisationally specific it may provide a sound broad basis to begin. The Australian based definition of IIT formed through this research is:

> *Intentional insider threat is when a person of trust (employee, contractor, consultant, vendor) who has/had legitimate access to an organisation attempts to cause harm through counterproductive behaviour intended to result in the loss, disclosure, or damage to that organisation's information, resources, assets, or reputation.*

According to the majority of panel experts an *employee* was ranked as the greatest risk when it comes to IIT (out of employee, contractor, and consultant). However, follow up in qualitative form demonstrated that this was not upheld from a consensus perspective (less than 70% agreement). As such, it appears from this research that all individuals engaged with an organisation present as a potential insider threat. This is consistent with the definitions presented by Catrantzos (2012) and Cappelli et al. (2012) which articulate the insider threat to be from anyone with legitimate access regardless on the type of engagement. It is also consistent with the final definition advanced from the current thesis.

Barriers to Insider Threat Initiatives

The cost of implementing insider threat initiatives was raised by the panel as a barrier to implementation. This was evident around psychological assessment, where panel experts noted that the cost (in both time and funds) could be a deterrent. Securing resource requires the engagement of senior managers (Clarke & Varma 1999; Dionne

2013; Standards Australia 2006), and the OVIT is able to provide a means for organisations to understand where they are at greatest risk. From a risk management perspective efficiency and value can be achieved and the selection of IIT initiatives tailored to ensure cost effectiveness and organisational compatibility (Fenz et al. 2011; Fenz et al. 2014; Khan & Khan 2014).

Interestingly there appeared to be two (overlapping) positions when it came to where insider threat initiatives were most effective with regards to the individual. Keeping potential threats out of the organisation (through pre-employment initiatives) versus monitoring employees once they were inside (as well as the combination of both). This is a topic covered briefly in the literature. Catrantzos (2012) appears the strongest proponent of employee engagement and monitoring over more "traditional" strategies such as background checks and updates, and invasive monitoring. He argues that initial screening is "a low hurdle" to overcome and greater value can be achieved with close probation, transparency, and a self-monitoring team. Regardless, the OVIT presents an opportunity to explore organisational effectiveness from both sides.

A Multi-disciplinary Approach

The Delphi study upheld the position that IIT can only be satisfactorily addressed through a multi-disciplinary approach. There was consensus that organisations should have cybersecurity skills available, whether internally or externally sourced. The Delphi study also proposed the importance of senior management dedication to security. Not only through the way management lead by example and build a positive security culture, but ultimately through a dedicated senior management position responsible for security. As such the fields of organisational psychology, risk management, management and leadership, information management, organisational behaviour, and futures studies were integrated as a holistic practice orientated approach to IIT.

5.3.6 Phase Two – Contributions

Theory
▪ Execution of an Australian based study that expands the current knowledge base on IIT ▪ Built on existing definition and formulated an Australian based definition ▪ Application of the Delphi method to the study of IIT ▪ The identification of further variables related to IIT not available in the extant literature ▪ Conference presentation. Providing information that condensed Delphi research outcomes
Practice
▪ The importance of a senior management position dedicated to security who answers to a Board member ▪ The need for a multidisciplinary approach to insider threat ▪ Contribution to the growing knowledge base on IIT through conference poster presentation
Self
▪ Enhanced collaboration and professional knowledge by developing greater networks in risk management and with experts in CWB/Insider threat ▪ Understanding of the Delphi Method and capacity to employ this research technique in future work-based projects

5.3.7 Phase Three – Research Question 3

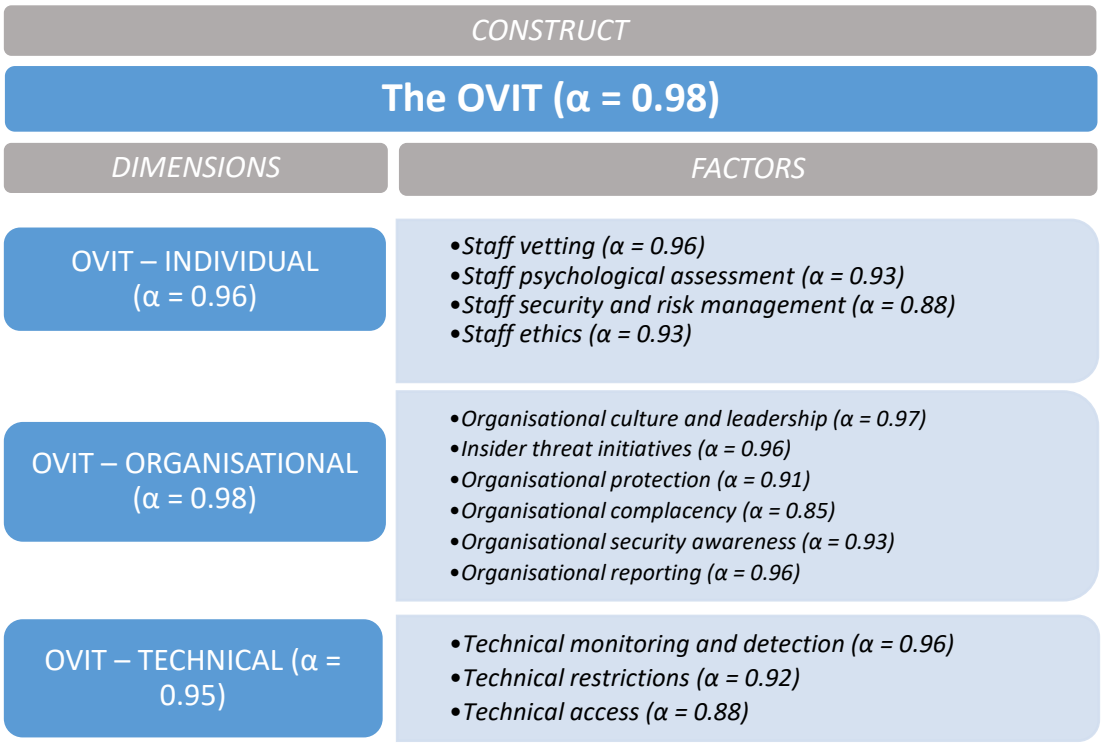
Research Question 3: *How is organisational vulnerability to IIT operationalised by the study?*

The results of the pilot process and full study Exploratory Factor Analysis (EFA) revealed that organisational vulnerability can be assessed through inventory format. Whilst only a preliminary and working model of the construct under investigation, the OVIT framework proposes three dimensions of organisational vulnerability to IIT with 13 representing factors. Theoretical support, with a lead from Sarkar (2010), justified the alignment of the factors with the three dimensions. The literature available provided a sufficient basis to assess the three dimensions of IIT (individual, organisational, and technical) and link these dimensions to the overall construct of organisational vulnerability to IIT. Further the triangulation of the data throughout all three phases supported the resulting item content of the diagnostic inventories.

This study investigated the three dimensions of IIT with a specific focus on elements of threat that are within organisational control. That is, what can organisations do that can increase, decrease, or mitigate against IIT. The diagnostic inventories were developed to provide organisations a greater understanding of their own vulnerability to IIT. The results of the EFA demonstrated statistically significant factor

structures and determined the three inventories as valid and reliable measures of each dimension (OVIT-Individual, α = 0.96; OVIT-Organisational, α = 0.98; OVIT-Technical, α = 0.95) and ultimately of the overall construct under investigation (The OVIT α = 0.98; see Figure 22).

Figure 22: Statistical representation of the OVIT.



Source: Developed for this study.

Sarkar (2010) advocated for a three-pronged approach to the assessment of insider threat to information security. He believes the use of "technical, behavioural, and organisational assessment is essential in facilitating the prediction of insider threats" (Sarkar 2010, p. 112). As presented in the literature review, historically insider threat assessment and mitigation has focused on technical evaluation and solutions. However, the importance of including individual and organisational factors in identifying and controlling threat is gaining attention.

The OVIT responds to the challenge presented by Sarkar (2010) by providing a means to assess the risk of organisational vulnerability to IIT using a three-pronged approach

(individual, organisational and technical). The evaluation of the responses to the OVIT also allows organisations to correct, detect, and prevent potential insider threat actions and assist organisations to prioritise and allocate resources to address potential IIT risk.

This research has identified 13 factors essential to the assessment of organisational vulnerability to IIT. The factors and their underlying questions oblige the best practice and "basic baseline" measures determined by Sarkar (2010) which include: strict HR policies; mandatory awareness training; technical controls; hardware controls; network controls; and auditing and monitoring as detecting controls. However, the OVIT extends beyond these baseline recommendations and demonstrates the importance of other factors to the assessment and mitigation of IIT. Moreover, the OVIT clearly demonstrates essential individual and organisational factors that organisations should be considering when determining a risk strategy.

5.3.8 Phase Three - Other Outcomes

Whilst the aim of the study was to develop a valid and reliable diagnostic tool for IIT, the study did reveal a valid and valuable insight into the practice of IIT approaches in Australia. As such, descriptive statistics yielded a description of the sample's characteristics and practice (e.g. lack of foresight, lack of inter-organisational collaboration, talent turnover, and lack of expertise, etc.).

Having established a preliminary construct of organisational vulnerability to IIT, interrogation of the demographic data provided further insights. Whilst this study did not hypothesise any relationships or influence of demographic data it certainly provided an understanding of the sample group. The frequency and descriptive statistics of this thesis provides an overview of what IIT looks like in the Australian context.

Based on the current research findings, there are two particularly significant findings which were extracted around insider threat expertise and organisational complacency.

Insider threat expertise

Based on the data available in the current study it was interesting to note that the majority of participants (79.6%) had at least some level of insider threat expertise. This may be a function of the sampling technique and the large number of survey participants (38.5%) being from the Defence, Security, Intelligence, and Law Enforcement industry. However, it does suggest a high level of insider threat awareness among the participant group. There appears to be a growing understanding and appreciation of IIT and based on this research, awareness is broad and not just targeted at senior management level.

Organisational complacency

Given the above result, that there is a high level of awareness and expertise in insider threat amongst the survey participants, it is interesting to note that the organisations to which these participants belong are engaged in a level of complacency. Given there is a lot of information on the costs (not just monetary) of insider threat it appears organisations are not prepared or participating as vigorously against the threat. So whilst individuals within organisations may be alert to insider threat potential, this does not necessarily extrapolate or influence the organisations in which they work. Organisations appear to be increasing their vulnerability through a lack of engagement with, or employment of, trained professionals to identify and manage insider threat risks. Further, many organisations are not utilising insider threat initiatives. For example, nearly half of the organisations represented by the survey group are not employing psychological assessment as a measure of protection or mitigation. And, over 70 percent are making minimal effort to integrate insider threat mitigation as part of the enterprise risk management strategy.

In addition, assessment of security culture is being overlooked with more than 30% of organisations rarely or never assessing security culture. An Australian study by Parsons et al. (2015) found that improving security culture can lead to positive employee behaviour, extrapolated to include compliance with security. As well, Renaud and Goucher (2014) found that security culture is tied with security behaviour. It appears that this Australian based sample falls in line with previous

reporting on the need for greater attention to insider threat and implementation of initiatives.

The low rate of uptake when it comes to insider threat initiatives present a means for intervention. However, as already explored above, the Delphi panel raised concern about cost and the literature presented similar findings. The apparent complacency of the organisations represented by this sample, despite the awareness and experience of the individual respondents with insider threat, may be cost related. Regardless, it provides an avenue for further investigation into the main reasons of complacency. Given the cost of compromise there is worth in understanding the benefit-cost ratio and value-benefit of IIT initiatives, which is outside the scope of the current study.

5.3.9 Phase Three – Contributions

Theory
▪ Present a model that operationalises organisational vulnerability to IIT ▪ Plan and execute an Australian based study that expands the current knowledge base on IIT ▪ Development of a quantitative diagnostic instrument measuring IIT ▪ Statistical validation and establishment of the reliability of model of organisational vulnerability to IIT ▪ Development of a measurement model which defines the construct of organisational vulnerability to IIT along with its dimensions and factors ▪ Testing of a factorial structure operationalising the IIT concept
Practice
▪ Development of a measurement instrument that can be applied in the organisational context, providing a means of education, a way to demonstrate trends in organisations that can lead to IIT behaviour, and provide an organisation with information on its vulnerability to IIT ▪ Providing professional practitioners a valid and reliable tool to detect and diagnose IIT ▪ Description of the Australian context and what IIT looks like - frequencies and descriptive statistics
Self
▪ Enhanced objective judgment, analytical skills, and research techniques ▪ Improved subject positioning, status and expertise in the field of insider threat

5.4 Summary of Contributions

5.4.1 Contribution to theory

By the very nature of undertaking the current research project a contribution to theory and research pertinent to IIT has been achieved. It was clear from the

literature review that there is limited Australian contribution to the study of IIT, which is dominated by US and UK representation. Further until now there has been less emphasis on the organisational dimension of IIT in favour of technical and individual approaches. Certainly, there has not been an overarching approach where the IIT construct incorporates a holistic view of all three dimensions.

The use of the Delphi method, and gathering of expert opinion, in the study of insider threat is not new (see Catrantzos 2012; Greitzer et al. 2013; Greitzer et al. 2009; Kraemer et al. 2009). However, this research has demonstrated its utility in the Australian context and in the development of survey and measurement instruments. Importantly the Delphi process resulted in an enhanced definition of IIT relevant to the Australian context which is proposed to be relevant to the international context. Further, incorporating the Delphi method established a mixed method approach to the research, enhancing reliability and validity indicators. The mixed method approach is also the first of its kind exploring organisational vulnerability to IIT in the Australian context.

This thesis has elucidated the foundational concepts related to IIT and comprehensively expressed coverage of the individual, organisational, and technical aspects of the problem. Utilising literature findings and Delphi outcomes, the thesis provided a simple conceptualisation of the construct and related it to existing models, theory, and risk management methodology. The Delphi process also identified new variables for consideration not previously recorded in the extant literature. Phase three allowed for a more comprehensive understanding of the construct of IIT. A comprehensive model which reflects the overall construct, its three dimensions, and the factors underneath is a significant theoretical contribution. To the researcher's knowledge this is the first validated quantitative diagnostic instrument to detect and diagnose organisational vulnerability to IIT.

5.4.2 Contribution to professional practice

Being a work-based research study, the usefulness of this project is in transforming the research, academic, and theoretical contributions in to usable, practical, and

applied outcomes. The current research was borne out of a desire to assist in the fight against insider threat in a manner that all organisations can benefit, whilst also maintaining a focus on ethical considerations and beneficence (see Section 3.8). Catrantzos (2012) discussed that to date there has been a dearth of content providing recommendations or practical tools as a means of countermeasure. Whilst many reviews and recommendations have been made in order to try and reduce potential espionage and other insider threat (Williams 2000), this current research addresses recommendations to include a more rigorous and holistic focus on organisational predispositions and vulnerabilities (Band et al. 2006).

According to Hunker and Probst (2011) an integrated and multidisciplinary approach to insider threat, in a way that is useful to practitioners, has not been achieved. With other authors further claiming that the combination of technical controls, psychosocial considerations and organisational factors, hold the most promise for understanding, detecting, and preventing insider threat within organisations (Borrett et al. 2013; Gelles & Mitchell 2015; Greitzer et al. 2009; Kraemer et al. 2009). Here, with this exploratory research, three diagnostic inventories addressing IIT through a multidimensional focus and with input from a breadth of sources shows promise. The OVIT provides practitioners with a validated and reliable tool to detect and diagnose IIT.

Whilst the current study is not focused on work-based product it is interesting in how the undertaking itself has contributed to increased knowledge of others. Delphi feedback indicated that simply reading the questions of the OVIT increased awareness. The OVIT, by its implementation, appears to provide a means of education to those completing the inventories. From a practical perspective this is one way to increase knowledge and awareness, creating a vigilant workforce, which is an excellent defence against insider threat (Gelles 2016). The administration of the OVIT may also provide a cost effective strategy for intervention noting that all three phases of this research identified the cost barrier as being influential.

Further, the OVIT may provide a means of initial discussion and education on IIT. The comprehensive working model presented, which clearly articulates the relationships amongst the construct, dimensions, and factors, provides a means for education and a basis for developing mutual understanding through shared language. The OVIT also provides practical guidance on organisational baseline vulnerability and potential areas requiring proactive intervention.

5.4.3 Contribution to self

As presented earlier in this thesis the integration of research and practice is an important career objective for many organisational psychologists. The development of knowledge and skills, through practice and work-based research, allows for the development of effective psychological service as well as broader research and intervention skills. Undertaking the current research has contributed to an approach to lifelong learning and is consistent with the scientist-practitioner model.

Through each of the three phases of this research project there has been significant contribution to the self. The enhancement of knowledge and understanding of insider threat and risk management is evident. The development of high level qualitative and quantitative research skills has been established through utilisation of the Delphi method and multivariate statistics. The overall process presenting opportunity for developing greater objective judgment, analytical skills, and research techniques. The four years of effort culminating in the ability to demonstrate subject matter expertise in the field of insider threat.

Participation in this research study has also created opportunity for dialogue, creating conversations with others to ensure that knowledge and learning are more than just a cognitive process (Corlett 2012). As a researcher it is important to create opportunities for reflexive dialogue (Corlett 2012) acknowledging that such can be achieved through informal or formal channels (Benozzo & Colley 2007). Reflection therefore provides the ability to examine attitudes and behaviour and learn from this, enabling better choices or responses in the future (Nilsen et al. 2012b). Relevant conversations and reflections has been achieved through interaction with Delphi

participants, supervision sessions, professional networking, presentation at conferences, and publication.

Further reflection is achieved by revisiting the learning objectives associated with participation in this professional doctorate. From the outset the researcher acknowledged a level of competence across all learning areas, however, identified that improvement as a practitioner would be enhanced by focusing on methodological and personal/social capabilities. The learning objectives for this learning journey included:

Intellectual capabilities

1. Enhance theoretical knowledge by developing greater understanding of risk management and insider threat and use and apply this enhanced theoretical knowledge through practical application and articles.
2. Enhance professional knowledge, tolerance for ambiguity and critical judgement by increasing understanding of insider threat through use of high level research skills and synthesise this knowledge into a survey for assessing organisational vulnerability to IIT.

Methodological capabilities:

Enhance objective judgment, analytical skills, and research techniques, to develop and validate a survey to help organisations assess vulnerability to IIT.

Personal and social capabilities:

Enhance collaboration and professional knowledge by developing greater networks in risk management and with experts in CWB/Insider threat and demonstrate subject matter expertise through superior communication skills including in-house presentations and articles for publication.

Table 38 presents an overview of the learning journey and demonstrates how intellectual, methodological, and personal and social capabilities were enhanced throughout this doctorate research process.

Table 38: Achievement of learning objectives

Year	Task/Activity	Learning objective/capability
2014	Complete Candidature process	Intellectual capabilities 1 Personal and social capabilities
	Complete Ethics approval process	Intellectual capabilities 1
	Complete course on Endnote	Methodological capabilities
	Literature Review - Gather literature relevant to insider threat and risk management	Intellectual capabilities 1 and 2
	Complete course Certificate III in Government (Security)	Intellectual capabilities 1 Personal and social capabilities
2015	Synthesise relevant literature and research	Intellectual capabilities 1 and 2
	Delphi Study – review, understand, and develop	Intellectual capabilities 1 and 2 Methodological capabilities Personal and social capabilities
2016	Delphi Study – launch, completion, distill relevant themes	Intellectual capabilities 1 and 2 Methodological capabilities Personal and social capabilities
2016	Poster Presentation – 18th HCI International Conference - Canada	Personal and social capabilities
2016-2017	OVIT – development, pilot	Intellectual capabilities 1 and 2 Methodological capabilities
2017	Panel member for Cyber in Business Conference - Melbourne	Personal and social capabilities
2017-2018	OVIT – refinement and full deployment	Methodological capabilities
2018	OVIT – completion of EFA and understanding reliability and validity indicators	Methodological capabilities
2018	Completion of Thesis	Intellectual capabilities 1 and 2 Personal and social capabilities
2018	Completion of DPRS	Intellectual capabilities 1 and 2 Personal and social capabilities

Source: Developed for this study

Undertaking the current work based research has produced several benefits and numerous contributions as outlined above. From an academic perspective this thesis has contributed to organisational knowledge and understanding of IIT. The outcomes demonstrate support for a multidisciplinary approach to insider threat and emphasise the importance of a holistic approach which incorporates individual, organisational, and technical considerations. Advancement for professional practice has been accomplished through the operationalisation of IIT and an enhanced understanding of IIT in the Australian context. The OVIT provides a comprehensive working model which clearly articulates the construct, dimensions, and factors of IIT. Finally personal development has been achieved against intellectual, methodological, and, personal and social capabilities, which is consistent with lifelong learning and the scientist-practitioner model. In summary, the contributions of this study are noteworthy and demonstrate the importance of work based research for positive outcomes of academic, professional, and personal significance.

5.5 Limitations and Suggestions for Future Research

The limitations of the current research, along with the limitations of the literature, has been discussed thoroughly throughout this thesis. The limitations to the current positioning of IIT was discussed in Sections 2.1.7 and 2.4.5. Further Section 3.7 identified the confines of the current research along with relevant strategies to attempt to overcome methodological limitations.

From the beginning, this study delimited scope by focusing on IIT. In some ways the distinction between IIT and non-malicious insider threat, when looking through a risk management lense, has been argued as arbitrary. This is because organisational protective measures and mitigation strategies are seen to be of benefit regardless of the insider's intent (Cappelli et al. 2012; Pfleeger et al. 2010).

It has been highlighted throughout this thesis that the study of IIT is considered complex and difficult, and that the overall body of literature has been referred to as biased, insufficient, and lacking (Festa 2012a). The dearth of Australian representation on the topic is evident. Hence, the current research provided a means

of filling this gap. In doing so, however, it is presented with its own limitation; that is, a lack of generalisability to a broader population. It is possible that Australian expert opinion and experience differs from that of experts in other countries. Given this, it would be unwise to suggest the findings can be generalised internationally without further comparative research.

As Yin (1984) discussed, all research design and methods have advantages and disadvantages. In the current study an alignment with the pragmatic paradigm and mixed methods approach presents a rigorous research framework but also a recognised set of limitations. A common reference in the insider threat literature is that research has relied upon surveys and convenience samples raising questions regarding the generalisability of results (Hunker & Probst 2011; Randazzo et al. 2005). Here too, a survey design with a non-purposive and convenience sampling technique faces the same fate. As such, a broader qualitative enquiry, utilising interviews and real case studies, may have contributed further insights on IIT and helped alleviate some of these concerns. Still, the use of mixed methods in the research design contributes to the depth and breadth of research outcomes. However, the results are still limited by the exploratory and cross-sectional approach. The ability to generalise findings and assert causality is restricted and only overcome by capacity for future longitudinal research (Creswell 2014).

For organisations, the ability to identify and assess their risk to IIT is important and the utility of the OVIT may be in providing a baseline for future comparison (Frangopoulos et al. 2013). However, the strongest validation for the OVIT would be in its ability to predict actual insider exploits. The capacity to assert that the variables, factors, and dimensions, presented by the OVIT are linked to IIT occurrence rates requires validation of the hypothesised relationships through a longitudinal study (Greitzer et al. 2009; Hunker & Probst 2011). This same research could also help further determine construct validity especially discriminant validity.

Discriminant validity is the determination that conceptually similar concepts are in fact distinct (Neuman 2011). In the current study, the conceptualisation of insider

threat relies on some level of separation between individual, organisational, and technical dimensions. It is the overlap of vulnerabilities between these foci which are hypothesised to lead to insider threat potential. Given this assumption, it may be academically important to establish discriminant validity of the three inventories.

As with many exploratory studies, the issue of sample size has arisen. The pilot numbers did meet recommendations by several researchers (Johanson & Brooks 2010), however, the pilot sample was not sufficient to satisfy minimum requirements for statistical analyses. Instead it allowed for pragmatic input including content, comprehension, and presentation. Also, the study aimed to achieve 200 participants for the final OVIT analyses but due to difficulty in recruiting management level participants and time poor responders, only 141 valid responses was achieved.

The multivariate analysis of choice, the EFA, has been criticised for its subjectivity and heavy reliance on researcher decision making (Tabachnick & Fidell 2007; Williams et al. 2010). Reducing this bias is difficult but was attempted in the current research through ongoing expert, colleague, and supervisor input. Given that EFA is an exploratory procedure and is not designed to test hypotheses or theories, researchers caution against drawing substantive conclusions (Costello & Osborne 2005). As such, further research is required to substantiate the findings of the current study. Future projects may include use of factor scores in a regression to predict behavioural outcomes or CFA to validate the factorial validity of the model derived from the EFA (Hair et al. 2010).

Another caution of this work-based research related to sample size is the existence of a Heywood case in the OVIT-Individual sub-inventory. An Heywood case is represented by a communality equal to or greater than one (Harris 2001). Whilst there is debate about whether a Heywood case alone invalidates a solution, the absence of a Heywood case would present a more statistically robust representation of the individual dimension. Continuing to gather responses to the OVIT and increase the sample size may result in eradicating the Heywood concern (de Winter et al. 2009).

Looking at the practical application of the OVIT moves beyond the methodological and statistical limitations. More recently there has been a focus on ethical and legal considerations of insider threat initiatives. This work-based research has not explored the potential legal and ethical constraints for organisations adopting the OVIT. As such, further consideration of the legal ramifications of employing formalised insider threat initiatives is encouraged (Huth 2013). Whilst this research and the resultant measurement instruments does not look specifically at how to implement countermeasures, it does highlight the areas of concern which may benefit from active mitigation. Proactive mitigation may be considered invasive and excessive (Hunker & Probst 2011) and therefore should be managed with consideration and care.

Finally, it is important to acknowledge the ever-changing landscape of IIT and the importance that the OVIT remains current. The inventories are based on literature review, expert opinions, and statistical analyses conducted between 2014 and 2018. The inventories are therefore limited to what was known about IIT at the time or what the Delphi experts were able to forecast. In order to remain relevant the OVIT will require ongoing review and change is expected. As new technologies arise and the landscape of insider threat changes the OVIT, without updating, could become obsolete. Certainly IIT will be affected by the fast paced technological and social changes in the workplace (Colwill 2010). Insider threat motivation has demonstrated change. Initial and early studies highlighted the financial drivers, with more recent research identifying a shift to ideological and mixed motivations (Fischer 2000; Herbig 2008; Randazzo et al. 2005; Shaw et al. 2009) Therefore, maintaining a focus on IIT trends, changes in the IIT space, new research, ongoing commitment to infusing expert knowledge, and ongoing research will help maintain relevance. This approach is also consistent with pragmatic paradigm which encourages change for better utility and real world application.

5.6 Summary

This chapter has discussed the research findings, implications of results, limitations of the study, and suggestions for future research. The pragmatic paradigm provided

the opportunity to explore IIT from a practical and applied perspective but within a rigorous approach to academic research. As such, this exploratory research has been able to investigate and operationalise organisational vulnerability to IIT in a manner which was able to contribute to theory, practice, and the self.

This work-based research was borne out of a professional interest to investigate the construct of organisational vulnerability to IIT. Gaining a deeper understanding of IIT through the review of current literature and insights from Australian experts provided the opportunity to develop statistically derived, robust, reliable, and valid inventories aimed at diagnosing organisational vulnerability to IIT. This study has produced three inventories assessing different dimensions of IIT (Individual, Organisational, and Technical) as well as a working model conceptualising and operationalising organisational vulnerability to IIT.

Undertaking the Doctorate of Professional Studies has provided the opportunity to study organisational vulnerability to IIT through a rigorous approach to research. However, the outcomes and contributions go beyond the academic sphere. The success of this exploratory research is evident, not only in the research outcomes but also in the professional and personal contributions and achievement. Certainly the additional contributions to theory and methodology through use of the Delphi approach, underpinning risk management principles, and assumed pragmatic worldview have enhanced the broader utility of the study. Furthermore, applied and ancillary contributions, including an Australian definition and embryonic contribution to foresight and futures studies cannot be overlooked. Beyond the academic and practise contribution there is also recognition of oneself as a research practitioner with the capacity to contribute to the field of IIT.

References

Adler, M & Ziglio, E 1996, *Gazing into the oracle: the Delphi method and its application to social policy and public health*, Jessica Kingsley Publishers, London.

Agrafiotis, I, Nurse, JRC, Buckley, O, Legg, P, Creese, S & Goldsmith, M 2015, 'Identifying attack patterns for insider threat detection', *Computer Fraud & Security*, vol. 2015, no. 7, pp. 9-17.

Alavi, R, Islam, S & Mouratidis, H 2014, 'A conceptual framework to analyze human factors of information security management system (ISMS) in organizations', *Human Aspects of Information Security, Privacy, and Trust: Second International Conference,* Part of HCI International 2014, Heraklion, Crete, Greece, June 22-27, 2014, pp. 297-305.

Alessi, E & Martin, JI 2010, 'Conducting an internet-based survey: benefits, pitfalls, and lessons learned', *Social Work Research*, vol. 34, no. 2, pp. 122-8.

Andretta, M 2014, 'Some considerations on the definition of risk based on concepts of systems theory and probability', *Risk Analysis*, vol. 34, no. 7, pp. 1184-95.

Armsby, P 2000, 'Methodologies of work based learning', in D Portwood & C Costley (eds), *Work based learning and the university: new perspectives and practices*, Staff and Educational Development Association, Birmingham, West Midlands, pp. 35-42.

Attorney General's Department 2016, *Protective Security Policy Framework*, Commonwealth Government, Canberra, ACT, viewed 11 September 2016, <https://www.protectivesecurity.gov.au/Pages/default.aspx>.

Attorney General's Department 2018, *Right to self-determination*, Commonwealth Government, Canberra, ACT, viewed 21 January 2018, <https://www.ag.gov.au/RightsAndProtections/HumanRights/Human-rights-scrutiny/PublicSectorGuidanceSheets/Pages/Righttoselfdetermination.aspx>.

Australian Cyber Security Centre 2015, *Australian Cyber Security Centre threat report 2015*, Australian Cyber Security Centre, Canberra, ACT, viewed 28 July 2016,<https://acsc.gov.au/publications/ACSC_Threat_Report_2015.pdf>.

Aven, T 2013, 'On how to deal with deep uncertainties in a risk asessment and management context', *Risk Analysis*, vol. 33, no. 12, pp. 2082-91.

Aven, T & Zio, E 2014, 'Foundational issues in risk assessment and risk management', *Risk Analysis*, vol. 34, no. 7, pp. 1164-72.

Band, SR, Cappelli, DM, Fischer, LF, Moore, AP, Shaw, ED & Trzeciak, RF 2006, *Comparing insider IT sabotage and espionage: a model-based analysis*, Carnegie Mellon University, Pittsburgh,PA,<ftp://ftp.sei.cmu.edu/pub/documents/06.reports/pdf/06tr026.pdf>.

Baracaldo, N & Joshi, J 2013, 'An adaptive risk management and access control framework to mitigate insider threats', *Computers & Security*, vol. 39, pp. 237-54.

Bartol, K, Tein, M, Matthews, G & Sharma, B (eds) 2008, *Management: a Pacific Rim focus*, 5th edition, McGraw-Hill, North Ryde, NSW.

Benozzo, A & Colley, H 2007, 'Emotion and learning in the workplace: critical perspectives', *The Journal of Workplace Learning*, vol. 24, no. 5, pp. 304-16.

Bishop, M, Engle, S, Frincke, D, Gates, C, Greitzer, F, Peisert, S & Whalen, S 2010, 'A risk management approach to the "insider threat"', in CW Probst, et al. (eds), *Insider threats in cyber security*, Springer US, Boston, MA, vol. 49, pp. 115-37.

Bojanc, R & Jerman-Blažič, B 2013, 'A quantitative model for information-security risk management', *Engineering Management Journal*, vol. 25, no. 2, pp. 25-37.

Borrett, M, Carter, R & Wespi, A 2013, 'How is cyber threat evolving and what do organisations need to consider?', *Journal of Business Continuity & Emergency Planning*, vol. 7, no. 2, pp. 163-71.

Borum, R, Felker, J, Kern, S, Dennesen, K & Feyes, T 2015, 'Strategic cyber intelligence', *Information & Computer Security*, vol. 23, no. 3, pp. 317-32.

Bowen, BM, Salem, MB, Keromytis, AD & Stolfo, SJ 2010, 'Monitoring technologies for mitigating insider threats', in CW Probst, et al. (eds), *Insider threats in cyber security*, Springer US, Boston, MA, pp. 197-217.

Brackney, R & Anderson, R 2004, *Understanding the insider threat*, RAND Corporation, Santa Monica, CA, viewed 22 June 2014, <http://www.rand.org/pubs/conf_proceedings/CF196/index.html>.

Brady, SR 2015, 'Utilizing and adapting the Delphi method for use in qualitative research', *International Journal of Qualitative Methods*, vol. 14, no. 5, pp. 1-6.

Brewer, E 2007, *Delphi technique. Encyclopedia of measurement and statistics*, Sage Publications, Thousand Oaks, CA.

Brown, JD 2009, 'Choosing the right type of rotation in PCA and EFA', *JALT Testing & Evaluation SIG Newsletter*, vol. 13, no. 3, pp. 20-5, viewed 10 June 2018, <http://hosted.jalt.org/test/PDF/Brown31.pdf>

Cabrera-Nguyen, P 2010, 'Author guidelines for reporting scale development and validation results in the Journal of the Society for Social Work and Research', *Journal of the Society for Social Work and Research*, vol. 1, no. 2, pp. 99-103.

Campbell, SM 2004, 'How do stakeholder groups vary in a Delphi technique about primary mental health care and what factors influence their ratings?', *Quality and Safety in Health Care*, vol. 13, no. 6, pp. 428-34.

Cappelli, DM & Moore, AP 2010, *Risk mitigation strategies: lessons learned from actual insider attacks*, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, viewed 07 February 2016, <https://resources.sei.cmu.edu/asset_files/Presentation/2008_017_001_52131.pdf>.

Cappelli, DM, Moore, AP & Shaw, E 2006, *A risk mitigation model: lessons learned from actual insider sabotage*, Software Engineering Institute and Carnegie Mellon University, Pittsburgh, PA, viewed 07 February 2016, <http://resources.sei.cmu.edu/asset_files/Presentation/2006_017_001_52084.pdf>.

Cappelli, DM, Moore, AP & Trzeciak, RF 2012, *The CERT guide to insider threats: how to prevent, detect, and respond to information technology crimes (theft, sabotage, fraud)*, Pearson Education Inc, New Jersey.

Carnegie Mellon University 2016, *Software Engineering Institute*, Carnegie Mellon University, Pittsburh, PA, viewed 28 August 2016, <http://www.cert.org/insider-threat/>.

Carpenter, D, McLeod, A, Hicks, C & Maasberg, M 2018, 'Privacy and biometrics: an empirical examination of employee concerns', *Information Systems Frontiers*, vol. 20, no. 1, pp. 91-110.

Catrantzos, N 2012, *Managing the insider threat: no dark corners*, CRC Press, Boca Raton, Florida.

Cert Australia & Australian Cyber Security Centre 2015, *2015 Cyber security survey: major Australian businesses*, Australian Cyber Security Centre, Canberra, ACT, viewed 07 December 2016,<https://acsc.gov.au/publications/ACSC_CERT_Cyber_Security_Survey_2015.pdf>.

Chinchani, R, Iyer, A, Ngo, HQ & Upadhyaya, S 2005, 'Towards a theory of insider threat assessment', The International Conference on Dependable Systems and Networks, 28 June-1 July 2005, Yokohama, Japan, pp. 108-117.

Cho, I & Lee, K 2016, 'Advanced risk measurement approach to insider threats in cyberspace', *Intelligent Automation & Soft Computing*, vol. 22, no. 3, pp. 405-13.

Choo, K-KR, Bishop, M, Glisson, W & Nance, K 2018, 'Internet- and cloud-of-things cybersecurity research challenges and advances', *Computers & Security*, vol. 74, pp. 275-6.

Civiello, CL 1999, 'Cyberspace, trusted insiders, and organizational threat', *The Psychologist-Manager Journal*, vol. 3, no. 2, pp. 149-66.

Clarke, CJ & Varma, S 1999, 'Strategic risk management: the new competitive edge', *Long Range Planning*, vol. 32, no. 4, pp. 414-24.

Clearswift 2013, *The enemy within research 2013*, Clearswift, Theale, UK, viewed 07 February 2016, <https://www.clearswift.com/about-us/pr/press-releases/enemy-within-research-2013>.

Clegg, SR & Bailey, JR (eds) 2008, *International encyclopedia of organization studies*, 4 vols., Sage Publications, Thousand Oaks, California.

Cole, E 2006, *Insider threat protecting the enterprise from sabotage, spying, and theft*, Syngress, Rockland Mass.

Coles-Kemp, L & Theoharidou, M 2010, 'Insider threat and information security management', in CW Probst, et al. (eds), *Insider threats in cyber security*, Springer US, Boston, MA, pp. 45-71.

Colwill, C 2010, 'Human factors in information security: the insider threat - who can you trust these days?', *Information Security Technical Report*, vol. 14, pp. 186-96.

Comrey, AL & Lee, HB 2013, *A first course in factor analysis*, 2nd edn, Psychology Press, New York.

Cooper, HM 1988, 'Organizing knowledge synthesis: a taxonomy of literature reviews', *Knowledge in Society*, vol. 1, no. 104-126.

Corlett, S 2012, *'Participant learning in and through research as reflexive dialogue: being 'struck' and the effects of recall*, Sage Full-Text Collections, Humanities & Social Sciences, 10 August 2014.

Costa, DL, Collins, ML, Perl, SJ, Albrethsen, MJ, Silowash, GJ & Spooner, D 2014, *An ontology for insder threat indicators: development and applications*, Software Engineering Institute, Pittsburgh, PA, viewed 07 February 2016,<http://resources.sei.cmu.edu/asset_files/conferencepaper/2014_021_001_426817.pdf>.

Costello, AB & Osborne, J 2005, 'Best practices in exploratory factor analysis: four recommendations for getting the most from your analysis', *Practical Assessment*, vol. 10, no. 7, pp. 1-9.

CPNI 2013, *CPNI insider data collection study: report of main findings*, CPNI, UK, viewed 21 June 2014, <http://www.cpni.gov.uk/Documents/Publications/2013/2013003-insider_data_collection_study.pdf>.

CPNI & PA Consulting Group 2012, *Holistic management of employee risk (HoMER)*, CPNI, UK, viewed 21 June 2014,<http://www.cpni.gov.uk/advice/personnel-security1/homer>.

Crampton, J & Huth, M 2010, 'Towards an access-control framework for countering insider threats', in CW Probst, et al. (eds), *Insider threats in cyber security*, Springer US, Boston, MA, pp. 173-95.

Creswell, J, Clark, P, Gutmann, M & Hanson, W 2003, 'Advanced mixed methods research designs', in A Tashakkori & C Teddlie (eds), *Handbook of mixed methods in social and behavioral research*, Sage Publications, Thousand Oaks, California, pp. 209-40.

Creswell, JW 2009, *Research design : qualitative, quantitative, and mixed methods approaches*, 3rd edn, Sage Publications, Thousand Oaks, California.

Creswell, JW 2011, *Designing and conducting mixed methods research*, 2nd edn, Sage Publications, Los Angeles.

Creswell, JW 2014, *Research design: qualitative, quantitative, and mixed method approaches*, 4th edn, Sage Publications, Los Angeles.

CSO Magazine, U. S. Secret Service, Software Engineering Institute & Price Waterhouse Cooper 2014, *2014 US State of Cybercrime Survey*, Carnegie Mellon University, Pittsburgh, PA, viewed 28 July 2016,<http://resources.sei.cmu.edu/asset_files/Presentation/2014_017_001_298322.pdf>.

Cyber Security Division 2009, *A roadmap for cybersecurity research*, Department of Homeland Security, Washington D. C, viewed 07 February 2016,<https://www.dhs.gov/sites/default/files/publications/CSD-DHS-Cybersecurity-Roadmap.pdf>.

Cycyota, CS & Harrison, DA 2006, 'What (not) to expect when surveying executives: a meta-analysis of top manager response rates and techniques over time', *Organizational Research Methods*, vol. 9, no. 2, pp. 133-60.

Daft, RL 2007, *Organization theory and design*, 9th edn, South Western, Mason, Ohio.

de Meyrick, J 2003, 'The Delphi method and health research', *Health Education*, vol. 103, no. 1, pp. 7-16.

de Winter, JCF, Dodou, D & Wieringa, PA 2009, 'Exploratory factor analysis with small sample sizes', *Multivariate Behavioral Research*, vol. 44, no. 2, pp. 147-81.

Deloitte 2015, *Responding to cyber threats in the new reality: a shift in paradigm is vital*, Deloitte & Touche LLP, Singapore, viewed 05 January 2016,<https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-thought-leadership-noexp.pdf>.

Desai, MS & von der Embse, TJ 2008, 'Managing electronic infomraiton: an ethics perspective', *Information Management & Computer Security*, vol. 16, no. 1, pp. 20-7.

Diamond, IR, Grant, RC, Feldman, BM, Pencharz, PB, Ling, SC, Moore, AM & Wales, PW 2014, 'Defining consensus: a systematic review recommends methodologic criteria for reporting of Delphi studies', *Journal of clinical epidemiology*, vol. 67, no. 4, pp. 401-9.

Dionne, G 2013, 'Risk management: history, definition, and critique', *Risk Management and Insurance Review*, vol. 16, no. 2, pp. 147-66.

Director of Central Intelligence 1990, *Project SLAMMER Interim Report*, FBI, Washington D. C., viewed 07 February 2016,<https://www.cia.gov/library/readingroom/docs/DOC_0000218679.pdf>.

Dorminey, J, Fleming, AS, Kranacher, M-J & Riley Jr, RA 2012, 'The evolution of fraud theory', *Issues in Accounting Education*, vol. 27, no. 2, pp. 555-79.

Elo, S & Kyngäs, H 2008, 'The qualitative content analysis process', *Journal of Advanced Nursing*, vol. 62, no. 1, pp. 107-15.

Engel, RJ & Schutt, RK 2009, *The practice of research in social work*, Sage Publications, Thousand Oaks, California.

Epifantsev, BN, Zhumazhanova, SS & Lozhnikov, PS 2016, 'Insider threats to information security: problem areas in neutralization', *17th International Conference of Young*

Specialists on Micro/Nanotechnologies and Electron Devices (EDM), Erlagol, Russia, pp. 133-136.

Etikan, I 2016, 'Comparison of convenience sampling and purposive sampling', *American Journal of Theoretical and Applied Statistics*, vol. 5, no. 1, pp. 1-4.

Farahmand, F & Spafford, E 2013, 'Understanding insiders: an analysis of risk-taking behavior', *Information Systems Frontiers*, vol. 15, no. 1, pp. 5-15.

Fenz, S, Ekelhart, A & Neubauer, T 2011, 'Information security risk management: in which security solutions is it worth investing', *Communications of the Association for Information Systems*, vol. 28, no. 1, pp. 329-56.

Fenz, S, Heurix, J, Neubauer, T & Pechstein, F 2014, 'Current challenges in information security risk management', *Information Management & Computer Security*, vol. 22, no. 5, pp. 410-30.

Festa, JP 2012a, 'New technologies and emerging threats: personnel security adjudicative guidelines in the age of social networking', MA thesis, Naval Postgraduate School, Monterey, California.

Festa, JP 2012b, *New technologies and emerging threats: personnel security adjudicative guidelines in the age of social networking*, DTIC Document.

Field, A 2013, *Discovering statistics using IBM SPSS statistics: and sex and drugs and rock 'n' roll*, 4th edn, Sage Publications, Los Angeles.

Fischer, LF 2000, *Espionage: why does it happen?*, DoD Security Institute, Quantico, viewed 27 June 2016, <http://www.hanford.gov/files.cfm/whyhappens.pdf>.

Flegel, U, Vayssière, J & Bitz, G 2010, 'A state of the art survey of fraud detection technology', in CW Probst, et al. (eds), *Insider threats in cyber security*, Springer US, Boston, MA, pp. 73-84.

Flowerday, SV & Tuyikeze, T 2016, 'Information security policy development and implementation: the what, how and who', *Computers & Security*, vol. 61, pp. 169-83.

Ford, J, Willey, L, White, BJ & Domagalski, T 2015, 'New concerns in electronic employee monitoring: have you checked your policies lately?', *Journal of Legal, Ethical & Regulatory Issues*, vol. 18, no. 1, pp. 51-70.

Frangopoulos, ED, Eloff, MM & Venter, LM 2013, 'Psychosocial risks: can their effects on the security of information systems really be ignored?', *Information Management & Computer Security*, vol. 21, no. 1, pp. 53-65.

Funston, F & Wagner, S 2010, *Surviving and thriving in uncertainty: creating the risk intelligent enterprise*, Wiley, Hoboken, New Jersey.

Gelles, MG 2016, *Insider Threat : Prevention, Detection, Mitigation, and Deterrence*, Butterworth-Heinemann, US.

Gelles, MG & Mitchell, K 2015, 'Top 10 considerations for building an insider threat mitigation program', *Journal of Threat Assessment and Management*, vol. 2, no. 3-4, pp. 255-7.

Gorusch, RL 1983, *Factor analysis*, 2nd edn, Lawrence Erlbaum Associates, Inc., Hillsdale, NJ.

Grace, MF, Leverty, JT, Phillips, RD & Shimpi, P 2015, 'The value of investing in enterprise risk management', *Journal of Risk and Insurance*, vol. 82, no. 2, pp. 289-316.

Graham, JM, Guthrie, AC & Thompson, B 2003, 'Consequences of not interpreting structure coefficients in published CFA research: a reminder', *Structural Equation Modeling: A Multidisciplinary Journal*, vol. 10, no. 1, pp. 142-53.

Greitzer, FL & Hohimer, RE 2011, 'Modeling human behavior to anticipate insider attacks', *Journal of Strategic Security*, vol. 4, no. 2, pp. 25-48.

Greitzer, FL, Kangas, LJ, Noonan, CF, Brown, CR & Ferryman, T 2013, 'Psychosocial modeling of insider threat risk based on behavioral and word use analysis', *e-Service Journal*, vol. 9, no. 1, pp. 106-38.

Greitzer, FL, Paulson, RP, Lars, JK, Lyndsey, RF, Thomas, WE & Frincke, D, A. 2009, *Predictive modeling for insider threat mitigation*, Department of Energy, Springfield, VA, viewed 07 February 2016,<http://www.pnl.gov/CogInformatics/media/pdf/TR-PACMAN-65204.pdf>.

Guadagnoli, E & Velicer, WF 1988, 'Relation to sample size to the stability of component patterns', *Psychological Bulletin*, vol. 103, no. 2, pp. 265-75.

Gutierrez, O 1989, 'Experimental techniques for information requirements analysis', *Information & Management*, vol. 16, no. 1, pp. 31-43.

Hair, JF, Black, WC, Babin, BJ & Anderson, RE 2010, *Multivariate data analysis: a global perspective*, 7th edn, Pearson Education, Upper Saddle River, NJ.

Hall, DB & Wang, L 2005, 'Two-component mixtures of generalized linear mixed effects models for cluster correlated data', *Statistical Modeling*, vol. 5, no. 1, pp. 21-37.

Hanson, W, Creswell, JW, Clark, V, Petska, K & Creswell, JD 2005, 'Mixed methods research design in counselling psychology', *Journal of Counselling Psychology*, vol. 52, no. 2, pp. 224-35.

Harle, P, Havas, A, Kremer, A, Rona, D & Samandari, H 2016, *The future of bank risk managment*, McKinsey & Company, London, UK, viewed 28 December 2017, <https://www.mckinsey.com/business-functions/risk/our-insights/the-future-of-bank-risk-management>.

Harris, RJ 2001, *A primer of multivariate statistics*, 3rd edn, Lawrence Erlbaum Associates, Mahwah, N.J.

Hart, C 1998, *Doing a literature review: releasing the social science research imagination*, Sage Publications, London.

Hasson, F, Keeney, S & McKenna, H 2000, 'Research guidelines for the Delphi survey technique', *Journal of Advanced Nursing*, vol. 32, no. 4, pp. 1008-15.

Herbig, KL 2008, *Changes in Espionage by Americans, 1947-2007*, Department of Defense Personnel Security Research Center, Monterey, CA, viewed 29 March 2016, <http://www.dhra.mil/perserec/reports/tr08-05.pdf>.

Hewes, CA, Jr. 2016, 'Threat and challenges of cyber-crime and the response', *SAM Advanced Management Journal*, vol. 81, no. 2, p. 4.

Homeland Security 2009, *Current hard problems in INFOSEC research*, The Department of Homeland Security, Washington, D. C, viewed 21 September 2016, <https://www.dhs.gov/sites/default/files/publications/CSD-DHS-Cybersecurity-Roadmap.pdf>.

Homeland Security 2011, *Risk management fundamentals: Homeland secuirty risk managmeent doctrine*, The Department of Homeland Security, Washington, D. C, viewed 02 July 2016, <https://www.dhs.gov/publication/risk-management-fundamentals>.

Hooper, D 2012, 'Exploratory Factor Analysis', in H Chen (ed.), *Approaches to quantitative research – theory and its practical application: a guide to dissertation students*, Oak Tree Press, Cork, Ireland.

Hopkin, P 2014a, *Fundamentals of risk management understanding, evaluating and implementing effective risk management*, 3rd edn, Kogan Page, London.

Hopkin, P 2014b, 'Achieving enhanced organisational resilience by improved management of risk: summary of research into the principles of resilience and the practices of resilient organisations', *Journal of Business Continuity & Emergency Planning*, vol. 8, no. 3, pp. 252-62.

Horton, A 1999, 'A simple guide to successful foresight', *foresight*, vol. 1, no. 1, pp. 5-9.

Hu, Q, Dinev, T, Hart, P & Cooke, D 2012, 'Managing employee compliance with information secuirty policies: the critical role of top managment and organizational culture', *Decision Sciences*, vol. 43, no. 4, pp. 615-59.

Hunker, J & Probst, CW 2011, 'Insiders and insider threats - an overview of defnitions and mitigation techniques', *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 2, no. 1, pp. 4-27.

Huth, CL 2013, 'The insider threat and employee privacy: An overview of recent case law', *Computer Law & Security Review*, vol. 29, no. 4, pp. 368-81.

Intelligence and National Security Alliance 2013, *Preliminary examination of insider threat programs in the United States private sector*, Arlington, VA, viewed 20 September 2016, <http://www.insaonline.org/i/d/a/b/InsiderThreat_embed.aspx>.

IP Australia 2018, *Understanding IP*, Commonwealth Government, Canberra, ACT, viewed 21 January 2018, <https://www.ipaustralia.gov.au/understanding-ip>.

Jackson, DL, Gillaspy, JA & Purc-Stephenson, R 2009, 'Reporting practices in Confirmatory Factor Analysis: an overview and some recommendations', *Psychological Methods*, vol. 14, no. 1, pp. 6-23.

Johanson, GA & Brooks, GP 2010, 'Initial scale development: sample size for pilot studies', *Educational and Psychological Measurement*, vol. 70, no. 3, pp. 394-400.

Jones, JL & Mehr, SL 2007, 'Foundations and assumptions of the scientist-practitioner model', *American Behavioral Scientist*, vol. 50, no. 6, pp. 766-71.

Jones, MJ 1999, 'Critically evaluating an applications vs theory framework for research quality', *Omega*, vol. 27, no. 3, pp. 397-401.

Keeney, MM, Kowalski, EF, Cappelli, DM, Moore, AP, Shimeall, TJ & Rogers, SN 2005, *Insider threat study: computer system sabotage in critical infrastructure sectors* U.S. Secret Service and CERT Coordination Center, Washington, DC, viewed 01 July 2016, <http://resources.sei.cmu.edu/asset_files/SpecialReport/2005_003_001_51946.pdf>.

Keeney, S, McKenna, H & Hasson, F 2010, *The Delphi technique in nursing and health research*, John Wiley & Sons, Chichester, UK.

Khan, SA & Khan, RA 2014, 'Security assessment framework: a complexity perspective', *Computer Fraud & Security*, vol. 2014, no. 7, pp. 13-7.

Kline, RB 2005, *Principles and practice of structural equation modeling*, 2nd edn, Guilford Press, New York.

Kowalski, E, Conway, S, Keverline, M, Williams, D, Cappelli, DM, Willke, B & Moore, AP 2008, *Insider threat study: illicit cyber activity in the Government sector*, Software Engineering Institute CERT Program at Carnegie Mellon University, Pittsburgh, PA, viewed 23 November 2016, <http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=52227>.

KPMG 2012, *India Fraud Survey Report 2012*, http://www.kpmg.com/IN/en/IssuesAndInsights/ArticlesPublications/Documents/Evolution_of_fraud_inIndia.pdf >.

Kraemer, S, Carayon, P & Clem, J 2009, 'Human and organizational factors in computer and information security: pathways to vulnerabilities', *Computers & Security*, vol. 28, pp. 509-20.

Kroll 2015, *Global fraud report: vulnerabilties on the rise*, Kroll, New York, viewed 28 July 2016, <http://www.kroll.com/global-fraud-report>.

Kuckartz, U 2014, *Qualitative text analysis: a guide to methods, practice & using software*, SAGE Publications Ltd, London, viewed 19 January 2018, <http://methods.sagepub.com/book/qualitative-text-analysis>.

Landeta, J 1999, *El método Delphi: una técnica de previsión para la incertidumbre*, Ariel, Barcelona.

Lang, T 2001, *An overview of four futures methodologies (Delphi, environmental scanning, issues management and emerging issue analysis)*, Hawaii, viewed 09 January 2018, <http://158.132.155.107/posh97/private/research/methods-delphi/LANG.html>.

Lavrakas, PJ 2008, *Encyclopedia of Survey Research Methods*, Sage Publications., London, United Kingdom, viewed 22 January 2015, <http://dx.doi.org.ezproxy.usq.edu.au/10.4135/9781412963947>.

Lee, CC, Lee, C & Kim, S 2016, 'Understanding information security stress: focusing on the type of information security compliance activity', *Computers & Security*, vol. 59, pp. 60-70.

Legg, P, Moffat, N, Nurse, J, Happa, J, Agrafiotis, I, Goldsmith, M & Creese, S 2013, 'Towards a conceptual model and reasoning structure for insider threat detection', *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 4, no. 4, pp. 20-37.

Leitch, M 2010, 'ISO 31000:2009—The new international Standard on risk management', *Risk Analysis*, vol. 30, no. 6, pp. 887-92.

Leitch, M 2017, 'The risk management gap', *Board Leadership*, vol. 2017, no. 154, pp. 1-3.

Liang, NP & Biros, D 2016, 'Validating common characteristics of malicious insiders: Proof of concept study', *49th Hawaii International Conference on System Sciences (HICSS)*, Koloa, HI, USA, pp. 3716-3726.

Lilja, KK, Laakso, K & Palomki, J 2011a, 'Using the Delphi method', in Technology Management in the Energy Smart World (PICMET), 2011 Proceedings of PICMET '11:: *proceedings of theTechnology Management in the Energy Smart World (PICMET), 2011 Proceedings of PICMET '11:* pp. 1-10.

Lilja, KK, Laakso, K & Palomki, J 2011b, 'Using the Delphi method', *Technology Management in the Energy Smart World (PICMET '11)*, Portland, Oregon, USA, 31 July - 04 August 2011, pp. 1-10.

Ludwig, B 1997, 'Predicting the future: have you considered the Delphi methodology?', *Journal of Extension*, vol. 35, pp. 1-4.

Luko, SN 2013, 'Risk management terminology', *Quality Engineering*, vol. 25, no. 3, pp. 292-7, viewed 30 August 2015, <http://dx.doi.org/10.1080/08982112.2013.786336>

Lundberg, R & Willis, H 2015, 'Assessing Homeland security risks: a comparative assessment of ten hazards', *Homeland Security Affairs*, vol. 11, article 10, viewed 05 November 2015, < https://www.hsaj.org/articles/7707>

MacCallum, RC, Widaman, KF, Zhang, S & Hong, S 1999, 'Sample size in factor analysis', *Psychological Methods*, vol. 4, no. 1, pp. 84-99.

Mackenzie, N & Knipe, S 2006, 'Research dilemmas: paradigms, methods and methodology', *Issues in Educational Research*, vol. 16, no. 2, pp. 193-205.

Magklaras, G & Furnell, S 2010, 'Insider threat specification as a threat mitigation technique', in CW Probst, et al. (eds), *Insider threats in cyber security*, Springer US, Boston, MA, pp. 219-44.

McKenna, H 1994, 'The Delphi technique: a worthwhile approach for nursing?', *Journal of Advanced Nursing*, vol. 19, pp. 1221-5.

Meijering, JV, Kampen, JK & Tobi, H 2013, 'Quantifying the development of agreement among experts in Delphi studies', *Technological Forecasting and Social Change*, vol. 80, no. 8, pp. 1607-14.

Moore, A, Cappelli, D, Caron, T, Shaw, E, Spooner, D & Trzeciak, R 2011, *A preliminary model of insider theft of intellectual property*, Software Engineering Institute, Carnegie Mellon University, Pittsburg, PA, viewed 28 July 2016, <http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=9855>.

Moore, AP, Cappelli, DM & Trzeciak, RF 2008, 'The "big picture" of insider IT sabotage across U.S. critical infrastructures', in SJ Stolfo, et al. (eds), *Insider Attack and Cyber Security: Beyond the Hacker*, Springer US, Boston, MA, pp. 17-52.

Mouton, F, Leenen, L & Venter, HS 2016, 'Social engineering attack examples, templates and scenarios', *Computers & Security*, vol. 59, pp. 186-209.

Mullins, LJ 2010, *Management and organisational behaviour*, 9th edn, Financial Times Prentice Hall, Harlow.

Munshi, A, Dell, P & Armstrong, H 2012, 'Insider threat behavior factors: a comparison of theory with reported incidents', *45th Hawaii International Conference on System Sciences*, Maui, HI, USA, pp. 2402-2411.

Neuman, WL 2011, *Social research methods: qualitative and quantitative approaches*, 7th edn, Allyn and Bacon, Boston, MA.

Neumann, PG 2010, 'Combatting insider threats', in CW Probst, et al. (eds), *Insider threats in cyber security*, Springer US, Boston, MA, pp. 17-44.

Nilsen, P, Nordstrom, G & Ellstrom, P 2012a, 'Integrating research-based and practice-based knowledge through workplace reflection', *The Journal of Workplace Learning*, vol. 24, no. 6, pp. 403-15.

Nilsen, P, Nordstrom, G & Ellstrom, P 2012b, ''Integrating research-based and practice-based knowledge through workplace reflection'', *The Journal of Workplace Learning*, vol. 24, no. 6, pp. 403-15.

Nurse, J, Buckley, O, Legg, PA, Goldsmith, M, Creese, S, Wright, G & Whitty, M 2014a, 'Understanding insider threat: a framework for characterising attacks', *Security and Privacy Workshops*, 17-18 May 2014, San Jose, CA, USA. pp. 214-218.

Nurse, J, Legg, PA, Buckley, O, Agrafiotis, I, Wright, G, Whitty, M, Upton, D, Goldsmith, M & Creese, S 2014b, 'A critical reflection on the threat from human insiders – its nature, industry perceptions, and detection approaches', *Human Aspects of Information Security,*

Privacy, and Trust, Second International Conference, Held as part of HCI International, 22-27 June 2014, Heraklion, Crete, Greece, pp. 270-281.

Nurse, JRC, Erola, A, Agrafiotis, I, Goldsmith, M & Creese, S 2015, 'Smart insiders: exploring the threat from insiders using the internet-of-things', *International Workshop on Secure Internet of Things (SIoT)*, 21-25 September 2015, Vienna, Austria, pp. 5-14.

Okoli, C & Pawlowski, S 2004, 'The Delphi method as a research tool: an example, design considerations and applications', *Information and Management*, vol. 42, pp. 15-29.

Oxford Unviersity Press 2016a, *Oxford Dictionaries: Language matters*, Oxford University Press, viewed 05 November 2016, <https://en.oxforddictionaries.com/definition/risk>.

Oxford Unviersity Press 2016b, *Oxford Dictionaries: Language matters*, Oxford University Press, viewed 06 August 2016, <http://www.oxforddictionaries.com/definition/english/motivation>.

Pace, C 2016, 'Why HR and IT departments should talk talk', *Strategic HR Review*, vol. 15, no. 3, pp. 118-22.

Pansiri, J 2005, 'A methodological approach to researching strategic alliances in tourism', *Tourism and Hospitality Planning & Development*, vol. 2, no. 3, pp. 191-206.

Parsons, K, McCormac, A, Butavicius, M, Pattinson, M & Jerram, C 2014, 'Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)', *Computers & Security*, vol. 42, pp. 165-76.

Parsons, K, Young, E, Butavicius, M, McCormac, A, Pattinson, M & Jerram, C 2015, 'The influence of organizational infomration security culture on information security decision making', *Journal of Cognitive Engineering and Decision Making*, vol. 9, no. 2, pp. 117-29.

Paté-Cornell, E & Cox, LA 2014, 'Improving risk ,anagement: from lame excuses to principled practice', *Risk Analysis*, vol. 34, no. 7, pp. 1228-39.

Paulhus, DL 1998, *Paulhus Deception Scales (PDS): the balanced inventory of desirable responding-7*, Multi-Health Systems Inc., Toronto, Ontario, Canada.

PERSEREC 2016, *Welcome to PERSEREC*, The Department of Defense, Monterey, California, viewed 28 July 2016, <http://www.dhra.mil/perserec/>.

Pett, MA, Lackey, NR & Sullivan, JJ 2003, *Making Sense of Factor Analysis: The Use of Factor Analysis for Instrument Development in Health Care Research*, SAGE Publications, Thousand Oaks, California.

Pfleeger, SL, Predd, JB, Hunker, J & Bulford, C 2010, 'Insiders behaving badly: addressing bad actors and their actions', *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 1, pp. 169-79.

Powell, TC 2001, 'Competitive advantage: logical and philosophical considerations', *Strategic Management Journal*, vol. 22, no. 9, pp. 875-88.

Probst, CW, Hunker, J, Bishop, M & Gollmann, D 2008, 'Countering insider threats', Dagstuhl Seminar Proceedings, <http://drops.dagstuhl.de/opus/volltexte/2008/1793>.

Probst, CW, Hunker, J, Gollmann, D & Bishop, M 2010a, *Insider threats in cyber security*, Springer US, Boston, MA.

Probst, CW, Hunker, J, Gollmann, D & Bishop, M 2010b, 'Aspects of insider threats', in CW Probst, et al. (eds), *Insider threats in cyber security*, Springer US, Boston, MA, pp. 1-15.

Protective Security Policy Section Attorney-General's Department, *Protective security framework: securing government business,* 2010, Attorney-General's Department, Barton, ACT.

Pulver, A & Medina, RM 2018, 'A review of security and privacy concerns in digital intelligence collection', *Intelligence and National Security*, vol. 33, no. 2, pp. 241-56.

Randazzo, MR, Keeney, MM, Kowalski, EF, Cappelli, DM & Moore, AP 2005, *Insider Threat Study: Illicit cyber activity in the banking and finance sector*, Carnegie Mellon University, Pittsburgh, PA, viewed 10 September 2016, <http://www.sei.cmu.edu/reports/04tr021.pdf>.

Reid, DJ 2018, 'Combating the enemy within: regulating employee misappropriation of business information', *Vanderbilt Law Review*, vol. 71, no. 3, p. 1033.

Renaud, K & Goucher, W 2014, 'The curious incidence of security breaches by knowledgeable employees and the pivotal role a of security culture', *Human Aspects of Information Security, Privacy, and Trust, Second International Conference*, Held as part of HCI International, 22-27 June 2014, Heraklion, Crete, Greece, pp. 361-372.

Romeu, JL 2006, 'On operations research and statistics techniques: keys to quantitative data mining', *American Journal of Mathematical and Management Sciences*, vol. 26, no. 3-4, pp. 293-328.

Rowe, WD 1977, *An anatomy of risk*, Wiley, New York.

Rowley, J & Slack, F 2004, 'Conducting a literature review', *Management Research News*, vol. 27, no. 6, pp. 31-9.

Royal, K 2016, '"Face validity" is not a legitimate type of validity evidence', *American Journal of Surgery*, vol. 212, no. 5, p. 1026.

Rozell, DJ 2015, 'A cautionary note on qualitative risk ranking of Homeland Security threats.', *Homeland Security Affairs*, vol. 11, Article 3, viewed 05 November 2016, <https://www.hsaj.org/articles/1800>

Safa, NS, Maple, C, Watson, T & Von Solms, R 2018, 'Motivation and opportunity based model to reduce information security insider threats in organisations', *Journal of Information Security and Applications*, vol. 40, pp. 247-57.

Sarkar, KR 2010, 'Assessing insider threats to information security using technical, behavioural and organisational measures', *Information Security Technical Report*, vol. 15, no. 3, pp. 112-33.

Sauser, WI 2007, 'Employee theft: who, how, why, and what can be done', *Society for Advanced Management Journal*, vol. 72, no. 3, pp. 13-25.

Schoemaker, P 2015, *Strategic approaches to managing uncertainty*, The Wharton School, Philadelphia, PA, viewed 27 December 2017, <http://opim.wharton.upenn.edu/risk/conference/pprs/Schoemaker_Strategic-Approaches-to-Managing-Uncertainty.pdf>.

Schultz, E 2002, 'A framework for understanding and predicting insider attacks', *Computers & Security*, vol. 21, no. 6, pp. 523-31, viewed 30 October 2002, <https://www.sciencedirect.com/science/article/pii/S016740480201009X>

Shariff, N 2015, 'Utilizing the Delphi survey approach: a review', *Jounral of Nursing Care*, vol. 43, no. 3, pp. 246-51.

Shaw, E & Fischer, L 2005, *Ten tales of betrayal: the threat to corporate infrastructures by information technology insiders: analysis and observations*, Defense Personnel Security Research Centre, Monterey, California, viewed 21 June 2014, <http://www.dhra.mil/perserec/reports/tr05-13.pdf>.

Shaw, ED 2006, 'The role of behavioral research and profiling in malicious cyber insider investigations', *Digital Investigation*, vol. 3, no. 1, pp. 20-31.

Shaw, ED & Stock, HV 2011, *Behavioral risk indicators of malicious insider theft of intellectual property: misreading the writing on the wall*, Symantec, Mountain View, CA, viewed 27 June 2016, <http://www.symantec.com/content/en/us/about/media/pdfs/symc_malicious_insider_whitepaper_Dec_2011.pdf>.

Shaw, ED & Sellers, L 2015, 'Application of the critical-path method to evaluate insider risks', *Studies in Intelligence*, vol. 59, no. 2, pp. 1-8, viewed 01 September 2015, <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol-59-no-2/pdfs/Shaw-Critical%20Path-June-2015.pdf>

Shaw, ED, Ruby, KG & Post, JM 1998, *The insider threat to information systems: the psychology of the dangerous insider*, Department of Defense Security Institute, Richmond, VA, viewed 29 March 2016, <http://www.pol-psych.com/sab.pdf>.

Shaw, ED, Fischer, LF & Rose, AE 2009, *Insider risk evaluation and audit*, Defense Personnel Security Research Centre, Monterey, California, viewed 21 June 2014, <http://www.dhra.mil/perserec/reports/tr09-02.pdf>.

Shechter, OG & Lang, EL 2011, *Identifying personality disorders that are security risks: field test results*, Defense Personnel Security Research Center, Monterey, CA, viewed 19 June 2014, <http://www.dhra.mil/PERSEREC/Selected-Reports/#TR1105>.

Sheehan, KB 2002, 'Online research methodology: reflections and speculations', *Journal of Interactive Advertising*, vol. 3, no. 1, pp. 56-61.

Skulmoski, G, Hartman, F & Krahn, J 2007, 'The Delphi method for graduate research', *Journal of Information Technology Education*, vol. 6, pp. 1-21.

Slade, SC, Dionne, CE, Underwood, M & Buchbinder, R 2014, 'Standardised method for reporting exercise programmes: protocol for a modified Delphi study', *BMJ Open*, vol. 4, no. 12.

Sokolowski, J & Banks, C 2015, 'Agent implementation for modeling insider threat', *Winter Simulation Conference (WSC)*, 06-09 December 2015, Huntington Beach, CA, USA, pp. 266-275.

Sokolowski, JA, Banks, CM & Dover, TJ 2016, 'An agent-based approach to modeling insider threat', *Computational and Mathematical Organization Theory*, vol. 22, no. 3, pp. 273-87.

Stafford, T, Deitz, G & Li, Y 2018, 'The role of internal audit and user training in information security policy compliance', *Managerial Auditing Journal*, vol. 33, no. 4, pp. 410-24.

Standards Australia 2006, *Security risk management*, HB 167:2006, Standards Australia/Standards New Zealand, Sydney, NSW.

Standards Australia 2009, *Risk management- Principles and guidelines*, AS/NZS ISO 31000:2009, Standards Australia/Standards New Zealand, Sydney, NSW.

Tabachnick, BG & Fidell, LS 2007, *Using multivariate statistics*, Pearson Education, Boston, MA.

Tabachnick, BG & Fidell, LS 2013, *Using Multivariate Statistics*, Pearson Education, Boston, MA.

Tang, M, Li, Mg & Zhang, T 2016, 'The impacts of organizational culture on information security culture: a case study', *Information Technology and Management*, vol. 17, no. 2, pp. 179-86.

Tashakkori, A & Teddlie, C (eds) 2003, *Handbook of mixed methods in social & behavioral research*, Sage Publications, Thousand Oaks, California.

The Australian Psychological Society 2007, *Code of Ethics*, The Australian Psychological Society, Melbourne, VIC.

The National Health and Medical Research Council, The Australian Research Council Australian, & The Australian Vice-Chancellors' Committee, 2007 (updated March 2014), *National Statement on Ethical Conduct in Human Research*, Commonwealth of Australia, Canberra, ACT.

Theoharidou, M, Kokolakis, S, Karyda, M & Kiountouzis, E 2005, 'The insider threat to information systems and the effectiveness of ISO17799', *Computers & Security*, vol. 24, no. 6, pp. 472-84.

Trevelyan, EG & Robinson, PN 2015, 'Delphi methodology in health research: how to do it?', *European Journal of Integrative Medicine*, vol. 7, no. 4, pp. 423-8.

Turner, T 2015, 'The profit in proprietary education: an exploratory examination of student loan rates and earnings', *Pressacademia*, vol. 2, no. 1, pp. 79-89.

University of Southern Queensland 2014, *ICT Infromation Management and Security Policy*, Univeristy of Southern Queensland, Toowoomba, QLD, viewed 21 January 2018, <http://policy.usq.edu.au/documents/13340PL#4.3_Information_Security_and_Cyber_Security>.

Vaidyanathan, G & Berhanu, N 2012, 'Impact of security countermeasures in organizational information convergence: a theoretical model', *Issues in Information Systems*, vol. 13, no. 2, pp. 21-5.

van der Laan, L 2008, 'The imperative of strategic foresight to strategic thinking', *Journal of Futures Studies*, vol. 13, no. 1, pp. 21-42.

van der Laan, L 2014, 'Community capacity building: the question of sustainability? ', in *Community capacity building: lessons from adult learning in Australia*, NIACE, Leicester, United Kingdom, pp. 205-25.

van der Laan, L & Yap, J 2015, *Foresight and Strategy in the Asia Pacific Region : Practice and Theory to Build Enterprises of the Future*, Springer, Singapore.

van der Laan, LW 2010, 'Foresight competence and the strategic thinking of strategy-level leaders'.

van Zolingen, SJ & Klaassen, CA 2003, 'Selection processes in a Delphi study about key qualifications in Senior Secondary Vocational Education', *Technological Forecasting and Social Change*, vol. 70, no. 4, pp. 317-40.

Vashisth, A & Kumar, A 2013, 'Corporate espionage: the insider threat', *Business Information Review*, vol. 30, no. 2, pp. 83-90.

Verizon and U.S. Secret Service 2010, *2010 Data Breach Investigations Report*, Verizon, New York, viewed 07 February 2016, <http://tinyurl.com/26cqfj2>.

Von der Gracht, HA 2012, 'Consensus measurement in Delphi studies', *Technological Forecasting & Social Change*, vol. 79, no. 8, pp. 1525-36.

Webb, J, Ahmad, A, Maynard, S & Shanks, G 2014a, 'A situation awareness model for information security risk management', *Computers & Security*, vol. 44, pp. 1-15.

Webb, J, Maynard, S, Ahmad, A & Shanks, G 2014b, 'Information security risk management: an intelligence-driven approach', *Australasian Journal of Information Systems*, vol. 18, no. 3, pp. 391-404.

Wee Yong, Y, Ah Keng, K & Leng Leng, T 1989, 'A Delphi forecast for the Singapore tourism industry: future scenario and marketing implications', *European Journal of Marketing*, vol. 23, no. 11, pp. 15-26.

Werlinger, R, Muldner, K, Hawkey, K & Beznosov, K 2010, 'Preparation, detection, and analysis: the diagnostic work of IT secruity incident response', *Information Management & Computer Security*, vol. 18, no. 1, pp. 26-42.

West, S, Finch, J & Curran, P 1995, 'Structural equation models with nonnormal variables: problems and remedies.', in RH Hoyle (ed.), *Structural equation modeling: Concepts, issues and applications.*, Sage Publications, Newbery Park, CA, pp. 56-75.

Williams, B, Brown, T & Onsman, A 2010, 'Exploratory factor analysis: a five-step guide for novices', *Australasian Journal of Paramedicine*, vol. 8, no. 3, pp. 1-13.

Williams, D 2000, *Improving security within government*, news release, Inspector General of Intelligence and Security (IGIS), Canberra, viewed 19 June 2014, <http://www.igis.gov.au/public_statements/media_release/Improving_Security_Within_Government.pdf>.

Williams, PAH 2008, 'In a 'trusting' environment, everyone is responsible for information security', *Information Security Technical Report*, vol. 13, no. 4, pp. 207-15.

Worthington, RL & Whittaker, TA 2006, 'Scale development research: a content analysis and recommendations for best practices', *The Counseling Psychologist*, vol. 34, no. 6, pp. 806-38.

Yin, R 1984, *Case study research: design and methods*, Sage Publications, Beverly Hills, CA.

Yong, AG & Pearce, S 2013, 'A beginners guide to factor analysis: focusing on exploratory factor analysis', *Tutorials in Quantitative Methods for Psychology*, vol. 9, no. 2, pp. 79-94.

Young, S 2017, 'Slipping through the cracks: background investigations after Snowden', *Surveillance & Society*, vol. 15, no. 1, pp. 123-36.

Zafar, H, Ko, M & Clark, J 2014, 'Security risk management in healthcare: a case study ', *Communications of the Association for Information Systems*, vol. 34, no. 37, pp. 737-50.

Appendices

Appendix A - Delphi Email Invitation

Dear [name]

ORGANISATIONAL VULNERABILITY TO INSIDER THREAT

You are invited to participate in an important research project on the topic of organisational vulnerability to intentional insider threat. This is an exciting and important Delphi study (for more information on the Delphi method, please see below) aimed at gaining greater understanding of insider threats to organisations as distilled from the feedback from a panel of experts.

This research is being conducted by Ms Justine Bedford, a Doctoral Candidate at the University of Southern Queensland under the supervisions of Dr Luke Van der Laan (University of Southern Queensland) and Dr Janson Yap (Deloitte).

This study will extend the scope of insider threat research by examining broader organisational influences on intentional insider threat. The applied result of the project is to develop a comprehensive organisational assessment survey, in part, based on the Delphi method outcomes that can help assess how vulnerable an organisation is to intentional insider threat risks.

You can find more details of this research project in the participant information sheet attached. You can also contact me via email at justine@jconsulting.net.au.
We sincerely hope you agree to participate. To participate in the research project as a Delphi expert, please read the participant information sheet and consent form attached and respond via reply email, by the 20 November 2015, acknowledging your consent to participate.

Once your consent email is received the first round of the Delphi will be emailed to you on the 24 November 2015. Your participation in this research is very important and much appreciated by the research team.

Yours Sincerely

Justine Bedford

What is a Delphi study?
The Delphi method gathers the opinion of experts through a series of semi-structured questionnaires. The Delphi method is an iterative process whereby the results of each round are summarised and fed back to participants for further contribution and to achieve group consensus or highlight key points of difference.

Experts respond independently and anonymously. In this study the Delphi will be administered by the research team using an email platform for ease of use and efficiency.

Why have you been invited to participate?
As an established expert in the field we are keen to get your views about intentional insider threat and specifically organisational factors that may give rise / constrain such risk. If you are aware of other experts that may be interested in participating, please let me know at justine@jconsulting.net.au.

***What will you be required to do**?*
As you are an expert on insider threat, we are inviting you to participate in this research as a Delphi panel member. As a Delphi participant you will receive, via email, a pre-determined list of semi-structured questions. The questions may include scales, multiple choice questions and the possibility to comment on certain questions and statements related to insider threat. It is expected that there will be three rounds of the Delphi and that the time to complete each round will be approximately 20 minutes.

Please be assured that participation is entirely voluntary and you are able to withdraw from the process at any time. All data collected will be kept completely confidential and the identities of participants will only be known to the primary researcher. No results will be reported in any manner that would reveal identities of participants to other panel members or associate any participants with their answers.

Appendix B - Delphi Consent Form

University of Southern Queensland

Delphi Method Consent Form

Project Details	
Title of Project:	ORGANISATIONAL VULNERABILITY TO INSIDER THREAT – Development of an organisational vulnerability assessment identifying intentional insider threat risk
Human Research Ethics Approval Number:	**H15REA112**

Research Team Contact Details	
Principal Investigator Details	**Principal Supervisor Details**
Ms Justine Bedford Doctoral Candidate: Professional Studies Email: justine@jconsulting.net.au Telephone: 0425 793 618	Dr Luke Van Der Laan Director: Professional Studies Program Email: luke.vanderlaan@usq.edu.au Telephone: (07) 4631 5508

Statement of Consent

By replying to this email acknowledging your consent to participate, you are indicating that you:

- Have read and understood the information sheet regarding this project.
- Have had any questions answered to your satisfaction.
- Understand that if you have any additional questions you can contact the research team.
- Understand that you are free to withdraw at any time, without comment or penalty.
- Understand that while information gained during the study may be published, you will not be identified and your personal information and participation in the research will remain confidential.
- Understand that the information obtained during the research will be stored securely on a password protected computer. At the end of the study information will be transferred to password-protected encrypted electronic storage device and locked in a safe. All information will be destroyed five years after the end of the research project.
- Understand that you can contact the University of Southern Queensland Ethics Coordinator on (07) 4631 2690 or email ethics@usq.edu.au if you do have any concern or complaint about the ethical conduct of this project.
- Are over 18 years of age and have expertise in the field of Insider Threat.
- Agree to participate in the project.

Please reply via email to justinebedford@jconsulting.net.au acknowledging your consent to participate in this research as a Delphi expert panel member.

Appendix C - Delphi Participant Information Sheet

University of Southern Queensland

Delphi Method
Participant Information Sheet

Project Details	
Title of Project:	ORGANISATIONAL VULNERABILITY TO INSIDER THREAT – Development of an organisational vulnerability assessment identifying intentional insider threat risk
Human Research Ethics Approval Number:	**H15REA112**

Research Team Contact Details	
Principal Investigator Details	**Principal Supervisor Details**
Ms Justine Bedford Doctoral Candidate: Professional Studies Email: justine@jconsulting.net.au Telephone: 0425 793 618	Dr Luke Van Der Laan Director: Professional Studies Program Email: luke.vanderlaan@usq.edu.au Telephone: (07) 4631 5508

Project Information

Historically, the research on insider threat has been more individually focused providing a narrow perspective of examining the topic. The literature has been useful but has ignored or undervalued broader organisational influences.

It is the aim of the current research to develop an organisational assessment survey that helps organisations to identify potential weaknesses that may make it more susceptible to intentional insider threat behaviour. In order to do this a greater understanding of the organisational influences on intentional insider threat is required.

This project is being undertaken as part of Doctor of Professional Studies program at the USQ.

Participation

We would like to invite you to take part in this important research project and provide your expert opinion on organisational vulnerability to intentional insider threat.

1. Procedures

- Participation in this project will involve responding to email questions that will take approximately 20-30 minutes to complete for each round.
- It is expected that there will be three rounds of email questions.
- Data will be collected using re-identifiable data but stored anonymously.
- Data will be aggregated for use in a research report and the development of a survey designed to assess an organisation's vulnerability to insider threat.

2. Voluntary Participation

Participation is entirely voluntary. If you do not wish to take part you are not obliged to. If you decide to start in the project you are welcome to answer only the questions you would like to and you may stop at any time.

Your decision whether to take part or not to take part, or to take part and then withdraw, will not affect your relationship with the University of Southern Queensland or the researcher. Please notify the researcher if you decide to withdraw from this project (details above).

Should you have any queries regarding the progress or conduct of this research, you can contact the principal investigator or the supervisor of the research project as outlined above. You may also request a summary of results from the research team, which will be made available once the study is completed.

Expected Benefits

As a participant in this project your expert opinion will provide an important contribution to the field of insider threat specifically (and more broadly CWB). You will receive in summary format a collation of the responses from the whole Delphi panel – all leaders in this area and representing multiple industries. A final report and draft survey questionnaire will also be provided. This also represents a unique opportunity to gain new insights into this under-researched area.

Risks

There are no anticipated risks beyond normal day-to-day living associated with your participation in this project.

Privacy and Confidentiality

All comments and responses will be treated confidentially unless required by law.

Any data collected as a part of this project will be stored securely as per University of Southern Queensland's Research Data Management policy.

Consent to Participate

Please read the Consent Form attached and acknowledge your consent to participate in a return email by the 20 November 2015.

Questions or Further Information about the Project

Please refer to the Research Team Contact Details at the top of the form to have any questions answered or to request further information about this project.

Concerns or Complaints Regarding the Conduct of the Project

If you have any ethical concerns with how the research is being conducted or any queries about your rights as a participant please feel free to contact the University of Southern Queensland Ethics Coordinator on (07) 4631 2690 or email ethics@usq.edu.au. The Ethics Coordinator is not connected with the research project and can facilitate a resolution to your concern in an unbiased manner.

Thank you for taking the time to help with this research project. Please keep this sheet for your information.

Appendix D - Delphi Survey Round 1

ORGANISATIONAL VULNERABILITY AND INTENTIONAL INSIDER THREAT: A DELPHI STUDY

Introduction

Being able to reduce an organisations vulnerability to intentional insider threat is a critical issue for most public and private organisations. Despite this and signs that insider threat will increase, research to better understand and address the problem is rare. Figures suggest that as much as 75 percent of corporate value can be tied to intangible assets (Shaw & Fischer 2009), including intellectual property, and so protection of such materials and knowledge is becoming increasingly important. Behaviours such as espionage, sabotage, theft and terrorism (Shaw & Fischer 2009) can cause significant damage to organisations.

Approaches to the study of insider threat to date has been narrow in focus even though preliminary research results has suggested that organisational risk factors are critically relevant. Indeed, there is agreement that the risk of cyber security has become a permanent board agenda item and budget line expense of most informed boards.

This study will comprise a thematic review of literature that examines insider risk behaviour and the use of the Delphi Method to gather expert opinion (in the fields of security, risk management, organisational behaviour, cyber security, and intelligence) in order to determine organisational factors that are relevant to assessment of intentional insider threat risk. This information will then be used to develop an online organisational assessment survey, which will be piloted and validated.

Contact: Justine Bedford, justine@jconsulting.net.au, Mobile: 0425 793 618

'Compromise is expensive. It can include financial losses, damage to reputation, loss of intellectual property and disruption to business. Australia cannot afford this' –

Australian Cyber Security Centre.

UNIVERSITY OF SOUTHERN QUEENSLAND AUSTRALIA

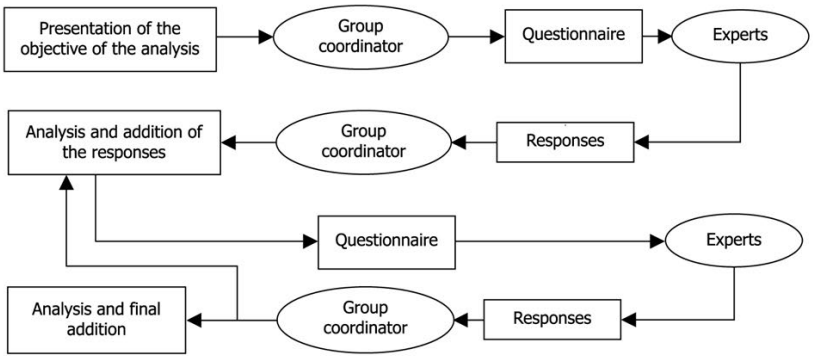
What is The Delphi Method?

The Delphi method seeks to synthesise contributions from a panel of experts aimed at addressing a clearly stated problem. Panel members respond to semi-structured questions, in this case via email. The primary researcher is responsible for the collation and distillation of responses, by processing the information and filtering out irrelevant content. This avoids the negative effects of face-to-face panel discussions and solves the usual problems of group dynamics. It also protects the identity of participants.

Regular feedback is provided. Participants comment on their own perspectives and the responses of others. At any moment they can revise their earlier statements. While in regular group meetings participants tend to stick to previously stated opinions and often conform too much to the group leader, the Delphi method prevents it.

Usually all participants remain anonymous. Their identity is not revealed, even after the completion of the final report. This prevents the authority, personality, or reputation of some participants from dominating others in the process. Arguably, it also frees participants (to some extent) from their personal biases, minimizes the "bandwagon effect" or "halo effect", allows free expression of opinions, encourages open critique, and facilitates admission of errors when revising earlier judgments.

The Delphi method has also been used as a tool to implement multi-stakeholder approaches for participative decision making and strategy development. As a result, widely acknowledged value in the form of collective intelligence is recognised, especially in an environment of rapid change.



Source: Adapted from Landeta (1999)

Question 1

What is intentional insider threat?

1A. The following words appear in the associated literature related to the definition of insider threat. Please rate to what extent you agree or disagree with these key words in defining *intentional* insider threat.

	Strongly Disagree	Disagree	Neither Agree or Disagree	Agree	Strongly Agree
Action	☐	☐	☐	☐	☐
Contractor/Consultant	☐	☐	☐	☐	☐
Critical information	☐	☐	☐	☐	☐
Employee	☐	☐	☐	☐	☐
Inaction	☐	☐	☐	☐	☐
Intent	☐	☐	☐	☐	☐
Knowledge	☐	☐	☐	☐	☐
Legitimate Access	☐	☐	☐	☐	☐
Loss	☐	☐	☐	☐	☐
Person of Trust	☐	☐	☐	☐	☐
Protected information	☐	☐	☐	☐	☐
Sensitive information	☐	☐	☐	☐	☐
Unauthorised	☐	☐	☐	☐	☐
Valued Assets	☐	☐	☐	☐	☐

1B. Please provide a definition, description or additional words explaining what *intentional* insider threat means to you.

QUESTION 2

What factors do you consider INCREASE the likelihood of intentional insider threat?

2A. Previous studies provide insight on factors which may increase the likelihood of insider threat. The following are current factors we are aware of through our research and believe to be most significant. Please rate to what extent you agree or disagree that vulnerabilities within each factor contributes to an *increased* risk of intentional insider threat.

INDIVIDUAL FACTORS ***Internal***	Strongly Disagree	Disagree	Neither Agree or Disagree	Agree	Strongly Agree
Personality vulnerability/disorder	☐	☐	☐	☐	☐
Mental health concerns	☐	☐	☐	☐	☐
Disgruntlement	☐	☐	☐	☐	☐
Motivational issues	☐	☐	☐	☐	☐
Ego/sense of entitlement	☐	☐	☐	☐	☐
Ethical flexibility	☐	☐	☐	☐	☐
History of security violations	☐	☐	☐	☐	☐
INDIVIDUAL FACTORS ***External***	Strongly Disagree	Disagree	Neither Agree or Disagree	Agree	Strongly Agree
Lack of social connectedness	☐	☐	☐	☐	☐
Criminal associations	☐	☐	☐	☐	☐
Financial pressures	☐	☐	☐	☐	☐
Targeted by competitors/foreign intelligence	☐	☐	☐	☐	☐
Foreign attachments	☐	☐	☐	☐	☐
Negative/stressful life events	☐	☐	☐	☐	☐
Personal computer behaviour; addiction, delinquency, etc	☐	☐	☐	☐	☐

ORGANISATIONAL FACTORS ***Internal***	Strongly Disagree	Disagree	Neither Agree or Disagree	Agree	Strongly Agree
Poor organisational culture	☐	☐	☐	☐	☐
Disparate values	☐	☐	☐	☐	☐
Lack of leadership	☐	☐	☐	☐	☐
Organisational change: restructuring, downsizing	☐	☐	☐	☐	☐
Poor security culture	☐	☐	☐	☐	☐
Reduced budget/economic position	☐	☐	☐	☐	☐
Use of contractors/transient workforce	☐	☐	☐	☐	☐
ORGANISATIONAL FACTORS ***External***	Strongly Disagree	Disagree	Neither Agree or Disagree	Agree	Strongly Agree
Poor reputation	☐	☐	☐	☐	☐
Increased market competition	☐	☐	☐	☐	☐
Outsourcing work	☐	☐	☐	☐	☐
Overseas/remote/satellite locations	☐	☐	☐	☐	☐
Ineffective/lack of collaboration with others	☐	☐	☐	☐	☐
Moles – placed by criminal associations or competitors	☐	☐	☐	☐	☐
Mobile workforce	☐	☐	☐	☐	☐
TECHNOLOGICAL FACTORS ***Internal***	Strongly Disagree	Disagree	Neither Agree or Disagree	Agree	Strongly Agree
Lack of electronic access controls	☐	☐	☐	☐	☐
No/limited auditing and monitoring	☐	☐	☐	☐	☐
Poor sophistication of IT systems	☐	☐	☐	☐	☐
Old IT policies and procedures	☐	☐	☐	☐	☐
High IT staff turnover	☐	☐	☐	☐	☐

Use of personal technology devices	☐	☐	☐	☐	☐
Limited authentication procedures	☐	☐	☐	☐	☐
TECHNOLOGICAL FACTORS ***External***	Strongly Disagree	Disagree	Neither Agree or Disagree	Agree	Strongly Agree
Increase in number of cyber adversaries	☐	☐	☐	☐	☐
Social networking	☐	☐	☐	☐	☐
Speed of developing technologies	☐	☐	☐	☐	☐
IT job market/skills shortage	☐	☐	☐	☐	☐
Planting: logic bombs, key logging devices	☐	☐	☐	☐	☐
Unsecured networks: cafes, airports	☐	☐	☐	☐	☐
Limited hardware controls	☐	☐	☐	☐	☐

2B. In this rapidly changing environment there might be emerging factors and we want to capture them. Some further factors in the research include: religion, moral development, intelligence, family influences, staff resourcing, size of organisation, type of intellectual property, computer behaviour, loyalty, framing, lack of consistent policies, use of generic software, economic position, workplace deviance, cyber deviance, etc. Please list below which of these extra factors (if any) are *critical* in increasing the risk of insider threat. Please list below any other *critical* factors or vulnerabilities that you consider *increase* the likelihood of intentional insider threat.

QUESTION 3

What factors do you consider DECREASE the likelihood of an intentional insider threat?

3A. Research also provides insight on factors which may help decrease the likelihood of insider threat. The following are current factors we are aware of through our research. Please rate to what extent you agree or disagree that capabilities within each factor may *decrease* the risk of intentional insider threat.

INDIVIDUAL FACTORS ***Internal***	Strongly Disagree	Disagree	Neither Agree or Disagree	Agree	Strongly Agree
Self-awareness	☐	☐	☐	☐	☐
Loyalty	☐	☐	☐	☐	☐
Resilience	☐	☐	☐	☐	☐
Conscientiousness	☐	☐	☐	☐	☐
Sound judgment	☐	☐	☐	☐	☐
Ability to accept and integrate feedback	☐	☐	☐	☐	☐
Aligned values	☐	☐	☐	☐	☐
INDIVIDUAL FACTORS ***External***	Strongly Disagree	Disagree	Neither Agree or Disagree	Agree	Strongly Agree
Positive support networks	☐	☐	☐	☐	☐
Extracurricular involvement	☐	☐	☐	☐	☐
Help-seeking	☐	☐	☐	☐	☐
Ongoing education	☐	☐	☐	☐	☐
Sound work history	☐	☐	☐	☐	☐
Cultural understanding	☐	☐	☐	☐	☐
Sound and reliable behaviour outside of work	☐	☐	☐	☐	☐

ORGANISATIONAL FACTORS ***Internal***	Strongly Disagree	Disagree	Neither Agree or Disagree	Agree	Strongly Agree
Security awareness training	☐	☐	☐	☐	☐
Behavioural monitoring	☐	☐	☐	☐	☐
Strict use of probation	☐	☐	☐	☐	☐
Positive organisational culture	☐	☐	☐	☐	☐
Strong leadership	☐	☐	☐	☐	☐
Employee assistance programs	☐	☐	☐	☐	☐
Relevant security policies and procedures	☐	☐	☐	☐	☐
ORGANISATIONAL FACTORS ***External***	Strongly Disagree	Disagree	Neither Agree or Disagree	Agree	Strongly Agree
Benchmarking	☐	☐	☐	☐	☐
Positive reputation	☐	☐	☐	☐	☐
Positive economic position	☐	☐	☐	☐	☐
Vetting and background checks	☐	☐	☐	☐	☐
Control of physical security environment	☐	☐	☐	☐	☐
Sharing knowledge of insider risks outside the organisation	☐	☐	☐	☐	☐
Strict exit controls on staff leaving the organisation	☐	☐	☐	☐	☐
TECHNOLOGICAL FACTORS ***Internal***	Strongly Disagree	Disagree	Neither Agree or Disagree	Agree	Strongly Agree
Impeded access/access controls	☐	☐	☐	☐	☐
Random auditing	☐	☐	☐	☐	☐
Computer monitoring	☐	☐	☐	☐	☐
Sophistication/knowledge of IT staff	☐	☐	☐	☐	☐
Positive IT subculture	☐	☐	☐	☐	☐

Relevant IT policies and procedures	☐	☐	☐	☐	☐
Minimum privilege access	☐	☐	☐	☐	☐
TECHNOLOGICAL FACTORS ***External***	Strongly Disagree	Disagree	Neither Agree or Disagree	Agree	Strongly Agree
Cyber vetting	☐	☐	☐	☐	☐
Use of third party products/vendors	☐	☐	☐	☐	☐
Ongoing IT training/education	☐	☐	☐	☐	☐
Perimeter controls	☐	☐	☐	☐	☐
External back up system	☐	☐	☐	☐	☐
Use of cyber security consultants	☐	☐	☐	☐	☐

3B. In this rapidly changing environment there might be emerging factors and we want to capture them. Some further factors in the research include: resilience, attachment, self-control, polygraph, drug and alcohol testing, ongoing personnel checks, regional culture, patriotism, blocking spam/phishing emails, firewalls, etc. Please list below which of these extra factors (if any) are *critical* in *decreasing* the risk of insider threat. Please list below any other *critical* factors or capabilities that you consider *decrease* the likelihood of intentional insider threat.

QUESTION 4

In your experience of specific cases of intentional insider threat, what ORGANISATIONAL factors were exploited?

4A. The literature provides insight on specific *organisational* conditions which may influence the likelihood of intentional insider threat. In your experience, to what extent do you believe that each of these organisational conditions contributes to an increased or decreased risk of intentional insider threat? Additional comments are optional.

	Strongly Decrease	Decrease	Neither Increase or Decrease	Increase	Strongly Increase	Additional comments (optional)
Access	☐	☐	☐	☐	☐	
Background updates/reevaluations	☐	☐	☐	☐	☐	
Bag checks	☐	☐	☐	☐	☐	
Collaboration with government or other businesses	☐	☐	☐	☐	☐	
Cyber vetting	☐	☐	☐	☐	☐	
Drug and alcohol testing	☐	☐	☐	☐	☐	
Electronic access controls	☐	☐	☐	☐	☐	
Employee assistance programs/Staff counselling	☐	☐	☐	☐	☐	
Employee engagement	☐	☐	☐	☐	☐	
Employee monitoring	☐	☐	☐	☐	☐	
Employee screening & selection	☐	☐	☐	☐	☐	

	Strongly Decrease	Decrease	Neither Increase or Decrease	Increase	Strongly Increase	Additional comments (optional)
Impeded access (to systems, sensitive areas)	☐	☐	☐	☐	☐	
Increase in staff counterproductive behaviour	☐	☐	☐	☐	☐	
IT monitoring of employees	☐	☐	☐	☐	☐	
IT/cyber security functions	☐	☐	☐	☐	☐	
Leadership	☐	☐	☐	☐	☐	
Management	☐	☐	☐	☐	☐	
Organisational behaviour monitoring (legal use of employee data)	☐	☐	☐	☐	☐	
Organisational culture	☐	☐	☐	☐	☐	
Organisational economic pressures	☐	☐	☐	☐	☐	
Organisational values	☐	☐	☐	☐	☐	
Outsourcing	☐	☐	☐	☐	☐	
Overseas locations	☐	☐	☐	☐	☐	
Performance evaluations	☐	☐	☐	☐	☐	
Physical access controls	☐	☐	☐	☐	☐	
Policy and procedures	☐	☐	☐	☐	☐	
Polygraph	☐	☐	☐	☐	☐	
Psychological assessment	☐	☐	☐	☐	☐	

	Strongly Decrease	Decrease	Neither Increase or Decrease	Increase	Strongly Increase	Additional comments (optional)
Random auditing	☐	☐	☐	☐	☐	
Recruitment	☐	☐	☐	☐	☐	
Referee checks	☐	☐	☐	☐	☐	
Regulatory oversight	☐	☐	☐	☐	☐	
Rotation of duties	☐	☐	☐	☐	☐	
Security awareness/education	☐	☐	☐	☐	☐	
Security culture	☐	☐	☐	☐	☐	
Security governance	☐	☐	☐	☐	☐	
Security reporting	☐	☐	☐	☐	☐	
Separation of duties	☐	☐	☐	☐	☐	
Size of the organisation	☐	☐	☐	☐	☐	
Social engineering	☐	☐	☐	☐	☐	
Specific insider threat training	☐	☐	☐	☐	☐	
Staff morale	☐	☐	☐	☐	☐	
Team members reporting	☐	☐	☐	☐	☐	
Trust	☐	☐	☐	☐	☐	
Undue secrecy	☐	☐	☐	☐	☐	
Use of probation	☐	☐	☐	☐	☐	
Vetting	☐	☐	☐	☐	☐	

	Strongly Decrease	Decrease	Neither Increase or Decrease	Increase	Strongly Increase	Additional comments (optional)
Video/CCTV	☐	☐	☐	☐	☐	

4B. Given your experience, please list any further **organisational vulnerabilities** that you consider *increase* the likelihood of intentional insider threat.

4C. Based on your experience, please list any further **organisational capabilities** that you consider could *decrease* the likelihood of intentional insider threat.

QUESTION 5

The researcher is very aware that this research is being conducted close to the holiday season. For planning purposes, please indicate if you will be able to respond to the second round of the Delphi before the 21 December 2015?

YES	NO	Don't Know
☐	☐	☐

Appendix E - Delphi Survey Round 2

ORGANISATIONAL VULNERABILITY AND INTENTIONAL INSIDER THREAT: A DELPHI STUDY

Introduction

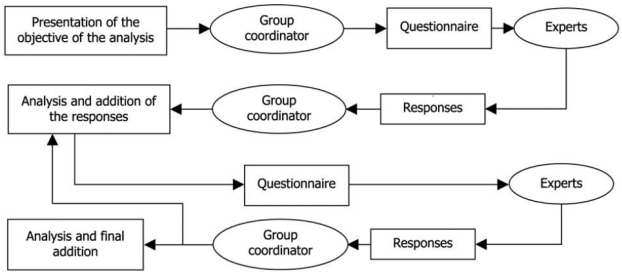
Being able to reduce an organisations vulnerability to intentional insider threat is a critical issue for most public and private organisations. Despite this and signs that insider threat will increase, research to better understand and address the problem is rare.

This study will comprise a thematic review of literature that examines insider risk behaviour and the use of the Delphi Method to gather expert opinion (in the fields of security, risk management, organisational behaviour, cyber security, and intelligence) in order to determine organisational factors that are relevant to assessment of intentional insider threat risk.

What is The Delphi Method?

The Delphi method seeks to synthesise contributions from a panel of experts aimed at addressing a clearly stated problem. Panel members respond to semi-structured questions, in this case via email. The primary researcher is responsible for the collation and distillation of responses, by processing the information and filtering out irrelevant content. This avoids the negative effects of face-to-face panel discussions and solves the usual problems of group dynamics. It also protects the identity of participants.

Regular feedback is provided. Participants comment on their own perspectives and the responses of others. At any moment they can revise their earlier statements.



Source: Adapted from Landeta (1999)

'Compromise is expensive. It can include financial losses, damage to reputation, loss of intellectual property and disruption to business. Australia cannot afford this' –

Australian Cyber Security Centre.

Contact: Justine Bedford, justine@jconsulting.net.au, Mobile: 0425 793 618

Analysis of Round 1

For this project descriptive statistics and P-P Plots were used to assess the responses from panel experts. Consensus on a question was deemed to be achieved if at least 70 percent of panel members agreed on the direction of the response (see Annex A). Where any item achieved at least 70% agreement it was considered to have reached consensus and eliminated from this Delphi round (Round 2).

Descriptive data analysis and P-P Plots were used to determine the normality and variability of the data. Questions were also eliminated when panel responses were assessed as being along a normal distribution, with a low variability and minimal outliers.

Based on these statistical techniques the panel demonstrated a high level of consensus across the questions of the first Delphi round. In Round 2 we look at the questions that have not reached consensus and also further explore the results of Round 1. Please answer the following questions.

Question 1

What is intentional insider threat?

Generally there was a strong agreement on the key words associated with defining insider threat. For Round 2 we would like to further explore the following:

1. The definitions and words that reached consensus tended to focus on an individual's risk to an organisation. It did not explore the perspective of the *Organisation* as part of the definition or how characteristics of the *Organisation* may contribute to intentional insider threat. *Inaction* was one word where a third of panel members 'neither agreed nor disagreed'. In an organisation *inaction* may suggest that the organisation is reactive (rather than proactive) to intentional insider threat. Do you agree? Explain.

2. The terms *contractor and consultant* were combined in the first Round Delphi. However, if we separate these terms and define them differently, would you rate the potential risk of intentional insider threat differently?

    a. Contractor: a fixed term employee
    b. Consultant: an external expert

    Who do you believe poses a bigger intentional insider threat: an employee, consultant, or contractor? To what degree (%)? Why?

Question 2

2a. What factors do you consider INCREASE the likelihood of intentional insider threat?

1. One hundred percent of the panel agreed that sense of entitlement/ego plays a critical role in increasing risk of insider threat. In the later stages of the first round questions, however, the use of psychological assessment was not considered an organisational technique to decrease the risk of intentional insider threat.
    a. Why do you think this is so?

    b. What other methods can you think of and / or your organisation already uses, to assess for sense of entitlement/ego in relation to possible future intentional insider threat?

2. A shortage of IT talent as well as a high turnover of IT staff is a growing concern in the practice environment, especially when it comes to cyber security. The responses provided by the panel suggested a lack of consensus that this could extend to a potential insider threat concern. For example, less than 70% of the panel indicated that high IT staff turnover, increase in market competition, IT skills shortages, or sophistication of IT staff were factors that could increase intentional insider threat. Please explain your thoughts on this further.

Please continue on next page.

INTENTIONAL INSIDER THREAT: Delphi Study Round 2

2b. Below are additional factors from the first Delphi round that the Panel indicated may also be critical in increasing intentional insider threat. Please rate to what extent you agree or disagree that vulnerabilities within each factor contributes to an *increased* risk of intentional insider threat.

FACTORS	Strongly Disagree	Disagree	Neither Agree or Disagree	Agree	Strongly Agree
Addictions (particularly gambling)	☐	☐	☐	☐	☐
Affiliations (religious, criminal)	☐	☐	☐	☐	☐
Concerns with moral development	☐	☐	☐	☐	☐
Corporate Governance	☐	☐	☐	☐	☐
Cyber deviance	☐	☐	☐	☐	☐
Financial concerns that could lead to embarrassment (i.e. gambling, poor investments)	☐	☐	☐	☐	☐
Ideology (religious, social, etc)	☐	☐	☐	☐	☐
Lack of consistency of policies and expectations across all levels of the organisation	☐	☐	☐	☐	☐
Lack of individual coping mechanisms/resources	☐	☐	☐	☐	☐
Lack of monitoring and enforcing policies	☐	☐	☐	☐	☐

INTENTIONAL INSIDER THREAT: Delphi Study Round 2

FACTORS	Strongly Disagree	Disagree	Neither Agree or Disagree	Agree	Strongly Agree
Lack of oversight of senior managers	☐	☐	☐	☐	☐
Lack of perceived support to staff	☐	☐	☐	☐	☐
Lack of personal connection to organisational values and mission	☐	☐	☐	☐	☐
Perception that management is treated differently	☐	☐	☐	☐	☐
Perception that managers do not value staff	☐	☐	☐	☐	☐
Type of IP of the organisation	☐	☐	☐	☐	☐
Unachievable goals set by management	☐	☐	☐	☐	☐
Workplace deviance	☐	☐	☐	☐	☐

QUESTION 3

3a. What factors do you consider DECREASE the likelihood of an intentional insider threat?

1. From Questions 2 and 3 in the first Delphi round, there was a high consensus that organisations generally have a good level of control over factors that can increase (or decrease) intentional insider threat. Internal control measures across individual, organisational, and technical areas are generally thought of as sufficient. Why then, do you believe intentional insider threat is such a dominant issue in practice, research, and risk enterprise and risk professional services?

2. The panel highly endorsed that a strong positive organisational culture and security culture were important methods to decrease the likelihood of intentional insider threat. What do you think is the relationship between traditional HR practices and an organisation's ability to develop these positive cultures?

3b. Below are additional factors that the Panel highlighted may be critical in decreasing intentional insider threat.

Please rate to what extent you agree or disagree that capabilities within each factor contributes to a *decreased* risk of intentional insider threat.

FACTORS	Strongly Disagree	Disagree	Neither Agree or Disagree	Agree	Strongly Agree
"pulse" surveys	☐	☐	☐	☐	☐
Career mobility	☐	☐	☐	☐	☐
Compliance and risk management education	☐	☐	☐	☐	☐
Education on social media	☐	☐	☐	☐	☐
Improving research on how offenders "evaluate an opportunity"	☐	☐	☐	☐	☐
Leadership that is connected and supportive of staff	☐	☐	☐	☐	☐
Obvious and declared security controls	☐	☐	☐	☐	☐
Organisational resilience	☐	☐	☐	☐	☐
Positive leadership and change management	☐	☐	☐	☐	☐
Staff consultation	☐	☐	☐	☐	☐
Whistleblower protection policies	☐	☐	☐	☐	☐

Question 4

In your experience of specific cases of intentional insider threat, what ORGANISATIONAL factors were exploited?

1. An increase in staff counterproductive workplace behaviour was considered to strongly increase the risk of intentional insider threat.
    a. Please explain why you believe this to be the case.

    b. What methods or evidence may show a trending increase in staff counterproductive workplace behaviour?

2. Variability in responses suggests that about 15% of the panel believe that the following organisational conditions - electronic access controls, employee monitoring, employment screening and selection, and random auditing - may increase the risk of intentional insider threat. Why?

4B/4C. Listed below are additional organisational vulnerabilities and capabilities that the Panel considered could increase or decrease the likelihood of intentional insider threat.

In your experience, to what extent do you believe that each of these organisational conditions contributes to an increased or decreased risk of intentional insider threat? Additional comments are optional.

FACTORS	Strongly Decrease	Decrease	Neither Increase or Decrease	Increase	Strongly Increase	Additional comments (optional)
Appropriate reporting of red flags	☐	☐	☐	☐	☐	
Awareness campaigns	☐	☐	☐	☐	☐	
Better communication across organisations	☐	☐	☐	☐	☐	
Clear organisational goals and objectives	☐	☐	☐	☐	☐	
Complacency	☐	☐	☐	☐	☐	
Enforcing security mandated policies (e.g. mandatory holidays/leave)	☐	☐	☐	☐	☐	
High employee engagement	☐	☐	☐	☐	☐	
Identifying red flags	☐	☐	☐	☐	☐	
Lack of connection to employee issues	☐	☐	☐	☐	☐	
Lack of management of issues at the emerging stages	☐	☐	☐	☐	☐	
Poor application of security	☐	☐	☐	☐	☐	

FACTORS	Strongly Decrease	Decrease	Neither Increase or Decrease	Increase	Strongly Increase	Additional comments (optional)
Poor organisational communication	☐	☐	☐	☐	☐	
Poor security practices of leadership	☐	☐	☐	☐	☐	
Program of security training/awareness training	☐	☐	☐	☐	☐	
Senior management understanding of Intentional insider threat	☐	☐	☐	☐	☐	
Staff involvement in development of security policies and processes	☐	☐	☐	☐	☐	
Witnessing other staff get away with poor security behaviour with no consequence	☐	☐	☐	☐	☐	

QUESTION 5

5a. Thinking to the future, where do you believe the focus should be on decreasing organisational vulnerability to intentional insider threat? What is *probable* and what is *possible*?

5b. Another dimension has emerged from the analysis of the Round 1 Delphi related to the proactive development of staff's ability to think about the future and anticipate threat. This is in contrast to a view that automation, software and hardware is sufficient to mitigate risk. Do you agree?

ANNEX A: For Information

Annex A provides the responses of panel members in percentage format.

Question 1

What is intentional insider threat?

1A. The following words appear in the associated literature related to the definition of insider threat. Please rate to what extent you agree or disagree with these key words in defining *intentional* insider threat.

	Strongly Disagree	Disagree	Neither Agree or Disagree	Agree	Strongly Agree
Action	0.0	6.7	33.3	46.7	13.3
Contractor/Consultant	6.7	26.7	20.0	46.7	0.0
Critical information	0.0	6.7	13.3	46.7	33.3
Employee	0.0	0.0	20.0	40.0	40.0
Inaction	13.3	33.3	20.0	26.7	6.7
Intent	0.0	0.0	6.7	26.7	66.7
Knowledge	0.0	0.0	21.4	64.3	14.3
Legitimate Access	0.0	6.7	0.0	80.0	13.3
Loss	0.0	6.7	13.3	66.7	13.3
Person of Trust	0.0	0.0	13.3	53.3	33.3
Protected information	0.0	0.0	13.3	66.7	20.0
Sensitive information	0.0	0.0	6.7	66.7	26.7
Unauthorised	0.0	6.7	13.3	60.0	20.0
Valued Assets	0.0	6.7	13.3	66.7	13.3

QUESTION 2

What factors do you consider INCREASE the likelihood of intentional insider threat?

2A. Previous studies provide insight on factors which may increase the likelihood of insider threat. The following are current factors we are aware of through our research and believe to be most significant. Please rate to what

extent you agree or disagree that vulnerabilities within each factor contributes to an *increased* risk of intentional insider threat.

INDIVIDUAL FACTORS ***Internal***	Strongly Disagree	Disagree	Neither Agree or Disagree	Agree	Strongly Agree
Personality vulnerability/disorder	0.0	6.7	20.0	26.7	46.7
Mental health concerns	0.0	6.7	26.7	46.7	20.0
Disgruntlement	0.0	0.0	6.7	53.3	40.0
Motivational issues	0.0	6.7	13.3	60.0	20.0
Ego/sense of entitlement	0.0	0.0	0.0	60.0	40.0
Ethical flexibility	0.0	0.0	6.7	66.7	26.7
History of security violations	0.0	6.7	0.0	66.7	26.7
INDIVIDUAL FACTORS ***External***	Strongly Disagree	Disagree	Neither Agree or Disagree	Agree	Strongly Agree
Lack of social connectedness	0.0	13.3	53.3	26.7	6.7
Criminal associations	0.0	13.3	13.3	40.0	33.3
Financial pressures	0.0	6.7	13.3	66.7	13.3
Targeted by competitors/foreign intelligence	0.0	6.7	20.0	60.0	13.3
Foreign attachments	6.7	13.3	53.3	20.0	6.7
Negative/stressful life events	0.0	6.7	20.0	53.3	20.0
Personal computer behaviour; addiction, delinquency, etc	0.0	20.0	33.3	40.0	6.7
ORGANISATIONAL FACTORS ***Internal***	Strongly Disagree	Disagree	Neither Agree or Disagree	Agree	Strongly Agree
Poor organisational culture	0.0	6.7	0.0	60.0	33.3
Disparate values	0.0	20.0	26.7	33.3	20.0
Lack of leadership	0.0	0.0	26.7	60.0	13.3

Organisational change: restructuring, downsizing	0.0	6.7	20.0	73.3	0.0
Poor security culture	0.0	0.0	6.7	73.3	20.0
Reduced budget/economic position	0.0	13.3	60.0	26.7	0.0
Use of contractors/transient workforce	0.0	26.7	40.0	33.3	0.0
ORGANISATIONAL FACTORS ***External***	Strongly Disagree	Disagree	Neither Agree or Disagree	Agree	Strongly Agree
Poor reputation	0.0	40.0	53.3	6.7	0.0
Increased market competition	0.0	13.3	60.0	26.7	0.0
Outsourcing work	0.0	20.0	33.3	46.7	0.0
Overseas/remote/satellite locations	0.0	0.0	40.0	46.7	13.3
Ineffective/lack of collaboration with others	0.0	6.7	26.7	60.0	6.7
Moles – placed by criminal associations or competitors	6.7	13.3	6.7	46.7	26.7
Mobile workforce	0.0	33.3	46.7	20.0	0.0
TECHNOLOGICAL FACTORS ***Internal***	Strongly Disagree	Disagree	Neither Agree or Disagree	Agree	Strongly Agree
Lack of electronic access controls	0.0	0.0	0.0	73.3	26.7
No/limited auditing and monitoring	0.0	0.0	0.0	60.0	40.0
Poor sophistication of IT systems	0.0	6.7	0.0	73.3	20.0
Old IT policies and procedures	0.0	0.0	6.7	86.7	6.7
High IT staff turnover	0.0	13.3	40.0	46.7	0.0
Use of personal technology devices	0.0	13.3	46.7	33.3	6.7
Limited authentication procedures	0.0	0.0	13.3	73.3	13.3
TECHNOLOGICAL FACTORS ***External***	Strongly Disagree	Disagree	Neither Agree or Disagree	Agree	Strongly Agree
Increase in number of cyber adversaries	0.0	6.7	26.7	53.3	13.3

Social networking	0.0	13.3	53.3	33.3	0.0
Speed of developing technologies	0.0	26.7	26.7	46.7	0.0
IT job market/skills shortage	0.0	53.3	26.7	13.3	6.7
Planting: logic bombs, key logging devices	0.0	13.3	33.3	46.7	6.7
Unsecured networks: cafes, airports	0.0	13.3	33.3	53.3	0.0
Limited hardware controls	0.0	13.3	0.0	80.0	6.7

QUESTION 3

What factors do you consider DECREASE the likelihood of an intentional insider threat?

3A. Research also provides insight on factors which may help decrease the likelihood of insider threat. The following are current factors we are aware of through our research. Please rate to what extent you agree or disagree that capabilities within each factor may *decrease* the risk of intentional insider threat.

INDIVIDUAL FACTORS ***Internal***	Strongly Disagree	Disagree	Neither Agree or Disagree	Agree	Strongly Agree
Self-awareness	0.0	13.3	13.3	53.3	20.0
Loyalty	0.0	6.7	13.3	46.7	33.3
Resilience	0.0	6.7	6.7	60.0	26.7
Conscientiousness	0.0	13.3	13.3	46.7	26.7
Sound judgment	0.0	6.7	13.3	60.0	20.0
Ability to accept and integrate feedback	0.0	6.7	26.7	46.7	20.0
Aligned values	0.0	0.0	20.0	46.7	33.3
INDIVIDUAL FACTORS ***External***	Strongly Disagree	Disagree	Neither Agree or Disagree	Agree	Strongly Agree
Positive support networks	0.0	6.7	20.0	46.7	26.7
Extracurricular involvement	0.0	20.0	60.0	20.0	0.0
Help-seeking	0.0	13.3	20.0	46.7	20.0

Ongoing education	0.0	26.7	60.0	13.3	0.0
Sound work history	0.0	0.0	46.7	40.0	13.3
Cultural understanding	6.7	0.0	40.0	53.3	0.0
Sound and reliable behaviour outside of work	0.0	6.7	0.0	66.7	26.7
ORGANISATIONAL FACTORS ***Internal***	Strongly Disagree	Disagree	Neither Agree or Disagree	Agree	Strongly Agree
Security awareness training	0.0	0.0	6.7	60.0	33.3
Behavioural monitoring	0.0	6.7	6.7	60.0	26.7
Strict use of probation	0.0	13.3	26.7	46.7	13.3
Positive organisational culture	0.0	6.7	6.7	33.3	53.3
Strong leadership	0.0	0.0	6.7	66.7	26.7
Employee assistance programs	6.7	0.0	46.7	26.7	20.0
Relevant security policies and procedures	0.0	0.0	6.7	60.0	33.3
ORGANISATIONAL FACTORS ***External***	Strongly Disagree	Disagree	Neither Agree or Disagree	Agree	Strongly Agree
Benchmarking	0.0	13.3	40.0	46.7	0.0
Positive reputation	0.0	13.3	33.3	53.3	0.0
Positive economic position	0.0	13.3	66.7	20.0	0.0
Vetting and background checks	0.0	6.7	6.7	66.7	20.0
Control of physical security environment	0.0	6.7	13.3	66.7	13.3
Sharing knowledge of insider risks outside the organisation	0.0	6.7	40.0	40.0	13.3
Strict exit controls on staff leaving the organisation	0.0	0.0	20.0	66.7	13.3
TECHNOLOGICAL FACTORS ***Internal***	Strongly Disagree	Disagree	Neither Agree or Disagree	Agree	Strongly Agree

Impeded access/access controls	0.0	0.0	0.0	73.3	26.7
Random auditing	0.0	0.0	6.7	73.3	20.0
Computer monitoring	0.0	0.0	6.7	60.0	33.3
Sophistication/knowledge of IT staff	0.0	13.3	20.0	60.0	6.7
Positive IT subculture	0.0	6.7	40.0	46.7	6.7
Relevant IT policies and procedures	0.0	0.0	6.7	86.7	6.7
Minimum privilege access	0.0	0.0	0.0	66.7	33.3
TECHNOLOGICAL FACTORS ***External***	Strongly Disagree	Disagree	Neither Agree or Disagree	Agree	Strongly Agree
Cyber vetting	0.0	0.0	40.0	53.3	6.7
Use of third party products/vendors	0.0	13.3	46.7	40.0	0.0
Ongoing IT training/education	0.0	6.7	26.7	66.7	0.0
Perimeter controls	0.0	20.0	13.3	53.3	13.3
External back up system	6.7	6.7	26.7	60.0	0.0
Use of cyber security consultants	6.7	13.3	33.3	46.7	0.0

QUESTION 4

In your experience of specific cases of intentional insider threat, what ORGANISATIONAL factors were exploited?

4A. The literature provides insight on specific *organisational* conditions which may influence the likelihood of intentional insider threat. In your experience, to what extent do you believe that each of these organisational conditions contributes to an increased or decreased risk of intentional insider threat? Additional comments are optional.

	Strongly Decrease	Decrease	Neither Increase or Decrease	Increase	Strongly Increase
Access	7.1	7.1	0.0	50.0	35.7
Background updates/reevaluations	0.0	35.7	42.9	14.3	7.1

	Strongly Decrease	Decrease	Neither Increase or Decrease	Increase	Strongly Increase
Bag checks	7.1	50.0	35.7	7.1	0.0
Collaboration with government or other businesses	15.4	23.1	46.2	15.4	0.0
Cyber vetting	0.0	38.5	46.2	15.4	0.0
Drug and alcohol testing	7.1	21.4	64.3	7.1	0.0
Electronic access controls	14.3	71.4	0.0	14.3	0.0
Employee assistance programs/Staff counselling	14.3	42.9	42.9	0.0	0.0
Employee engagement	35.7	50.0	7.1	0.0	7.1
Employee monitoring	14.3	64.3	0.0	14.3	7.1
Employee screening & selection	21.4	57.1	7.1	7.1	7.1
Impeded access (to systems, sensitive areas)	35.7	50.0	0.0	14.3	0.0
Increase in staff counterproductive behaviour	0.0	0.0	14.3	35.7	50.0
IT monitoring of employees	14.3	64.3	7.1	14.3	0.0
IT/cyber security functions	21.4	57.1	14.3	7.1	0.0
Leadership	14.3	71.4	7.1	7.1	0.0
Management	21.4	64.3	7.1	0.0	7.1
Organisational behaviour monitoring (legal use of employee data)	21.4	50.0	21.4	7.1	0.0
Organisational culture	21.4	57.1	7.1	7.1	7.1
Organisational economic pressures	7.1	0.0	57.1	35.7	0.0
Organisational values	7.1	50.0	21.4	21.4	0.0
Outsourcing	7.1	7.1	35.7	50.0	0.0
Overseas locations	0.0	7.1	35.7	57.1	0.0
Performance evaluations	0.0	64.3	21.4	7.1	7.1
Physical access controls	14.3	71.4	7.1	7.1	0.0
Policy and procedures	14.3	57.1	14.3	14.3	0.0

	Strongly Decrease	Decrease	Neither Increase or Decrease	Increase	Strongly Increase
Polygraph	7.1	14.3	78.6	0.0	0.0
Psychological assessment	7.1	42.9	35.7	14.3	0.0
Random auditing	7.1	64.3	14.3	7.1	7.1
Recruitment	7.1	50.0	28.6	7.1	7.1
Referee checks	7.1	50.0	28.6	7.1	7.1
Regulatory oversight	0.0	50.0	28.6	14.3	7.1
Rotation of duties	7.1	50.0	35.7	0.0	7.1
Security awareness/education	14.3	57.1	14.3	7.1	7.1
Security culture	21.4	64.3	0.0	7.1	7.1
Security governance	15.4	76.9	0.0	7.7	0.0
Security reporting	7.7	69.2	15.4	7.7	0.0
Separation of duties	14.3	57.1	14.3	7.1	7.1
Size of the organisation	0.0	7.1	85.7	7.1	0.0
Social engineering	0.0	0.0	69.2	30.8	0.0
Specific insider threat training	7.1	57.1	21.4	7.1	7.1
Staff morale	0.0	57.1	7.1	21.4	14.3
Team members reporting	0.0	57.1	21.4	7.1	14.3
Trust	0.0	42.9	28.6	21.4	7.1
Undue secrecy	0.0	0.0	28.6	57.1	14.3
Use of probation	14.3	35.7	42.9	7.1	0.0
Vetting	14.3	42.9	28.6	14.3	0.0
Video/CCTV	7.1	50.0	35.7	7.1	0.0

Appendix F - Delphi Survey Round 3

ORGANISATIONAL VULNERABILITY AND INTENTIONAL INSIDER THREAT: A DELPHI STUDY

Introduction

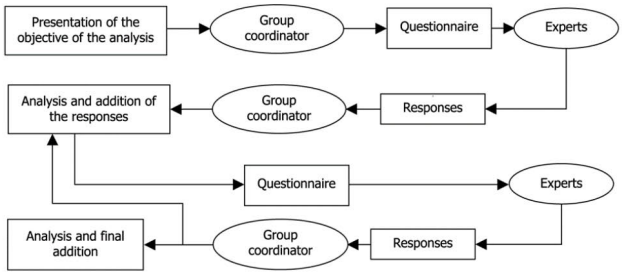
Being able to reduce an organisations vulnerability to intentional insider threat is a critical issue for most public and private organisations. Despite this and signs that insider threat will increase, research to better understand and address the problem is rare.

This study will comprise a thematic review of literature that examines insider risk behaviour and the use of the Delphi Method to gather expert opinion (in the fields of security, risk management, organisational behaviour, cyber security, and intelligence) in order to determine organisational factors that are relevant to assessment of intentional insider threat risk.

What is The Delphi Method?

The Delphi method seeks to synthesise contributions from a panel of experts aimed at addressing a clearly stated problem. Panel members respond to semi-structured questions, in this case via email. The primary researcher is responsible for the collation and distillation of responses, by processing the information and filtering out irrelevant content. This avoids the negative effects of face-to-face panel discussions and solves the usual problems of group dynamics. It also protects the identity of participants.

Regular feedback is provided. Participants comment on their own perspectives and the responses of others. At any moment they can revise their earlier statements.



Source: Adapted from Landeta (1999)

'Compromise is expensive. It can include financial losses, damage to reputation, loss of intellectual property and disruption to business. Australia cannot afford this' –

Australian Cyber Security Centre.

Contact: Justine Bedford, justine@jconsulting.net.au, Mobile: 0425 793 618

Analysis of Round 2

Eighty-six percent of panel experts responded to the Delphi Round 2.

The data was screened and tested for normality (P-P plots). Descriptive statistics data variance were used to assess the responses from panel experts and determine the level of consensus. Consensus on a question was deemed to be achieved if a) at least 70 percent of panel members agreed on the direction of the response and b) there was no abnormal distribution of responses i.e. normal distribution, with a low variability and minimal outliers. Where any item achieved at least 70% agreement and there were no 'polar-opposite' responses of concern it was considered to have reached consensus.

Content analysis of qualitative data was used to determine emerging themes from responses to open ended questions. Based on this analytical technique the panel demonstrated a high level of consensus across the questions during the second round Delphi.

Factors and themes of vulnerabilities and capabilities were then reviewed to determine those that were of *primary* importance (where more than 90% of panel experts agreed or raised an issue/idea and at least one third strongly agreed with that factor) and *secondary* importance (all other factors that reached consensus).

Please consider and respond to the following questions.

Question 1

What is intentional insider threat?

Generally there was a strong consensus on the words that should be included in a definition of Intentional Insider Threat. Based on the outcomes of the first two Delphi rounds the following definition is presented:

Insider threat is when: a person of trust (employee, contractor, consultant, vendor) who has/had legitimate access to an organisation attempts to cause harm through counterproductive behaviour intended to result in the loss, disclosure, or damage to that organisation's information, resources, or assets.

Do you agree with the above definition?

YES	NO
☐	☐

Would you like to add further comments that may enhance the definition?

PLEASE CONTINUE TO NEXT PAGE.

QUESTION 2

What factors do you consider INCREASE the likelihood of intentional insider threat?

Below are a list of primary and secondary factors – based on Delphi results – that increase the likelihood of insider threat.

PRIMARY WEAKNESSES/VULNERABILITIES	SECONDARY WEAKNESSES/VULNERABILITIES
PEOPLE	PEOPLE
1. Ego/sense of entitlement 2. Disgruntlement 3. Ethical flexibility 4. Increase in staff CWB/workplace deviance	1. Lack of strong and supportive leadership/management 2. Addictions – particularly gambling 3. Questionable moral development 4. Associations/affiliations (criminal, moles, etc) 5. Financial pressures 6. Negative stressful life events 7. Other individual vulnerabilities; Lack of self-awareness, Lack of coping resources, Lack of loyalty to the organisation 8. Values not aligned with organisational values 9. Lack of oversight of senior managers 10. Lack of connection to staff issues 11. Lack of staff involvement in organisational decisions 12. Perception that staff are not valued
PROCESS	PROCESS
5. Poor security practices of leadership 6. Poor application of security 7. No consequences for poor security behaviour	13. No alignment of HR practices with security policy/practices 14. Lack of alignment between HR practices and leadership practices 15. No policies/procedures on how to manage potential security issues at emerging stages 16. Out of date IT policies 17. No/limited security governance 18. Not managing inappropriate workplace behaviour including security behaviour
TECHNOLOGY	TECHNOLOGY
8. Limited/no auditing and monitoring capabilities 9. Lack of electronic access controls	19. Limited IT/cyber security focus 20. No use of authentication procedures 21. Out of date/not maintained IT systems 22. Limited hardware controls 23. Poor sophistication of IT systems
STRATEGIC	STRATEGIC
10. Lack of strong and well-defined organisational culture	24. Poor organisational communication 25. Ineffective change management 26. Undue secrecy 27. Complacency

QUESTION 2a

Do you agree that the primary factors listed above are the most important when identifying organisational vulnerability to insider threat?

YES	NO
☐	☐

Do you believe any of the secondary factors should be included in the top 10? If so, which factors should be included in the top 10?

Would you like to add further comments or add any factors?

PLEASE CONTINUE TO NEXT PAGE.

QUESTION 3

What factors do you consider DECREASE the likelihood of an intentional insider threat?

Below are a list of primary and secondary factors – based on Delphi results - that decrease the likelihood of insider threat.

PRIMARY STRENGTHS/MITIGATION	**SECONDARY STRENGTHS/MITIGATION**
PEOPLE	PEOPLE
1. Regular staff education and training; including security awareness 2. Strong and supportive leadership/positive leadership	1. Providing avenues for staff engagement and input, including performance reviews, staff surveys 2. Provision of an EAP/Staff counselling service 3. Compliance and risk management training for staff 4. Individual strengths; positive social support networks, conscientiousness, sound judgment 5. Screening and section (including psychological assessments, assessment centres, referees reports) 6. Performance reviews 7. High employee engagement 8. Background checks, including vetting and referee reports 9. Individual strengths; resilience, sound and reliable behaviour
PROCESS	PROCESS
3. Whistle-blower protection policies 4. Relevant security policies and procedures	10. Aiming for consistency across all organisational policies and processes 11. Relevant policies and training on how to identify and report concerning behaviour/security issues 12. Performance review policies 13. Feedback processes 14. Monitoring and enforcing policies 15. Relevant IT policies and procedures 16. Physical access control 17. Behaviour monitoring 18. Ongoing and evolving focus on risk management 19. Sound record keeping
TECHNOLOGY	TECHNOLOGY
5. Impeded access controls 6. Minimum privilege access 7. Obvious and declared security controls 8. Computer monitoring	20. Open source monitoring 21. Employee monitoring 22. Random auditing 23. Random audits 24. Data analytics 25. Automation of detection

STRATEGIC	STRATEGIC
9. Positive change management 10. Developing organisational resilience	26. Focus on research including, how offenders evaluate opportunity 27. Pulse surveys

QUESTION 3a

Do you agree that the primary factors listed above are the most important when identifying organisational factors that decrease insider threat?

YES ☐ NO ☐

Do you believe any of the secondary factors should be included in the top 10? If so, which factors should be included in the top 10?

Would you like to add further comments?

PLEASE CONTINUE TO NEXT PAGE.

QUESTION 4

Further questions have emerged from the analysis of the Delphi Round 2.

Question 4a

Do you believe organisations should have a separate Security section that is not part of Human Resources?

YES	NO	DON'T KNOW
☐	☐	☐

Please explain.

Question 4b

Do you believe organisations should have a formalised Cyber Security section or sub-contract ongoing cyber-security services?

YES	NO	DON'T KNOW
☐	☐	☐

Please explain.

QUESTION 5

Please rate the extent to which you agree to the following statements:

	Strongly Disagree	Disagree	Disagree a little	Neither Agree or Disagree	Agree a little	Agree	Strongly Agree
A lack of advanced technology is the principle cause of vulnerability to insider threat	☐	☐	☐	☐	☐	☐	☐
Organisational structure, processes, operations and culture are the principle cause of vulnerability to insider threat	☐	☐	☐	☐	☐	☐	☐
Current HR practices for existing employees and recruitment practices for prospective employees is the principle cause of vulnerability to insider threat	☐	☐	☐	☐	☐	☐	☐
The individual, irrespective of organisational culture, HR practices, IS vulnerabilities is the principle cause of insider threat	☐	☐	☐	☐	☐	☐	☐

QUESTION 6

Would you like to add any further comments?

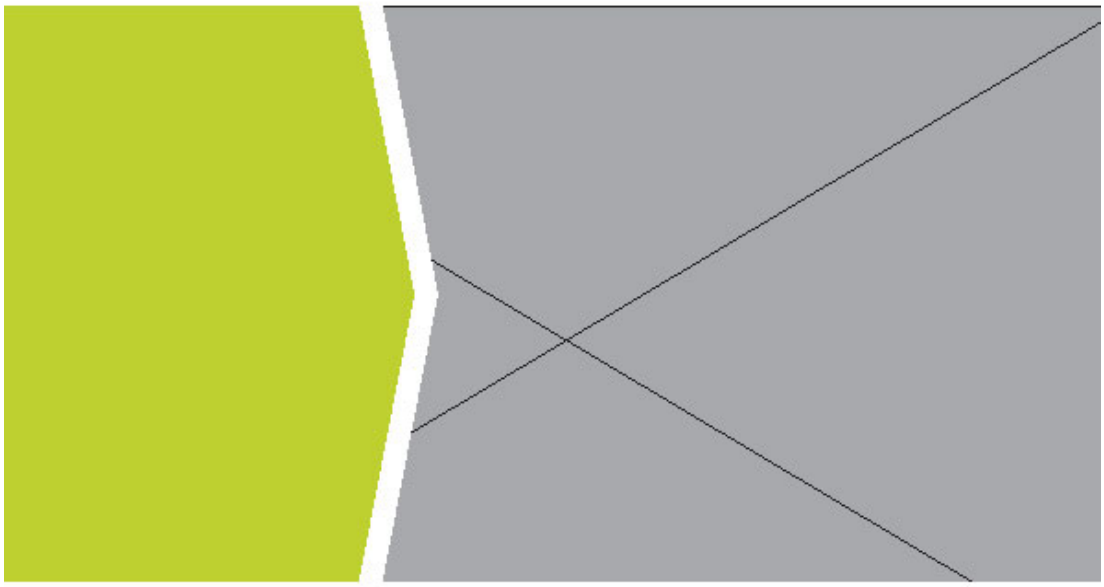
Thank- you.

Appendix G - Final Delphi Report

2016

FINAL REPORT

ORGANISATIONAL VULNERABILITY AND INTENTIONAL INSIDER THREAT:
A DELPHI STUDY



CONTACT: JUSTINE BEDFORD
justine@jconsulting.net.au
MOBILE: 0425 793 618

A DELPHI STUDY

INTRODUCTION

Being able to reduce an organisations vulnerability to intentional insider threat is a critical issue for most public and private organisations. Despite this and signs that insider threat will increase, research to better understand and address the problem is rare.

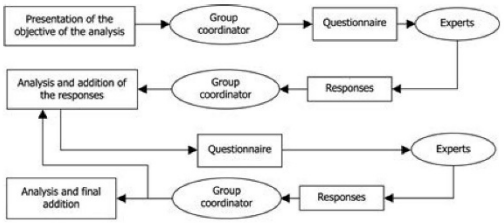
This study comprised a thematic review of literature to examine insider risk behaviour and utilised the Delphi Method to gather expert opinion (in the fields of security, risk management, organisational behaviour, cyber security, and intelligence) in order to determine organisational vulnerabilities that are relevant to assessment of intentional insider threat risk.

'COMPROMISE IS EXPENSIVE. IT CAN INCLUDE FINANCIAL LOSSES, DAMAGE TO REPUTATION, LOSS OF INTELLECTUAL PROPERTY AND DISRUPTION TO BUSINESS. AUSTRALIA CANNOT AFFORD THIS' –
AUSTRALIAN CYBER SECURITY CENTRE.

THE DELPHI METHOD

The Delphi method seeks to synthesise contributions from a panel of experts aimed at addressing a clearly stated problem. Panel members respond to semi-structured questions, in this case via email. The primary researcher is responsible for the collation and distillation of responses, by processing the information and filtering out irrelevant content. This avoids the negative effects of face-to-face panel discussions and solves the usual problems of group dynamics. It also protects the identity of participants.

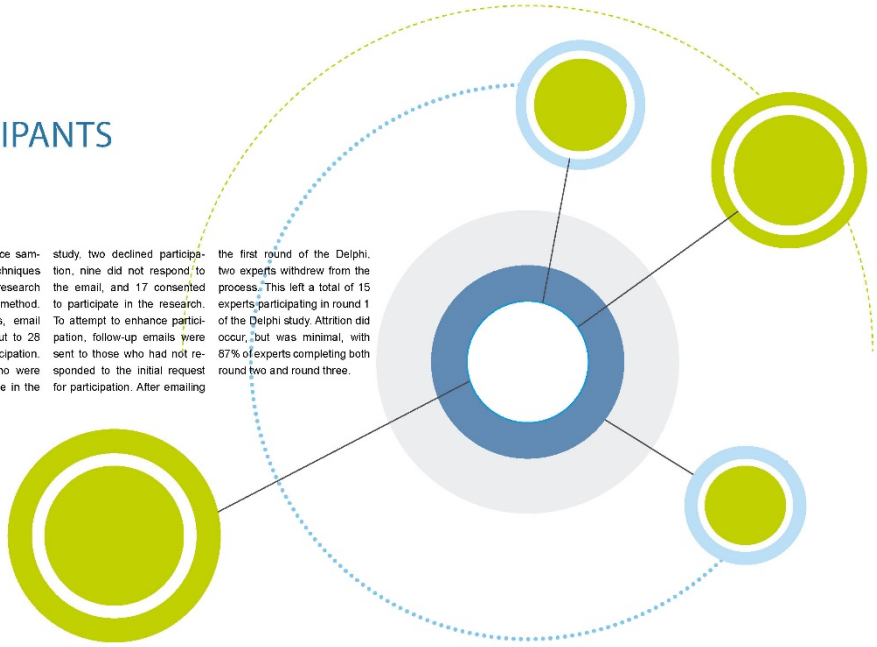
Regular feedback is provided. Participants comment on their own perspectives and the responses of others. At any moment they can revise their earlier statements.



Source: Adapted from Landeta (1999)

PARTICIPANTS

The use of convenience sampling and snowball techniques are commonplace in research employing the Delphi method. Using these methods, email requests were sent out to 28 experts inviting participation. Of the 28 experts who were contacted to participate in the study, two declined participation, nine did not respond to the email, and 17 consented to participate in the research. To attempt to enhance participation, follow-up emails were sent to those who had not responded to the initial request for participation. After emailing the first round of the Delphi, two experts withdrew from the process. This left a total of 15 experts participating in round 1 of the Delphi study. Attrition did occur, but was minimal, with 87% of experts completing both round two and round three.



ANALYSIS AND CONSENSUS

The data was screened and tested for normality (P-P plots). Descriptive statistics data variance were used to assess the responses from panel experts and determine the level of consensus. Consensus on a question was deemed to be achieved if a) at least 70 percent of panel members agreed on the direction of the response and b) there was no abnormal distribution of responses i.e. normal distribution, with a low variability and minimal outliers. Where any item achieved at least 70% agreement and there were no 'polar-opposite' responses of concern it was considered to have reached consensus.

Content analysis of qualitative data was used to determine emerging themes from responses to open ended questions.

Over the three rounds of the Delphi, factors and themes of vulnerabilities and capabilities were then further reviewed to determine those that were of primary importance (where more than 90% of panel experts agreed or raised an issue/idea and at least one third strongly agreed with that factor) and secondary importance (all other factors that reached consensus).

THE DEFINITION

Generally there was a strong agreement on the key words associated with defining insider threat early. By the end of the Delphi all panel experts agreed on the definition with the addition of reputation to be included. The final definition of intentional insider threat:

Intentional insider threat is when: a person of trust (employee, contractor, consultant, vendor) who has/had legitimate access to an organisation attempts to cause harm through counterproductive behaviour intended to result in the loss, disclosure, or damage to that organisation's information, resources, assets, or reputation.

ORGANISATIONAL VULNERABILITIES

Over the three rounds of the Delphi prominent vulnerabilities that increase the likelihood of insider threat became clear. 92.3% of panel experts agreed that the following were the 10 primary vulnerabilities.

PEOPLE	1. Ego/sense of entitlement 2. Disgruntlement 3. Ethical flexibility 4. Increase in staff counterproductive workplace behaviour/ workplace deviance
PROCESS	5. Poor security practices of leadership 6. Poor application of security 7. No consequences for poor security behaviour
TECHNOLOGICAL	8. Limited/no auditing and monitoring capabilities 9. Lack of electronic access controls
STRATEGIC	10. Lack of strong and well-defined organisational culture

NOTE: There were a number of panel experts who also wanted to include these secondary vulnerabilities in the top ten: The lack of strong and supportive leadership/management, No policies/procedures on how to manage potential security issues at emerging stages, Complacency.

ORGANISATIONAL STRENGTHS

Over the three rounds of the Delphi prominent strengths that decrease the likelihood of insider threat became clear. 100% of panel experts agreed that the following were the 10 primary strengths.

PEOPLE	1. Regular staff education and training, including security awareness 2. Strong and supportive leadership/positive leadership
PROCESS	3. Whistle-blower protection policies 4. Relevant security policies and procedures
TECHNOLOGICAL	5. Impeded access controls 6. Minimum privilege access 7. Obvious and declared security controls 8. Computer monitoring
STRATEGIC	9. Positive change management 10. Developing organisational resilience

NOTE: There were a number of panel experts who also wanted to include these secondary strengths in the top ten: Background checks, EAP services, Screening and selection (including psychological assessments, assessment centres, referee reports), Focus on risk management, Relevant policies and training on how to identify and report concerning behaviour/security issues.

OTHER FINDINGS

INSIDER THREAT IS A MULTIDISCIPLINARY CONCERN

Consensus (above 70% agreement) was not achieved for the following:

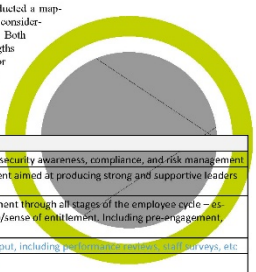
- A requirement to have a separate security and HR section.
- A lack of advanced technology being the principle cause of vulnerability to insider threat.
- Current HR practices for existing employees and recruitment practices for prospective employees being the principle cause of vulnerability to insider threat.
- No consensus on whether an employee, contractor, or consultant was more of a risk.

Consensus (above 70% agreement) was achieved for the following:

- 75% of experts agreed that organisations should have cybersecurity skills available whether internally or outsourced.
- 77% of the panel agreed that organisational structure, processes, operations and culture are the principle cause of vulnerability to insider threat.
- 77% of the experts indicated that the individual, irrespective of organisational culture, HR practices, and IS vulnerabilities is the principle cause of insider threat.
- Increasing staff counterproductive behaviour may be a sign of increased risk of intentional insider threat.

DETECTING AND PREVENTING INTENTIONAL INSIDER THREAT

Based on the Delphi outcomes the researcher conducted a mapping exercise to determine broad organisational considerations as they apply to intentional insider threat. Both primary and secondary vulnerabilities and strengths were considered. Please find below 15 themes for the detection and prevention of Intentional Insider Threat. These are broad themes which need further work but will likely underpin the proposed assessment tool in future stages of the Doctorate.



PEOPLE
1. Regular staff education and training; including security awareness, compliance, and risk management
2. Leadership training, education, and management aimed at producing strong and supportive leaders and managers
3. Appropriate employee monitoring and assessment through all stages of the employee cycle – especially as it relates to disgruntlement and ego/sense of entitlement. Including pre-engagement, engagement, and post-engagement
4. Providing avenues for staff engagement and input, including performance reviews, staff surveys, etc
5. Provision of an EAP/Staff counselling service
PROCESS
6. Relevant, endorsed, and monitored security policies and procedures; including whistle-blower protection policies, how to identify, report and manage concerning behaviour/security issues
7. Relevant, endorsed, and monitored IT policies and procedures
8. Aiming for consistency across all organisational policies and processes
TECHNOLOGY
9. Obvious and declared security controls
10. Random auditing and computer monitoring
11. Impeded access controls, including minimum privilege access, physical access controls, etc.
12. Open source monitoring
STRATEGY
13. Ongoing and evolving focus on risk assessment and management, including development of an Insider Threat response plan
14. Developing a resilient organisation with a strong organisational and security culture that can anticipate and manage negative workplace issues/behaviours
15. Focus on research including how offenders evaluate opportunity, how to develop a security culture, etc.

THANK YOU

A very big thank you to all the panel experts for their time and commitment to this Delphi Study. I have very much appreciated the efforts of all. I have enjoyed reading all of the commentary and hope I have synthesised the results in a meaningful way for you in this overview of the results.

If you have any further comments please do not hesitate to contact me.

JUSTINE BEDFORD

justine@jconsulting.net.au

0425 793 618

Appendix H - Ethics Approval

OFFICE OF RESEARCH
Human Research Ethics Committee
PHONE +61 7 4631 2690| FAX +61 7 4631 5555
EMAIL ethics@usq.edu.au

UNIVERSITY OF SOUTHERN QUEENSLAND AUSTRALIA

8 October 2015

Ms Justine Bedford
PO Box 302
Altona VIC 3018

Dear Justine

The USQ Human Research Ethics Committee has recently reviewed your responses to the conditions placed upon the ethical approval for the project outlined below. Your proposal is now deemed to meet the requirements of the *National Statement on Ethical Conduct in Human Research (2007)* and full ethical approval has been granted.

Approval No.	**H15REA112**
Project Title	Organisational vulnerability to insider threat - Development of an organisational vulnerability assessment identifying intentional insider threat risk
Approval date	8 October 2015
Expiry date	8 October 2018
HREC Decision	**Approved**

The standard conditions of this approval are:

(a) conduct the project strictly in accordance with the proposal submitted and granted ethics approval, including any amendments made to the proposal required by the HREC
(b) advise (email: ethics@usq.edu.au) immediately of any complaints or other issues in relation to the project which may warrant review of the ethical approval of the project
(c) make submission for approval of amendments to the approved project before implementing such changes
(d) provide a 'progress report' for every year of approval
(e) provide a 'final report' when the project is complete
(f) advise in writing if the project has been discontinued.

For (c) to (e) forms are available on the USQ ethics website:

http://www.usq.edu.au/research/ethicsbio/human

Please note that failure to comply with the conditions of approval and the *National Statement (2007)* may result in withdrawal of approval for the project.

You may now commence your project. I wish you all the best for the conduct of the project.

Annmaree Jackson
Ethics Coordinator

Copies to: justinebedford@hotmail.com

Appendix I – Original 242 Questions of the OVIT

1. Gender
2. Age
3. Education
4. Job Level
5. Industry
6. APS Industry Sector
7. Size of Organisation
8. My level of expertise on Insider Threat issues is...
9. does the organisation check civil records
10. does the organisation evaluate employee behaviour outside of the workplace
11. does the organisation have methods to assess sound and reliable behaviour of staff
12. does the organisation have policy and processes to manage staff with a history of security violations
13. does the organisation test for illegal drug use
14. does the organisation assess past substance use/abuse
15. does the organisation assess for problematic gambling behaviour
16. does the organisation have policies describing unacceptable workplace interpersonal behaviours
17. does the organisation have a good conduct policy
18. does the organisation review credit reports
19. is financial, credit, and bankruptcy history assessed by the organisation
20. does the organisation have methods to identify financial pressures of employees
21. does the organisation undertake a formal risk assessment of high risk employees/positions, determining level of risk and mitigation strategies
22. does the organisation have a means by which employees can report suspicious contacts from other employees or outsiders
23. does the organisation allow the hiring of employees with close connections to current staff (friends/family)
24. does the organisation assess for positive support networks of employees
25. does the organisation evaluate risk-related criminal associations
26. does the organisation check criminal records
27. does the organisation have policy/guidelines describing how to identify and respond to employees susceptible to social engineering (manipulation of people to get them to unwittingly perform actions that may cause harm)
28. does the organisation monitor foreign contacts of staff
29. does the organisation monitor staff travel
30. does the organisation have policy/guidelines describing how to identify and respond to employees experiencing stress

31. does the organisation have clear procedures describing access to and benefits of employee assistance programs and other employee support services
32. does the organisation monitor/assess staff after negative/stressful events
33. does the organisation conduct performance reviews and is therefore aware of declining performance ratings
34. does the organisation have policies and procedures for referring at-risk employees facing negative personnel actions to appropriate teams for evaluation
35. does the organisation have branches, suppliers, subcontractors or other affiliates abroad, where differences in cultural beliefs and values may affect loyalty to the organisation versus other local groups
36. is the organisation currently affected by economic or financial stressors that influence its treatment of employees in a manner that could increase insider risk
37. does the organisation have policies and procedures designed to improve loyalty
38. do policy and processes of the organisation promote individual differences (gender, culture, ethnicity)
39. are staff in the organisation educated on the different reasons behind insider threat actions
40. is motivation for employment assessed during recruitment processes
41. are individual attitudes assessed by the organisation
42. does the organisations structure allow for specific individuals to control majority of the power
43. are specific individual's politics and power a problem for the organisation
44. does the organisation assist staff/individuals to improve their communication
45. does the organisation use methods to assess alignment between employee values and organisational values
46. does the organisation utilise methods during recruitment processes to assess for ego/sense of entitlement
47. does the organisation use methods to assess for ethical flexibility of staff
48. does the organisation utilise methods to assess for employee resilience
49. does the organisation have methods to identify changes in employee resilience
50. does the organisation offer resilience training to staff
51. does the organisation utilise methods to assess for employee sound judgment
52. does the organisation utilise methods to assess for employee conscientiousness
53. does the organisation conduct mental health testing/assessment
54. does the organisation conduct personality testing to determine an employee's vulnerability to become an insider threat
55. are trained professionals employed by the organisation to identify and manage employees vulnerable to becoming an insider threat
56. does the organisation utilise methods to assess for employee self-awareness
57. does the organisation have programs to develop employee self-awareness
58. does the organisation have mechanisms in place in order to know of any pending sanctions of contractors and outside staff
59. does the organisation carefully consider any vendors/partnerships etc. based on ethical conduct
60. does the organisation assess moral development
61. the organisation has methods to assess for addictions

62. workplace deviance is handled appropriately within the organisation
63. the organisation encourages development of positive support networks
64. the organisation has methods for identifying and managing potential disgruntlement
65. the organisation actively manages employee expectation to minimise potential for unmet expectations
66. the organisation understands the cultures of partner stakeholders
67. commitment to the organisation is high amongst staff
68. people in the organisation value differences in culture, race, & ethnicity
69. the organisation has proactive initiatives and outreach to staff that may be at increased risk of insider threat actions
70. the attitude of staff is a problem in the organisation
71. positive individual attitudes are nurtured by the organisation
72. the organisations practices and policies promote individual power
73. the practices and policies of the organisation allows for individual specific agendas
74. the organisation suffers from poor politics
75. the organisation has a problem with individual communication
76. people in the organisation maintain high ethical standards
77. people in the organisation demonstrate high integrity & honesty
78. reporting procedures of the organisation allow staff to identify and report on the poor judgment of others
79. does the organisation have policies and practices mandating security awareness training
80. does the organisation offer specific training and education programs addressing policy and practice areas relevant to insider threat
81. does the organisation structure security awareness training and education efforts appropriately to the needs of different employees groups such as managers, system administrators, human resources personnel, etc.
82. does the organisation require attendees to demonstrate their competence in training and education programs as a condition of program completion
83. does the organisation have a dedicated team and trained staff to undertake vetting and background checks of prospective employees
84. are all staff (including vendor staff, contractors, and are outsourced roles) subject to vetting processes relevant to their level of access/role
85. do staff in the organisation receive training on risk management
86. does a specialised team (including HR, legal, employee assistance programs, physical and IT security, and behavioural science members) exist to evaluate the risk of insider threat
87. are a variety of informal and formal staff consultation methods utilised by the organisation to understand staff views/opinions
88. does the organisation have guidelines describing the organisations right to monitor and audit employee activity including their behaviour
89. does the organisation conduct informal online searches of employees
90. does the organisation use a variety of fair, ethical, transparent and legal means to monitor its employees
91. are employees actively monitored for insider risk behaviour during the probationary period

92. does the organisation have policies facilitating preemployment screening
93. does the organisation contact previous employers to understand the individual's competence and approach to dealing with workplace issues
94. does the organisation conduct periodic or follow-up investigative actions to ensure that employees remain reliable and are not subject to compromising factors
95. does the organisation utilise evidence-based recruitment and assessment methods
96. does the organisation conduct its own research on insider threat
97. does the organisation benchmark its processes and controls (technical and non-technical) against leading practices
98. does the organisation have policies and processes to attempt to identify moles
99. has the organisation identified moles in the past
100. does the organisation promote integrated approaches to insider threat management
101. does the organisation have a senior management position dedicated to security who answers to a Board member, with a dedicated security team to implement required measures
102. does the organisation have an established insider threat contingency management plan
103. are risk transfer methods (insurance, contracts, etc.) part of the organisations risk management
104. are management security actions enforced without discrimination, recorded, and subsequently evaluated for effectiveness
105. does the organisation have strong and positive leadership
106. does management in the organisation communicate clear plans & objectives for the organisation
107. does the organisation regularly use methods to identify and assess its own security culture
108. does the organisation have clear, publicly available, and consistently enforced methods for investigating and penalising inappropriate security behaviour
109. does the organisation track security compliance and take steps to confirm compliance
110. does the organisation have measures and processes in place to measure organisational culture
111. does the organisation have multiple means for tracking increases in counterproductive workplace behaviour
112. does the organisation have principles, policies, and practices to help manage the risk of counterproductive behaviour in the workplace
113. does the management of the organisation integrate insider threat mitigation as part of the broader enterprise risk mitigation strategy
114. is the organisation committed to the prevention, detection, deterrence, and response to insider threats
115. does the organisation undertake regular risk assessments as the environment changes
116. does the organisation assess level of employee engagement through annual surveys and/or pulse surveys
117. does the organisation actively assess job and organisational fit to ensure employee engagement
118. does the organisation encourage staff to participate in all organisational activities and events
119. does the organisation have processes in place to monitor at-risk employees after negative workplace events
120. does the organisation monitor external factors (economic downturns, competition) that may increase employee's potential for insider threat activity
121. is the organisation constantly/regularly undergoing some level of significant organisational change
122. is the organisation structured to allow for open and efficient communication across all levels

123. are organisational policies ill-defined or loosely enforced
124. does the organisation actively investigate reports of at-risk behaviours in a manner that does not deter future reports
125. do people in the organisation report suspicious behaviour in the workplace
126. does the organisation have obvious and declared security controls
127. does confidential reporting exist so that employees can report suspicious events without fear of repercussion
128. does the organisation have a whistle-blower protection policy
129. does the organisation have policies that protect the security of organisational information and IT resources
130. does the organisation have implemented security practices to prevent unauthorised disclosure of sensitive information
131. does the organisation regularly review and update insider threat and security policy and procedures
132. does the organisation have policy to conduct random reviews of exiting staff computer activities leading up the final date
133. are policies and processes in place to ensure that the privileges and accesses of staff leaving the organisation are disabled
134. does the organisation require that all staff, contractors, consultants, and vendors sign non-disclosure statements when leaving the organisation
135. does the organisation have policies protecting the physical security of facilities
136. does the organisation review physical access anomalies and denials
137. does the organisation capture information on an employee's physical movements within and around the organisations facility/ies
138. the organisation prevents unauthorised access to physical assets
139. the organisation keeps abreast of best practice when it comes to insider threat
140. the organisation is at risk of moles being placed within its ranks
141. the organisation is good at addressing underlying systemic issues that may be linked to increased risk of insider threat
142. the organisation integrates risk assessment into everyday business decisions
143. the organisation is better equipped to cope with insider threat challenges when compared to other organisations in the same sector
144. the organisation is able to learn from failures and mistakes
145. the organisation is resilient
146. the security practices of leadership in the organisation is poor
147. management in the organisation are accountable and responsible to others
148. management in the organisation lead by example when it comes to security practice
149. management in the organisation do not hesitate to provide the leadership that is needed
150. the organisation fosters an environment that is conducive to the success of insider threat initiatives
151. the organisation has a poor security culture
152. the values of the organisation are made explicit and help to build a strong security culture
153. management in the organisation provide the support and resources needed to help staff meet their goals
154. management in the organisation actively listen to problems of staff

155. management in the organisation take care to be informed about how others think and feel about things
156. management in the organisation encourage staff to speak up about employee issues
157. that, overall, staff of the organisation engage in poor security behaviour
158. management in the organisation value the input of all staff
159. staff in the organisation are treated fairly by management in the organisation
160. there is a perception in the organisation that management do not value staff
161. the organisation has a positive organisational culture
162. both overt and covert messages are corrected to create a positive organisational culture
163. the organisation regularly identifies and assesses its own organisational culture
164. there is an increasing level of counterproductive behaviour in the organisation
165. the organisation is prepared to respond to counterproductive workplace behaviour and enforce its policies
166. when it comes to insider threat the organisation is complacent
167. the organisation is aware of its risk tolerance level/risk appetite
168. staff of the organisation are aware of its critical assets that are worth protecting
169. there is a lack of management of potential insider threat issues at the emerging stages
170. staff are aware of how insider threat concerns are managed in the organisation
171. people in the organisation are willing to go above and beyond to achieve the organisations mission
172. there is a high level of collegiality within the organisation
173. the organisation increases its monitoring capabilities when significant organisational change occurs
174. leaders in the organisation communicate a clear vision of the future of the organisation
175. the organisation balances trust with the application of consistent employee monitoring
176. there is a high level of undue secrecy in the organisation
177. the organisation is open and honest with its employees
178. management in the organisation promote open communication and sharing of information
179. management in the organisation encourage staff to participate in important decisions
180. in general, people in the organisation are clear on the objectives of the organisation
181. policies and expectations are consistent across all levels of the organisation
182. security reporting is encouraged in the organisation
183. staff are aware of the security controls utilised by the organisation
184. the organisation has a whistle-blower policy that has the confidence of all employees
185. the organisation has relevant IT policies and procedures
186. the organisation is committed to improving security in order to protect its information and resources

187. security controls of the organisation are adequate and applied whenever necessary
188. the organisation is prepared to respond to security non-compliance and enforce its policies
189. staff in the organisation can identify and report on red flags
190. the organisation has a proactive and risk-based approach to mitigating emerging insider threats
191. security awareness is high among staff and considered in the daily activities of all organisational members
192. staff in the organisation are aware of and educated to support the insider threat program
193. the organisation provides tailored and relevant insider threat education and awareness to all staff
194. staff use relevant risk management and compliance considerations in everyday work decisions
195. staff in the organisation are vigilant and able to monitor emerging threats
196. the opinions and ideas of staff are important to the organisation
197. the organisation has strict exit controls in place for all exiting staff
198. does the organisation allow staff a variety of virtual work arrangements (including working from home)
199. does the organisation have a well-documented on-boarding process for all new starters that ensures appropriate access controls are implemented
200. does the organisation have guidelines to ensure that staff only have access to data, systems, and information required to perform their duties
201. does the organisation implement multi-factor authentication (e.g.- a password plus a one-time code from a hardware token)
202. do authentication procedures become more advanced with increasing access to critical information/data
203. are processes in place to ensure that staff changing roles/jobs within the organisation only maintain relevant access
204. is access to sensitive systems and areas enforced by authentication procedures monitored for anomalies
205. does the organisation have guidelines on how duties are separated for privileged functions
206. do staff with duties that require higher levels of access (such as administrative roles) have a separate account for more sensitive tasks (and not used for daily tasks such as checking email)
207. does the organisation require multiple users to action all modifications to critical systems, network, applications, and data
208. does the organisation restrict administrators from controlling auditing functions
209. is routine auditing of privileged functions conducted by the organisation
210. are advanced analytics tools used in the organisation to analyse and report on insider threat
211. are privileged accounts monitored and audited regularly
212. is random auditing of IT use implemented
213. is auditing part of performance reviews
214. does the organisation monitor common data exfiltration methods (e-mail, removable media) to identify anomalous behaviour
215. is network traffic and associated security logs collected centrally and monitored for anomalies
216. does the organisation monitor key databases, data access and movement
217. does the organisation monitor IT behaviour of employees

218. does the organisation use modern technologies to assist insider threat detection, deterrence, prevention and reporting
219. does the organisation have means to monitor trends in IT policy breaches to inform corrective action
220. does the organisation maintain pace with current technology lifecycles, with an organisation wide refresh every 5 years or so
221. does the organisation have back-up and recovery processes in place to avoid disruption
222. does the organisation have restrictions on hardware usage such that potential threats to unauthorised data removal are disabled (such as disabling all USB ports)
223. does the organisation allows its staff to use their own devices for work (BYOD)
224. does the organisation use regular penetration testing to strengthen defences
225. does the organisation hire technically sophisticated system administrators or programmers
226. do managers of IT/cyber employees have management training to improve their management of people not just technology
227. does the organisation have a clear list of access privileges for all roles
228. does the organisation review access request denials
229. does computing equipment connected to the corporate network of the organisation reside in an area that has electronic access controls in place (i.e.- requires a swipe card to access)
230. are special authentication procedures employed for database administrators
231. IT administrative accounts are limited and regularly audited
232. least privilege principles are enforced by the organisation
233. there is a lack of electronic access controls in the organisation
234. limited authentication procedures is a concern for the organisation
235. unauthorised persons are prevented from accessing resources and information
236. the organisation has well established access controls to ensure only authenticated users with the right permission can access information
237. no one individual can complete a critical business process from start to finish
238. targeted monitoring is increased when behavioural or technical precursors are discovered
239. the organisation has an holistic approach to monitoring utilising IT, HR, and physical security information for a more complete risk assessment
240. the sophistication of IT systems in the organisation is poor
241. the organisation has limited hardware controls
242. the organisation leaves insider threat responsibility to IT and information security sections

Appendix J – Ethical Decision Making Model

(https://www.psychology.org.au/inpsych/2013/december/ethics/)

1. Recognise that there is an ethical issue present

Learn to recognise potential ethical problems

Check if there are any personal 'clues' that may alert you, such as: changing your usual professional practices; providing more self-disclosure than usual; avoiding certain topics; ruminating after a session with a client; or feeling uncomfortable or regretful.

Ask yourself: "Would I be comfortable if my colleagues knew about this situation?"

Reflect on whether there is anything adversely influencing your capacity to assess the situation objectively, such as personal needs, values or biases that may be distorting your perception.

Consider discussing the issue with a colleague or supervisor to assess your initial response.

Determine whether the problem is an ethical one that is your responsibility

Articulate the problem as succinctly as you can and then consider the following questions:

Are there any legal obligations that apply in this situation that are contributing to or may even override the ethical issues

(e.g., a mandatory reporting obligation, a client's right of access to his/her health record)?

Is the problem based on information from factual material?

Has the information come from a reliable source?

Is the problem your responsibility or someone else's, or perhaps a shared responsibility?

2. Clarify the ethical issues

Identify the ethical principles involved

Identify which of the three General Principles of the *APS Code of Ethics* is relevant to the issue:
Respect for the rights and dignity of all people and peoples; Propriety; Integrity.
Drill down to identify the ethical standards that are relevant and consult the *Ethical Guidelines* where necessary to assist with this task.
Identify any competing ethical principles, e.g., the right to autonomy versus the right to confidentiality.
Identify any aspects of the situation that are exerting pressure on you to act quickly, and think about how to claim more time to make the best possible decision.

Evaluate the rights, responsibilities and vulnerabilities of all affected parties
Identify who else is involved, implicated or affected by this issue (including institutions or the general public where relevant).
Consider the rights and responsibilities of each of the people involved (e.g., the right to confidentiality, privacy, autonomy).
Consider how this issue will affect the welfare of each of the people involved, keeping in mind your responsibility to ensure your client's welfare takes precedence. Don't forget to consider your own rights, responsibilities and welfare in this situation.
Try to identify any gaps in your thinking and knowledge by talking with a colleague or supervisor.

3. Generate and examine available courses of action

Pause to consider all factors that might influence the decision you will make, including your level of competence.
Reflect on any social or cultural factors that should be taken into consideration.

Consider the timelines and include the decision to wait and gather more information, where appropriate and possible.
Identify possible alternative courses of action and examine the positive and negative consequences of each.
Consult a trusted colleague, supervisor and/or your professional organisation.

4. Choose and implement the most preferred option

Decide on your most preferred course of action and implement it.
Ensure that you document the issue and how you decided on the course of action, including any consultation with colleagues and reference to ethics resources, which may be required at a later date in the event of a complaint or legal action.

5. Reflect on and review the process

Reflect on your own role in the situation and ask yourself:
Could I have prevented the issue from developing?
Am I satisfied with the way I managed the situation and the processes I engaged in?
Could I have done anything differently at any stage?
Is there anything I can do differently in future to prevent such a situation (i.e., integrate my learning into my ongoing professional life)?

Appendix K – Ethical considerations of the current research

Ethical consideration	Definition	Applied to the Delphi Method	Applied to the Survey Method
Requirement for USQ Ethics Approval	Granting of ethics approval	Human Research Ethics Approval received.	Human Research Ethics Approval received.
Right to Autonomy and Informed consent	Benefits, rights, and risks of participation (Shariff 2015)	• Participants in the study required to acknowledge consent. • Participation was voluntary and there was no pressure, coercion, payment, or inducements as part of gaining consent. • Participants are all adults. • Information explaining the purpose of the study was provided at the request for participation and at each subsequent round. • The contact details of the researcher, supervisor, and ethics committee was made available to all participants.	• Participants in the study required to acknowledge consent. • Participation was voluntary and there was no pressure, coercion, payment, or inducements as part of gaining consent. • Participants are all adults. • Information explaining the purpose of the study was included on the landing page of the survey. • The contact details of the researcher, supervisor, and ethics committee was made available to all participants.
Accessibility	Ability to contact the researcher	• All communication regarding the research provided contact details of the primary researcher, the supervisory team, and the ethics committee. • No concerns were received throughout the duration of the project.	• Details of the primary researcher, the supervisory team, and the ethics committee were available on the survey. • No concerns were received throughout the duration of the project.
Anonymity and Confidentiality	Concealing the identity of participants (Shariff 2015)	• In the Delphi process anonymity of participants was assured through use of re-identifiable data (The National Health and Medical	• In the survey the participants were completely anonymous to the research team.

		Research Council 2007 (updated March 2014)) • Identifiers were replaced by a code or pseudonym. • Original identifiers were kept to a minimum, (for example only using initials and industry). • The details of the Delphi experts were only known to the primary researcher. • The researcher did not reveal identities of participants to others (Shariff 2015). • Judgements, opinions, and specific answers were not attributable to a specific person and remained strictly anonymous (McKenna 1994)	
Recruitment of participants	How participants were chosen for participation	• Participation in the study was voluntary. • Approach to adult convenience sample requesting participation via email. • Suggestions for further participants generated from these initial participants (snowball).	• Participation in the study was voluntary. • Approach to convenience sample via email. • Suggestions for further participants generated from these initial participants (snowball). • Convenience sample through LinkedIn network, USQ Master/Doctoral student network.
Right to Self-Determination	The entitlement of peoples to have control over their destiny and to be treated respectfully (Attorney General's Department 2018)	• Participation was voluntary. • Participants were able to choose which questions they answered and what information they chose to share with the researcher.	• Participation was voluntary. • Participants were able to choose which demographic questions they answered.

		• Participants were able to withdraw at any time without penalty.	• Participants were able to withdraw at any time without penalty.
Intellectual property	"the property of your mind or proprietary information" (IP Australia 2018)	Before commencing the research the development of a clear understanding between the researcher, academic supervisor, and workplace supervisor/s was established.	
Information security and Cyber security	The protection of Information from unauthorised use or accidental modification, loss or release (University of Southern Queensland 2014)	• To protect research data/information from improper access, IT measures such as appropriate firewalls and software controls were in place (Desai & von der Embse 2008).	
Disclosure	Release of information	• Data will be kept for the university minimum time of five years following completion of the research. • Participants in the Delphi were provided with a report of findings. • As participants of the survey were anonymous the provision of outcomes was not available. • Research outcomes may be available through publication.	

Appendix L – Descriptive Statistics

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation	Skewness		Kurtosis	
	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic	Std. Error
Gender	140	1	2	1.46	.501	.145	.205	-2.008	.407
Age	139	1	6	3.47	1.038	.384	.206	.460	.408
Education	140	1	7	4.18	1.248	-.615	.205	.452	.407
Job Level	139	1	6	3.32	1.532	.396	.206	-.821	.408
Industry	139	1	4	1.61	.776	1.275	.206	1.354	.408
APS Industry Sector	135	1	9	4.35	2.417	.327	.209	-1.500	.414
Size of Organisation	137	1	4	3.31	1.020	-1.213	.207	.074	.411
Location	39	1	7	3.41	1.666	.741	.378	.085	.741
My level of expertise on Insider Threat issues is...	137	1	5	2.93	1.279	-.304	.207	-1.266	.411
IND does the organisation check civil records	141	1	5	3.38	1.418	-.430	.204	-1.118	.406
IND does the organisation have methods to assess sound and reliable behaviour of staff	141	1	5	3.48	1.169	-.566	.204	-.467	.406
IND does the organisation have policy and processes to manage staff with a history of security violations	141	1	5	3.21	1.525	-.293	.204	-1.404	.406

IND does the organisation test for illegal drug use	141	1	5	2.39	1.520	.553	.204	-1.273	.406
IND does the organisation assess past substance use/abuse	141	1	5	2.50	1.620	.515	.204	-1.381	.406
IND does the organisation assess for problematic gambling behaviour	141	1	5	2.41	1.586	.595	.204	-1.265	.406
IND does the organisation have a good conduct policy	141	1	5	3.96	1.206	-1.230	.204	.719	.406
IND is financial, credit, and bankruptcy history assessed by the organisation	141	1	5	2.63	1.684	.343	.204	-1.604	.406
IND does the organisation have methods to identify financial pressures of employees	141	1	5	2.41	1.440	.471	.204	-1.218	.406
IND does the organisation undertake a formal risk assessment of high risk employees/positions, determining level of risk and mitigation strategies	141	1	5	2.79	1.476	.145	.204	-1.372	.406
IND does the organisation have a means by which employees can report suspicious contacts from other employees or outsiders	141	1	5	3.72	1.300	-.644	.204	-.730	.406
IND does the organisation allow the hiring of employees with close connections to current staff (friends/family)	141	1	5	3.44	1.130	-.360	.204	-.378	.406

IND does the organisation assess for positive support networks of employees	141	1	5	2.91	1.317	.026	.204	-1.144	.406
IND does the organisation evaluate risk-related criminal associations	141	1	5	3.01	1.645	-.031	.204	-1.629	.406
IND does the organisation check criminal records	141	1	5	3.82	1.499	-.867	.204	-.818	.406
IND does the organisation have policy/guidelines describing how to identify and respond to employees susceptible to social engineering (manipulation of people to get them to unwittingly perform actions that may cause harm)	141	1	5	2.47	1.427	.462	.204	-1.153	.406
IND does the organisation monitor foreign contacts of staff	141	1	5	2.43	1.475	.520	.204	-1.223	.406
IND does the organisation monitor staff travel	141	1	5	3.08	1.540	-.121	.204	-1.518	.406
IND does the organisation have clear procedures describing access to and benefits of employee assistance programs and other employee support services	141	1	5	3.72	1.306	-.709	.204	-.646	.406
IND does the organisation monitor/assess staff after negative/stressful events	141	1	5	3.43	1.232	-.435	.204	-.706	.406

IND does the organisation conduct performance reviews and is therefore aware of declining performance ratings	141	1	5	3.98	1.124	-.998	.204	.257	.406
IND does the organisation have policies and procedures for referring at-risk employees facing negative personnel actions to appropriate teams for evaluation	141	1	5	3.22	1.219	-.167	.204	-.762	.406
IND does the organisation have branches, suppliers, subcontractors or other affiliates abroad, where differences in cultural beliefs and values may affect loyalty to the organisation	141	1	5	2.62	1.257	.372	.204	-.841	.406
IND does the organisation have policies and procedures designed to improve loyalty	141	1	5	2.89	1.274	.076	.204	-1.079	.406
IND do policy and processes of the organisation promote individual differences (gender, culture, ethnicity)	141	1	5	3.57	1.232	-.494	.204	-.730	.406
IND are staff in the organisation educated on the different reasons behind insider threat actions	141	1	5	2.49	1.234	.383	.204	-.822	.406

IND is motivation for employment assessed during recruitment processes	141	1	5	3.63	1.239	-.569	.204	-.735	.406
IND does the organisations structure allow for specific individuals to control majority of the power	141	1	5	3.13	1.212	-.053	.204	-.985	.406
IND does the organisation assist staff/individuals to improve their communication	141	1	5	3.19	1.062	.081	.204	-.473	.406
IND does the organisation use methods to assess alignment between employee values and organisational values	141	1	5	3.11	1.269	-.075	.204	-.981	.406
IND does the organisation utilise methods during recruitment processes to assess for ego/sense of entitlement	141	1	5	3.16	1.366	-.112	.204	-1.273	.406
IND does the organisation utilise methods to assess for employee resilience	141	1	5	3.18	1.300	-.157	.204	-1.055	.406
IND does the organisation offer resilience training to staff	141	1	5	2.82	1.099	.210	.204	-.311	.406
IND does the organisation utilise methods to assess for employee sound judgment	141	1	5	3.04	1.206	-.083	.204	-.822	.406

IND does the organisation utilise methods to assess for employee conscientiousness	141	1	5	3.18	1.268	-.289	.204	-.876	.406
IND does the organisation conduct mental health testing/assessment	141	1	5	2.57	1.415	.406	.204	-1.165	.406
IND does the organisation conduct personality testing to determine an employee's vulnerability to become an insider threat	141	1	5	2.66	1.558	.365	.204	-1.417	.406
IND are trained professionals employed by the organisation to identify and manage employees vulnerable to becoming an insider threat	141	1	5	2.44	1.461	.609	.204	-1.052	.406
IND does the organisation utilise methods to assess for employee self-awareness	141	1	5	2.83	1.347	.102	.204	-1.168	.406
IND does the organisation have programs to develop employee self-awareness	141	1	5	2.60	1.164	.188	.204	-.882	.406
IND does the organisation have mechanisms in place in order to know of any pending sanctions of contractors and outside staff	141	1	6	3.81	1.989	-.156	.204	-1.610	.406

IND does the organisation carefully consider any vendors/partnerships etc. based on ethical conduct	141	1	6	3.86	1.650	-.167	.204	-1.179	.406
IND does the organisation assess moral development	141	1	6	3.39	1.923	.146	.204	-1.509	.406
IND the organisation has methods to assess for addictions	141	1	5	2.73	1.241	.073	.204	-1.232	.406
IND workplace deviance is handled appropriately within the organisation	141	1	5	3.10	1.084	-.166	.204	-.931	.406
IND the organisation has methods for identifying and managing potential disgruntlement	141	1	5	3.20	1.030	-.488	.204	-.618	.406
IND the organisation actively manages employee expectation to minimise potential for unmet expectations	141	1	5	3.06	.994	-.085	.204	-.636	.406
IND commitment to the organisation is high amongst staff	141	1	5	3.52	1.032	-.601	.204	-.134	.406
IND the attitude of staff is a problem in the organisation	141	1	5	2.57	1.104	.247	.204	-1.038	.406
IND positive individual attitudes are nurtured by the organisation	141	1	5	3.40	1.035	-.446	.204	-.411	.406
IND the practices and policies of the organisation allows for individual specific agendas	141	1	5	3.00	1.028	-.120	.204	-.557	.406

IND the organisation suffers from poor politics	141	1	5	2.84	1.240	.110	.204	-1.099	.406
IND the organisation has a problem with individual communication	141	1	5	2.86	1.169	.090	.204	-.946	.406
IND people in the organisation maintain high ethical standards	141	1	5	3.76	.909	-.657	.204	.261	.406
IND people in the organisation demonstrate high integrity & honesty	141	1	5	3.74	.961	-.577	.204	-.139	.406
does the organisation offer specific training and education programs addressing policy and practice areas relevant to insider threat	141	1	5	2.53	1.251	.260	.204	-1.085	.406
does the organisation structure security awareness training and education efforts appropriately to the needs of different employees groups such as managers, system administrators, human resources personnel, etc.	141	1	5	2.71	1.234	.063	.204	-1.086	.406
are all staff vetted	141	1	5	3.52	1.432	-.480	.204	-1.187	.406
does a specialised team (including HR, legal, employee assistance programs, physical and IT security, and behavioural science members) exist to evaluate the risk of insider threat	141	1	5	2.60	1.439	.272	.204	-1.331	.406

are a variety of informal and formal staff consultation methods utilised by the organisation to understand staff views/opinions	141	1	5	3.26	1.045	-.454	.204	-.021	.406
does the organisation have guidelines describing the organisations right to monitor and audit employee activity including their behaviour	141	1	5	3.27	1.346	-.415	.204	-.988	.406
does the organisation conduct informal online searches of employees	141	1	5	2.67	1.205	.247	.204	-.757	.406
does the organisation utilise evidence-based recruitment and assessment methods	141	1	5	3.48	1.211	-.730	.204	-.356	.406
does the organisation conduct its own research on insider threat	141	1	5	2.96	1.290	-.095	.204	-1.094	.406
does the organisation benchmark its processes and controls (technical and non-technical) against leading practices	141	1	5	2.32	1.244	.455	.204	-.927	.406
does the organisation have policies and processes to attempt to identify moles	141	1	5	2.23	1.280	.671	.204	-.654	.406
does the organisation promote integrated approaches to insider threat management	141	1	5	2.25	1.172	.637	.204	-.455	.406

does the organisation have a senior management position dedicated to security who answers to a Board member, with a dedicated security team to implement required measures	141	1	5	2.83	1.554	.010	.204	-1.593	.406
does the organisation have an established insider threat contingency management plan	141	1	5	2.50	1.356	.365	.204	-1.181	.406
are risk transfer methods (insurance, contracts, etc.) part of the organisations risk management	141	1	5	3.05	1.261	-.138	.204	-.980	.406
are management security actions enforced without discrimination, recorded, and subsequently evaluated for effectiveness	141	1	5	2.94	1.226	-.066	.204	-.895	.406
does the organisation have strong and positive leadership	141	1	5	3.52	1.066	-.585	.204	-.082	.406
does management in the organisation communicate clear plans & objectives for the organisation	141	1	5	3.48	1.125	-.612	.204	-.297	.406
does the organisation regularly use methods to identify and assess its own security culture	141	1	5	2.89	1.181	-.081	.204	-.877	.406

does the organisation have clear, publicly available, and consistently enforced methods for investigating and penalising inappropriate security behaviour	141	1	5	2.84	1.296	.089	.204	-1.125	.406
does the organisation track security compliance and take steps to confirm compliance	141	1	5	3.18	1.217	-.408	.204	-.763	.406
does the organisation have measures and processes in place to measure organisational culture	141	1	5	3.30	1.171	-.319	.204	-.578	.406
does the organisation have multiple means for tracking increases in counterproductive workplace behaviour	141	1	5	2.92	1.128	-.057	.204	-.795	.406
does the organisation have principles, policies, and practices to help manage the risk of counterproductive behaviour in the workplace	141	1	5	3.07	1.113	-.205	.204	-.672	.406
does the management of the organisation integrate insider threat mitigation as part of the broader enterprise risk mitigation strategy	141	1	5	2.62	1.240	.240	.204	-.996	.406
is the organisation committed to the prevention, detection, deterrence, and response to insider threats	141	1	5	2.86	1.339	.046	.204	-1.193	.406

does the organisation assess level of employee engagement through annual surveys and/or pulse surveys	141	1	5	3.49	1.285	-.550	.204	-.737	.406
does the organisation actively assess job and organisational fit to ensure employee engagement	141	1	5	3.31	1.147	-.407	.204	-.471	.406
is the organisation constantly/regularly undergoing some level of significant organisational change	141	1	5	3.24	1.075	-.356	.204	-.364	.406
is the organisation structured to allow for open and efficient communication across all levels	141	1	5	3.33	1.053	-.518	.204	-.176	.406
are organisational policies ill-defined or loosely enforced	141	1	5	2.81	1.021	.067	.204	-.549	.406
does the organisation actively investigate reports of at-risk behaviours in a manner that does not deter future reports	141	1	5	2.94	1.094	-.019	.204	-.588	.406
do people in the organisation report suspicious behaviour in the workplace	141	1	5	3.11	1.119	-.244	.204	-.647	.406
does confidential reporting exist so that employees can report suspicious events without fear of repercussion	141	1	5	3.49	1.240	-.454	.204	-.726	.406
does the organisation have a whistle-blower protection policy	141	1	5	3.08	1.435	-.139	.204	-1.319	.406

does the organisation have policies that protect the security of organisational information and IT resources	141	1	5	3.96	1.176	-1.145	.204	.501	.406
does the organisation have implemented security practices to prevent unauthorised disclosure of sensitive information	141	1	5	3.94	1.160	-1.044	.204	.322	.406
does the organisation regularly review and update insider threat and security policy and procedures	141	1	5	2.94	1.305	-.096	.204	-1.097	.406
does the organisation have policy to conduct random reviews of exiting staff computer activities leading up the final date	141	1	5	2.72	1.267	.187	.204	-.963	.406
are policies and processes in place to ensure that the privileges and accesses of staff leaving the organisation are disabled	141	1	5	3.90	1.173	-1.179	.204	.694	.406
does the organisation require that all staff, contractors, consultants, and vendors sign non-disclosure statements when leaving the organisation	141	1	5	3.38	1.477	-.389	.204	-1.286	.406
does the organisation have policies protecting the physical security of facilities	141	1	5	4.03	1.201	-1.235	.204	.658	.406

does the organisation review physical access anomalies and denials	141	1	5	3.57	1.261	-.653	.204	-.608	.406
does the organisation capture information on an employee's physical movements within and around the organisations facility/ies	141	1	5	3.12	1.412	-.186	.204	-1.301	.406
the organisation keeps abreast of best practice when it comes to insider threat	141	1	5	2.89	1.243	-.076	.204	-1.001	.406
the organisation is good at addressing underlying systemic issues that may be linked to increased risk of insider threat	141	1	5	2.75	1.190	.107	.204	-.918	.406
the organisation is better equipped to cope with insider threat challenges when compared to other organisations in the same sector	141	1	5	2.95	1.155	-.241	.204	-.624	.406
the organisation is able to learn from failures and mistakes	141	1	5	3.39	1.151	-.582	.204	-.580	.406
the organisation is resilient	141	1	5	3.75	.919	-.828	.204	.637	.406
management in the organisation are accountable and responsible to others	141	1	5	3.60	1.082	-.577	.204	-.307	.406
management in the organisation lead by example when it comes to security practice	141	1	5	3.39	1.027	-.362	.204	-.358	.406

management in the organisation do not hesitate to provide the leadership that is needed	141	1	5	3.53	1.073	-.383	.204	-.525	.406
the organisation fosters an environment that is conducive to the success of insider threat initiatives	141	1	5	2.71	1.137	.268	.204	-.465	.406
the organisation has a poor security culture	141	1	5	2.34	.992	.341	.204	-.706	.406
the values of the organisation are made explicit and help to build a strong security culture	141	1	5	3.48	.990	-.491	.204	-.139	.406
management in the organisation provide the support and resources needed to help staff meet their goals	141	1	5	3.41	1.008	-.604	.204	-.101	.406
management in the organisation take care to be informed about how others think and feel about things	141	1	5	3.29	1.131	-.354	.204	-.817	.406
management in the organisation encourage staff to speak up about employee issues	141	1	5	3.40	1.159	-.420	.204	-.629	.406
that, overall, staff of the organisation engage in poor security behaviour	141	1	5	2.35	1.056	.521	.204	-.395	.406
staff in the organisation are treated fairly by management in the organisation	141	1	5	3.54	1.079	-.656	.204	-.113	.406

there is a perception in the organisation that management do not value staff	141	1	5	2.63	1.161	.120	.204	-1.173	.406
the organisation has a positive organisational culture	141	1	5	3.48	1.073	-.339	.204	-.604	.406
both overt and covert messages are corrected to create a positive organisational culture	141	1	5	3.26	1.003	-.059	.204	-.805	.406
the organisation regularly identifies and assesses its own organisational culture	141	1	5	3.39	1.054	-.392	.204	-.537	.406
there is an increasing level of counterproductive behaviour in the organisation	141	1	5	2.47	1.046	.143	.204	-1.010	.406
when it comes to insider threat the organisation is complacent	141	1	5	2.85	1.088	.099	.204	-.828	.406
the organisation is aware of its risk tolerance level/risk appetite	141	1	5	3.43	.904	-.363	.204	-.099	.406
staff of the organisation are aware of its critical assets that are worth protecting	141	1	5	3.70	.971	-.637	.204	-.174	.406
there is a lack of management of potential insider threat issues at the emerging stages	141	1	5	2.94	1.002	-.217	.204	-.502	.406
staff are aware of how insider threat concerns are managed in the organisation	141	1	5	2.74	1.078	.145	.204	-.809	.406

people in the organisation are willing to go above and beyond to achieve the organisations mission	141	1	5	3.76	.970	-.450	.204	-.114	.406
there is a high level of collegiality within the organisation	141	1	5	3.64	.951	-.481	.204	-.029	.406
the organisation increases its monitoring capabilities when significant organisational change occurs	141	1	5	3.04	1.017	.011	.204	-.559	.406
the organisation balances trust with the application of consistent employee monitoring	141	1	5	3.14	1.018	-.001	.204	-.579	.406
there is a high level of undue secrecy in the organisation	141	1	5	2.64	1.044	.199	.204	-.591	.406
the organisation is open and honest with its employees	141	1	5	3.32	1.098	-.367	.204	-.557	.406
management in the organisation encourage staff to participate in important decisions	141	1	5	3.35	1.057	-.163	.204	-.794	.406
policies and expectations are consistent across all levels of the organisation	141	1	5	3.21	1.092	-.085	.204	-.934	.406
security reporting is encouraged in the organisation	141	1	5	3.60	.999	-.571	.204	-.123	.406
staff are aware of the security controls utilised by the organisation	141	1	5	3.48	1.004	-.382	.204	-.396	.406

the organisation has a whistle-blower policy that has the confidence of all employees	141	1	5	3.01	1.159	-.056	.204	-.847	.406
the organisation has relevant IT policies and procedures	141	1	5	3.88	.982	-1.041	.204	1.072	.406
the organisation is committed to improving security in order to protect its information and resources	141	1	5	3.78	.879	-.642	.204	.161	.406
security controls of the organisation are adequate and applied whenever necessary	141	1	5	3.54	.953	-.516	.204	.043	.406
staff in the organisation can identify and report on red flags	141	1	5	3.46	.982	-.532	.204	-.126	.406
the organisation has a proactive and risk-based approach to mitigating emerging insider threats	141	1	5	3.04	1.101	-.215	.204	-.596	.406
security awareness is high among staff and considered in the daily activities of all organisational members	141	1	5	3.40	1.020	-.290	.204	-.437	.406
staff use relevant risk management and compliance considerations in everyday work decisions	141	1	5	3.55	.929	-.542	.204	.225	.406
staff in the organisation are vigilant and able to monitor emerging threats	141	1	5	3.28	.911	-.061	.204	-.253	.406

the organisation has strict exit controls in place for all exiting staff	141	1	5	3.52	1.112	-.598	.204	-.369	.406
TECH does the organisation allow staff a variety of virtual work arrangements (including working from home)	141	1	5	3.17	1.183	-.152	.204	-.836	.406
TECH does the organisation have guidelines to ensure that staff only have access to data, systems, and information required to perform their duties	141	1	5	3.82	1.030	-.949	.204	.664	.406
TECH does the organisation implement multi-factor authentication (e.g.- a password plus a one-time code from a hardware token)	141	1	5	3.40	1.127	-.365	.204	-.540	.406
TECH do authentication procedures become more advanced with increasing access to critical information/data	141	1	5	3.45	1.143	-.525	.204	-.461	.406
TECH is access to sensitive systems and areas enforced by authentication procedures monitored for anomalies	141	1	5	3.41	1.153	-.404	.204	-.477	.406
TECH does the organisation require multiple users to action all modifications to critical systems, network, applications, and data	141	1	5	3.30	1.067	-.264	.204	-.338	.406

TECH does the organisation restrict administrators from controlling auditing functions	141	1	5	3.33	1.072	-.297	.204	-.328	.406
TECH is routine auditing of privileged functions conducted by the organisation	141	1	5	3.38	1.086	-.321	.204	-.323	.406
TECH are advanced analytics tools used in the organisation to analyse and report on insider threat	141	1	5	2.87	1.188	.043	.204	-.846	.406
TECH is random auditing of IT use implemented	141	1	5	3.19	1.177	-.380	.204	-.617	.406
TECH is auditing part of performance reviews	141	1	5	2.70	1.235	.287	.204	-.847	.406
TECH does the organisation monitor common data exfiltration methods (e-mail, removable media) to identify anomalous behaviour	141	1	5	3.21	1.218	-.272	.204	-.790	.406
TECH is network traffic and associated security logs collected centrally and monitored for anomalies	141	1	5	3.24	1.218	-.330	.204	-.688	.406
TECH does the organisation monitor key databases, data access and movement	141	1	5	3.28	1.197	-.388	.204	-.573	.406

TECH does the organisation use modern technologies to assist insider threat detection, deterrence, prevention and reporting	141	1	5	3.04	1.186	-.043	.204	-.738	.406
TECH does the organisation have means to monitor trends in IT policy breaches to inform corrective action	141	1	5	3.26	1.199	-.345	.204	-.608	.406
TECH does the organisation maintain pace with current technology lifecycles, with an organisation wide refresh every 5 years or so	141	1	5	3.37	1.111	-.361	.204	-.633	.406
TECH does the organisation have back-up and recovery processes in place to avoid disruption	141	1	5	3.94	.977	-.865	.204	.459	.406
TECH does the organisation have restrictions on hardware usage such that potential threats to unauthorised data removal are disabled (such as disabling all USB ports)	141	1	5	3.35	1.326	-.398	.204	-.912	.406
TECH does the organisation allows its staff to use their own devices for work (BYOD)	141	1	5	2.85	1.287	.058	.204	-1.146	.406
TECH does the organisation use regular penetration testing to strengthen defences	141	1	5	3.10	1.197	-.118	.204	-.723	.406

TECH does the organisation hire technically sophisticated system administrators or programmers	141	1	5	3.45	1.130	-.408	.204	-.596	.406
TECH do managers of IT/cyber employees have management training to improve their management of people not just technology	141	1	5	3.01	1.146	-.086	.204	-.713	.406
TECH does the organisation have a clear list of access privileges for all roles	141	1	6	4.23	1.311	-.545	.204	-.243	.406
TECH does the organisation review access request denials	141	1	6	4.11	1.661	-.392	.204	-1.005	.406
TECH does computing equipment connected to the corporate network of the organisation reside in an area that has electronic access controls in place (i.e.- requires a swipe card to access)	141	1	6	3.98	1.466	-.611	.204	-.623	.406
TECH are special authentication procedures employed for database administrators	141	1	6	4.29	1.457	-.618	.204	-.449	.406
Valid N (listwise)	37								

Appendix M – Inventory Percentages

INVENTORY QUESTION	Median	Never	Rarely	Occasionally	Often	Always	Don't Know/Not Applicable
I1. does the organisation check civil records	4.00	15.6	12.8	17.7	25.5	28.4	
I2. does the organisation have methods to assess sound and reliable behaviour of staff	4.00	7.8	12.8	22.7	37.6	19.1	
I3. does the organisation have policy and processes to manage staff with a history of security violations	4.00	22.7	12.1	13.5	24.8	27.0	
I4. does the organisation test for illegal drug use	2.00	45.4	14.2	9.9	17.0	13.5	
I5. does the organisation assess past substance use/abuse	2.00	44.0	14.2	10.6	9.9	21.3	
I6. does the organisation assess for problematic gambling behaviour	2.00	46.8	12.8	11.3	10.6	18.4	
I7. does the organisation have a good conduct policy	4.00	8.5	3.5	12.8	34.0	41.1	
I8. does the organisation assess financial, credit, and bankruptcy history	2.00	44.0	9.9	9.2	12.8	24.1	
I9. does the organisation have methods to identify financial pressures of employees	2.00	41.8	13.5	17.0	17.0	10.6	
I10. does the organisation undertake a formal risk assessment of high risk employees/positions	3.00	29.1	15.6	19.9	17.7	17.7	
I11. does the organisation have a means by which employees can report suspicious contacts from other employees or outsiders	4.00	7.8	11.3	21.3	20.6	39.0	
I12. does the organisation allow the hiring of employees with close connections to current staff (friends/family)	3.00	7.1	9.2	36.9	26.2	20.6	
I13. does the organisation assess for positive support networks of employees	3.00	18.4	22.0	22.7	23.4	13.5	
I14. does the organisation evaluate risk-related criminal associations	3.00	31.2	10.6	14.2	14.2	29.8	
I15. does the organisation check criminal records	5.00	13.5	10.6	9.2	13.5	53.2	
I16. does the organisation identify employees susceptible to social engineering (manipulation of people to get them to perform actions that do harm)	2.00	37.6	17.0	18.4	14.9	12.1	
I17. does the organisation monitor foreign contacts of staff	2.00	40.4	18.4	11.3	17.0	12.8	
I18. does the organisation monitor staff travel	3.00	24.1	17.0	10.6	23.4	24.8	
I19. does the organisation have clear procedures describing access to and benefits of employee assistance programs and other employee support services	4.00	8.5	11.3	17.7	24.8	37.6	
I20. does the organisation monitor/assess staff after negative/stressful events	4.00	9.2	12.8	26.2	29.1	22.7	
I21. does the organisation conduct performance reviews and is therefore aware of declining performance ratings	4.00	4.3	7.1	17.0	29.8	41.8	
I22. does the organisation have processes in place to monitor at-risk employees after negative workplace events	3.00	10.6	14.9	34.8	21.3	18.4	
I23. does the organisation have branches, suppliers, subcontractors or other affiliates where differences in cultural beliefs and values may affect loyalty to the organisation	2.00	22.0	28.4	24.8	14.9	9.9	
I24. does the organisation have policies and procedures designed to improve loyalty	3.00	16.3	25.5	22.7	23.4	12.1	
I25.does the organisation have policy and processes which promote individual differences (gender, culture, ethnicity)	4.00	7.1	13.5	23.4	27.7	28.4	
I26. does the organisation educate staff on the different reasons behind insider threat actions	2.00	27.7	24.1	27.0	14.2	7.1	
I27. does the organisation assess motivation for employment during recruitment processes	4.00	6.4	14.9	18.4	29.8	30.5	
I28. does the organisations structure allow for specific individuals to control majority of the power	3.00	9.2	24.8	24.8	26.2	14.9	
I29. does the organisation assist staff/individuals to improve their communication	3.00	5.0	19.1	41.8	19.9	14.2	
I30. does the organisation use methods to assess alignment between employee values and organisational values	3.00	12.8	19.9	28.4	22.0	17.0	
I31. does the organisation utilise methods during recruitment processes to assess for ego/sense of entitlement	3.00	13.5	24.1	16.3	24.8	21.3	

I32. does the organisation utilise methods to assess for employee resilience	3.00	12.8	19.1	24.8	24.1	19.1	
I33. does the organisation offer resilience training to staff	3.00	12.8	23.4	42.6	12.1	9.2	
I34. does the organisation utilise methods to assess for employee sound judgment	3.00	12.8	19.1	31.9	23.4	12.8	
I35. does the organisation utilise methods to assess for employee conscientiousness	3.00	14.2	13.5	28.4	27.7	16.3	
I36. does the organisation conduct mental health testing/assessment	2.00	31.2	22.7	17.0	15.6	13.5	
I37. does the organisation conduct personality testing to determine an employee's vulnerability to become an insider threat	2.00	34.0	20.6	11.3	13.5	20.6	
I38. does the organisation employ trained professionals to identify and manage employees vulnerable to becoming an insider threat	2.00	36.9	24.1	12.1	12.1	14.9	
I39. does the organisation utilise methods to assess for employee self-awareness	3.00	22.0	20.6	23.4	20.6	13.5	
I40. does the organisation have programs to develop employee self-awareness	3.00	21.3	26.2	28.4	19.1	5.0	
I41. does the organisation have mechanisms in place in order to know of any pending sanctions of contractors and outside staff	4.00	18.4	16.3	12.8	6.4	10.6	35.5
I42. does the organisation carefully consider any vendors/partnerships etc. based on ethical conduct	4.00	9.2	15.6	17.7	18.4	15.6	23.4
I43. does the organisation assess moral development	3.00	23.4	19.1	10.6	12.8	9.9	24.1
		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	
I44. the organisation has methods to assess for addictions	3.00	19.9	28.4	16.3	29.8	5.7	
I45. workplace deviance is handled appropriately within the organisation	3.00	6.4	27.7	22.7	36.2	7.1	
I46. the organisation has methods for identifying and managing potential disgruntlement	3.00	6.4	20.6	24.8	43.3	5.0	
I47. the organisation actively manages employee expectation	3.00	5.0	25.5	33.3	30.5	5.7	
I49. commitment to the organisation is high amongst staff	4.00	4.3	12.8	24.1	44.0	14.9	
I50. the attitude of staff is a problem in the organisation	2.00	17.0	38.3	17.7	24.8	2.1	
I51. positive individual attitudes are nurtured by the organisation	4.00	4.3	16.3	26.2	41.1	12.1	
I52. the practices and policies of the organisation allows for individual specific agendas	3.00	7.8	23.4	35.5	27.7	5.7	
I53. the organisation suffers from poor politics	3.00	15.6	29.8	19.1	26.2	9.2	
I54. the organisation has a problem with individual communication	3.00	12.8	29.8	24.1	25.5	7.8	
I55. people in the organisation maintain high ethical standards	4.00	1.4	8.5	22.0	48.9	19.1	
I56. people in the organisation demonstrate high integrity & honesty	4.00	1.4	10.6	22.0	44.7	21.3	

INVENTORY QUESTION	Median	Never	Rarely	Occasionally	Often	Always
O1. does the organisation offer specific training and education programs addressing policy and practice areas relevant to insider threat	2.00	27.7	23.4	22.7	20.6	5.7
O2. does the organisation structure security awareness training and education efforts appropriately to the needs of different employees groups	3.00	22.0	22.0	25.5	24.1	6.4
O3. does the organisation subject all staff (including vendor staff, contractors, and outsourced roles) to vetting processes relevant to their level of access/role	4.00	12.1	17.7	12.1	22.7	35.5
O4. does the organisation have a specialised and multidisciplinary team to evaluate the risk of insider threat	3.00	34.8	14.9	18.4	19.9	12.1
O5. does the organisation utilise a variety of informal and formal staff consultation methods to understand staff views/opinions	3.00	8.5	9.2	40.4	31.9	9.9
O6. does the organisation have guidelines describing the organisation's right to monitor and audit employee activity including their behaviour	4.00	16.3	11.3	21.3	31.2	19.9
O7. does the organisation conduct informal online searches of employees	3.00	20.6	24.1	31.9	14.9	8.5
O8. does the organisation utilise evidence-based recruitment and assessment methods	4.00	10.6	9.9	18.4	42.6	18.4
O9. does the organisation conduct its own research on insider threat	3.00	17.7	19.1	24.1	27.0	12.1
O10. does the organisation benchmark its processes and controls (technical and non-technical) against leading practices	2.00	36.9	18.4	25.5	14.2	5.0
O11. does the organisation have policies and processes to attempt to identify moles	2.00	41.1	18.4	23.4	9.9	7.1
O12. does the organisation promote integrated approaches to insider threat management	2.00	34.0	27.0	24.1	9.9	5.0
O13. does the organisation have a senior management position dedicated to security who answers to a Board member	3.00	34.0	10.6	10.6	27.7	17.0
O14. does the organisation have an established insider threat contingency management plan	2.00	33.3	20.6	17.7	19.9	8.5
O15. does the organisation utilise risk transfer methods (insurance, contracts, etc.) as part of the organisation's risk management	3.00	14.9	18.4	27.0	26.2	13.5
O16. does the organisation ensure management security actions are recorded and subsequently evaluated for effectiveness	3.00	16.3	18.4	31.2	23.4	10.6
O17. does the organisation have strong and positive leadership	4.00	5.7	9.9	28.4	39.0	17.0
O18. does management in the organisation communicate clear plans & objectives for the organisation	4.00	7.1	12.1	23.4	40.4	17.0
O19. does the organisation regularly use methods to identify and assess its own security culture	3.00	15.6	20.6	30.5	25.5	7.8
O20. does the organisation have publicly available methods for investigating and penalising inappropriate security behaviour	3.00	19.1	24.1	22.0	23.4	11.3
O21. does the organisation track security compliance and take steps to confirm compliance	3.00	13.5	13.5	26.2	34.8	12.1
O22. does the organisation have measures and processes in place to measure organisational culture	3.00	9.2	12.8	33.3	27.7	17.0
O23. does the organisation have multiple means for tracking increases in counterproductive workplace behaviour	3.00	12.1	24.1	30.5	26.2	7.1
O24. does the organisation have principles, policies, and practices to help manage the risk of counterproductive behaviour in the workplace	3.00	9.9	19.9	31.9	29.8	8.5
O25. does the organisation management integrate insider threat mitigation as part of the broader enterprise risk mitigation strategy	3.00	23.4	25.5	24.1	19.9	7.1
O26. does the organisation commit to the prevention, detection, deterrence, and response to insider threats	3.00	21.3	20.6	22.0	23.4	12.8
O27. does the organisation assess level of employee engagement through annual surveys and/or pulse surveys	4.00	10.6	12.1	20.6	31.2	25.5
O28. does the organisation actively assess job and organisational fit to ensure employee engagement	3.00	9.2	12.1	31.9	31.9	14.9
O29. does the organisation constantly/regularly undergo some level of significant organisational change	3.00	7.8	14.2	34.8	32.6	10.6
O30. does the organisation structure allow for open and efficient communication across all levels	3.00	7.1	12.1	31.9	38.3	10.6
O31. does the organisation have ill-defined or loosely enforced policies	3.00	9.9	29.1	35.5	21.3	4.3
O32. does the organisation actively investigate reports of at-risk behaviours in a manner that does not deter future reports	3.00	10.6	22.7	36.2	22.7	7.8
O33. does the organisation have people in the organisation report suspicious behaviour in the workplace	3.00	9.9	18.4	31.9	30.5	9.2
O34. does the organisation have confidential reporting so that employees can report suspicious events without fear of repercussion	4.00	8.5	12.8	25.5	27.7	25.5
O35. does the organisation have a whistle-blower protection policy	3.00	20.6	16.3	18.4	24.1	20.6
O36. does the organisation have policies that protect the security of organisational information and IT resources	4.00	6.4	7.1	11.3	34.8	40.4

O37. does the organisation implement security practices to prevent unauthorised disclosure of sensitive information	4.00	5.7	7.1	14.9	32.6	39.7
O38. does the organisation regularly review and update insider threat and security policy and procedures	3.00	19.9	16.3	26.2	25.5	12.1
O39. does the organisation have policy to conduct random reviews of exiting staff computer activities leading up the final date	3.00	22.0	22.0	28.4	17.7	9.9
O40. are policies and processes in place to ensure that the privileges and accesses of staff leaving the organisation are disabled	4.00	7.8	5.0	12.1	39.7	35.5
O41. does the organisation require that all staff, contractors, consultants, and vendors sign non-disclosure statements when leaving the organisation	4.00	16.3	15.6	13.5	22.7	31.9
O42. does the organisation have policies protecting the physical security of facilities	4.00	7.1	5.0	12.8	28.4	46.8
O43. does the organisation review physical access anomalies and denials	4.00	9.2	12.8	16.3	35.5	26.2
O44. does the organisation capture information on an employee's physical movements within and around the organisations facility/ies	3.00	18.4	18.4	15.6	27.7	19.9
		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
O45. the organisation keeps abreast of best practice when it comes to insider threat	3.00	18.4	18.4	28.4	25.5	9.2
O46. the organisation is good at addressing underlying systemic issues that may be linked to increased risk of insider threat	3.00	17.7	25.5	27.7	22.0	7.1
O47. the organisation is better equipped to cope with insider threat challenges when compared to other organisations in the same sector	3.00	16.3	12.1	39.7	24.1	7.8
O48. the organisation is able to learn from failures and mistakes	4.00	7.8	17.0	17.0	44.7	13.5
O49. the organisation is resilient	4.00	2.1	8.5	19.1	52.5	17.7
O50. management in the organisation are accountable and responsible to others	4.00	4.3	12.8	22.7	39.7	20.6
O51. management in the organisation lead by example when it comes to security practice	3.00	4.3	14.9	31.2	36.9	12.8
O52. management in the organisation do not hesitate to provide the leadership that is needed	4.00	3.5	14.2	27.7	34.8	19.9
O53. the organisation fosters an environment that is conducive to the success of insider threat initiatives	3.00	16.3	25.5	37.6	12.1	8.5
O54. the organisation has a poor security culture	2.00	21.3	39.0	24.8	14.2	0.7
O55. the values of the organisation are made explicit and help to build a strong security culture	4.00	3.5	12.8	29.1	41.8	12.8
O56. management in the organisation provide the support and resources needed to help staff meet their goals	4.00	5.0	13.5	27.0	44.7	9.9
O57. management in the organisation take care to be informed about how others think and feel about things	4.00	6.4	22.0	19.9	39.7	12.1
O58. management in the organisation encourage staff to speak up about employee issues	4.00	7.1	15.6	24.8	34.8	17.7
O59. that, overall, staff of the organisation engage in poor security behaviour	2.00	22.7	38.3	23.4	12.8	2.8
O60. staff in the organisation are treated fairly by management in the organisation	4.00	5.7	11.3	23.4	42.6	17.0
O61. there is a perception in the organisation that management do not value staff	2.00	19.1	31.9	18.4	27.7	2.8
O62. the organisation has a positive organisational culture	4.00	3.5	16.3	27.0	35.5	17.7
O63. both overt and covert messages are corrected to create a positive organisational culture	3.00	2.1	24.1	29.8	34.0	9.9
O64. the organisation regularly identifies and assesses its own organisational culture	4.00	4.3	17.7	25.5	39.7	12.8
O65. there is an increasing level of counterproductive behaviour in the organisation	2.00	20.6	32.6	27.0	19.1	0.7
O66. when it comes to insider threat the organisation is complacent	3.00	9.9	31.9	27.0	25.5	5.7
O67. the organisation is aware of its risk tolerance level/risk appetite	4.00	2.1	12.8	34.8	41.1	9.2
O68. staff of the organisation are aware of its critical assets that are worth protecting	4.00	1.4	13.5	17.7	48.9	18.4
O69. there is a lack of management of insider threat issues at the emerging stages	3.00	9.2	22.0	38.3	27.0	3.5
O70. staff are aware of how insider threat concerns are managed in the organisation	3.00	12.1	33.3	27.0	23.4	4.3
O71. people in the organisation are willing to go above and beyond to achieve the organisation's mission	4.00	2.1	5.7	31.9	34.8	25.5
O72. there is a high level of collegiality within the organisation	4.00	2.1	9.2	29.1	41.8	17.7
O73. the organisation increases its monitoring capabilities when significant organisational change occurs	3.00	5.7	25.5	35.5	26.2	7.1
O74. the organisation balances trust with the application of consistent employee monitoring	3.00	4.3	23.4	35.5	27.7	9.2

O75. there is a high level of undue secrecy in the organisation	3.00	14.2	32.6	31.9	17.7	3.5
O76. the organisation is open and honest with its employees	3.00	6.4	17.0	27.7	36.2	12.8
O77. management in the organisation encourage staff to participate in important decisions	3.00	2.8	21.3	27.7	34.0	14.2
O78. policies and expectations are consistent across all levels of the organisation	3.00	4.3	27.0	24.1	33.3	11.3
O79. security reporting is encouraged in the organisation	4.00	2.8	12.1	24.1	44.0	17.0
O80. staff are aware of the security controls utilised by the organisation	4.00	2.8	14.9	28.4	39.7	14.2
O81. the organisation has a whistle-blower policy that has the confidence of all staff	3.00	10.6	24.1	28.4	27.0	9.9
O82. the organisation has relevant IT policies and procedures	4.00	3.5	5.7	16.3	48.2	26.2
O83. the organisation is committed to improving security in order to protect its information and resources	4.00	0.7	9.2	19.9	51.8	18.4
O84. security controls of the organisation are adequate and applied whenever necessary	4.00	2.8	10.6	29.8	43.3	13.5
O85. staff in the organisation can identify and report on red flags	4.00	3.5	13.5	27.7	44.0	11.3
O86. the organisation has a proactive and risk-based approach to mitigating emerging insider threats	3.00	10.6	18.4	34.8	28.4	7.8
O87. security awareness is high among staff	3.00	3.5	15.6	31.9	35.5	13.5
O88. staff use relevant risk management and compliance considerations in everyday work decisions	4.00	2.8	9.2	31.2	44.0	12.8
O89. staff in the organisation are vigilant and able to monitor emerging threats	3.00	2.1	16.3	41.8	31.2	8.5
O90. the organisation has strict exit controls in place for all exiting staff	4.00	5.7	14.2	20.6	41.8	17.7

INVENTORY QUESTION	Median	Never	Rarely	Occasionally	Often	Always	Don't Know/Not Applicable
T1. does the organisation allow staff a variety of virtual work arrangements (including working from home)	3.00	9.2	20.6	28.4	27.7	14.2	
T2. does the organisation have guidelines to ensure that staff only have access to data, systems, and information required to perform their duties	4.00	4.3	6.4	18.4	44.7	26.2	
T3. does the organisation implement multi-factor authentication	3.00	6.4	14.2	29.8	31.9	17.7	
T4. does the organisation ensure authentication procedures become more advanced with increasing access to critical information/data	4.00	7.1	13.5	24.1	37.6	17.7	
T5. does the organisation ensure access to sensitive systems and areas enforced by authentication procedures are monitored for anomalies	3.00	7.8	11.3	31.9	29.8	19.1	
T6. does the organisation require multiple users to action all modifications to critical systems, network, applications, and data	3.00	6.4	13.5	37.6	29.1	13.5	
T7. does the organisation restrict administrators from controlling auditing functions	3.00	6.4	12.8	36.9	29.8	14.2	
T8. does the organisation conduct routine auditing of privileged functions	3.00	6.4	11.3	36.9	29.1	16.3	
T9. does the organisation use advanced analytics tools to analyse and report on insider threat	3.00	14.9	23.4	30.5	22.0	9.2	
T10. does the organisation implement random auditing of IT use implemented	3.00	12.1	12.8	31.2	31.9	12.1	
T11. does the organisation conduct auditing part of performance reviews	3.00	19.1	27.7	27.0	16.3	9.9	
T12. does the organisation monitor common data exfiltration methods (e-mail, removable media) to identify anomalous behaviour	3.00	11.3	15.6	29.1	28.4	15.6	
T13. does the organisation collect and monitor network traffic and security logs for anomalies	3.00	12.1	12.1	31.9	27.7	16.3	
T14. does the organisation monitor key databases, data access and movement	3.00	11.3	10.6	32.6	29.1	16.3	
T15. does the organisation use modern technologies to assist insider threat detection, deterrence, prevention and reporting	3.00	12.1	19.1	34.8	21.3	12.8	
T16. does the organisation have means to monitor trends in IT policy breaches to inform corrective action	3.00	11.3	11.3	33.3	27.7	16.3	
T17. does the organisation maintain pace with current technology lifecycles (organisation wide refresh every 5 years or so)	4.00	5.7	17.7	25.5	36.2	14.9	
T18. does the organisation have back-up and recovery processes in place to avoid disruption	4.00	2.1	6.4	18.4	41.1	31.9	
T19. does the organisation have restrictions on hardware usage such that potential threats to unauthorised data removal are disabled (such as disabling all USB ports)	3.00	13.5	11.3	25.5	25.5	24.1	
T20. does the organisation allows its staff to use their own devices for work (BYOD)	3.00	18.4	24.8	20.6	25.5	10.6	
T21. does the organisation use regular penetration testing to strengthen defences	3.00	12.1	16.3	35.5	22.0	14.2	
T22. does the organisation hire technically sophisticated system administrators or programmers	4.00	5.7	15.6	25.5	34.8	18.4	
T23. does the organisation ensure managers of IT/cyber employees have management training to improve their management of people not just technology	3.00	11.3	20.6	33.3	24.8	9.9	
T24. does the organisation have a clear list of access privileges for all roles	4.00	3.5	7.8	14.2	29.1	27.7	17.7
T25. does the organisation review access request denials	4.00	9.2	9.9	15.6	22.0	12.1	31.2

T26. does the organisation ensure computing equipment connected to the corporate network of the organisation reside in an area that has electronic access controls in place (i.e.- requires a swipe card to access)	4.00	8.5	10.6	13.5	20.6	35.5	11.3
T27. does the organisation employ special authentication procedures employed for database administrators	5.00	5.7	7.1	14.9	22.0	25.5	24.8