2015

An analysis of insider dysfunctional behavours in an accounting information system environment

Mohd Saiyidi Mat Roni
Edith Cowan University

2015

An analysis of insider dysfunctional behavours in an accounting information system environment

Mohd Saiyidi Mat Roni
Edith Cowan University

Edith Cowan University

Copyright Warning

An Analysis of Insider Dysfunctional Behaviours in an Accounting Information System Environment

Mohd Saiyidi Mokhtar Mat Roni

A thesis submitted in fulfilment of the requirement for the degree of
Doctor of Philosophy

School of Business
Faculty of Business and Law
Edith Cowan University
Perth, Western Australia

2015

An Analysis of
Insider Dysfunctional Behaviours
in an Accounting Information System Environment

School of Business
Faculty of Business and Law
Edith Cowan University
Perth, Western Australia

Principal Supervisor : Assoc. Prof. Dr Hadrian Djajadikerta

Co-Supervisor : Prof. Craig Standing

2015

USE OF THESIS

The Use of Thesis statement is not included in this version of the thesis.

Abstract

Insider deviant behaviour in Accounting Information Systems (AIS) has long been recognised as a threat to organisational AIS assets. The literature abounds with a plethora of perspectives in attempts to better understand the phenomenon, however, practitioners and researchers have traditionally focussed on technical approaches, which, although they form part of the solution, are insufficient to address the problem holistically. Managing insider threats requires an understanding of the interconnectedness between the human and contextual factors in which individuals operate, since technical methodologies in isolation have the potential to increase rather than reduce insider threats. This dilemma led many scholars to examine the behaviour of individuals, to further their understanding of the issues and in turn, control insider threats. Despite promising findings, some of these behavioural studies have inherent methodological limitations, and no attempt has been made to differentiate between apparently similar, yet fundamentally different, negative behaviours.

Using the theory of planned behaviour (TPB) and actor network theory (ANT) as a foundation, the current study addresses the first concern by integrating AIS complexity and organisational culture, and identifies the contextual factors influencing behaviours that lead to insider threats. Secondly, the study addresses concerns regarding methodological approaches, by categorising various deviant insider behaviours using the concept of *dysfunctional behaviour,* based on two-dimensional behaviour taxonomy.

Partial least square structural equation modelling (PLS-SEM) revealed that TPB's predictor variables: attitude (ATT), subjective norm (SN) and perceived behavioural control (PBC), together with the moderator variables of organisational culture (CULTURE) and AIS complexity (COMPLEX), accounted for substantial

variations in intention (INTENT) to engage in dysfunctional behaviour. The findings also indicated that PBC is a dual-factor construct. Changes in predictors at the behavioural subset level were highlighted, and the findings of previous studies, that ATT is a salient predictor of intention, were confirmed. This was significant across all four dysfunctional behaviour categories.

These findings add to the body of knowledge by contributing a theory that explains insider threats in AIS by deciphering dysfunctional behaviour using a predictive model. The study also provides a methodological foundation for future research to account for behavioural factors. Moreover, the findings have implications for managerial practices who want to reduce insider threats to an acceptable level by strengthening organisational culture, moderating AIS complexity, and focussing on management programs with sufficient momentum to impact attitudinal change.

Declaration

I certify that this thesis does not, to the best of my knowledge or belief:

i. Incorporate without acknowledgement any material previously submitted for a degree or diploma in any institution of higher education;

ii. Contain any material previously published or written by another person except where due reference is made in text; or

iii. Contain any defamatory material.

I also grant permission for the Library at Edith Cowan University to make duplicate copies of my thesis as required.

Date 21 June 2015

Acknowledgements

I would like to express my deepest gratitude and appreciation to my supervisors, Associate Professor Hadrian Djajadikerta and Professor Craig Standing, for their invaluable personal and professional guidance. Their wealth of knowledge, advice, and encouragement has made my doctoral endeavour possible.

My special thanks to Professor Malcolm Smith at the University of South Australia for his scholarly insights that paved the way for this journey; and Professor Dr Mizan Hitam of International Islamic University, Malaysia, for his professional advice and encouragement to keep up the momentum to conclude my doctoral journey.

I am also thankful for the help offered by the staff of the School of Business at Edith Cowan University, in particular Bev Lurie; and the wonderful team at the Graduate Research School for their assistance. My appreciation also goes to many of my friends and colleagues, in particular Azmi Nias Ahmad and Sharon Shan, for their valuable input and help.

Above all I would like to express my gratitude to my wife, Izariani Ismail, for the sacrifices made and support offered; to my children, Sofea Izyani, Syariq Iman, and my two little twins, Sasha and Sarra, who always cheer me up.

Finally, I would like to extend my gratitude to my employer and sponsor for the funding provided throughout my studies.

Table of Contents

List of Tables

List of Figures

Abbreviations

AFVIF:	Average full variance inflation factor
AIS:	Accounting information system
ANT:	Actor network theory
ATT:	Attitude
AVE:	Average variance extracted
AVIF:	Average variance inflation factor
COMPLEX:	Accounting information system complexity
COSO:	Committee of Sponsoring Organizations of the Treadway Commission
CULTURE:	Organisational culture
EAS:	Events accounting system
EPOS:	Electronic point of sales
IDS:	Intrusion detection system
IS:	Information system
ISO:	International organisation for standardisation
IT:	Information technology
PBC:	Perceived behavioural control
PBC-Out:	Perceived behavioural control over outcomes
PBC-Res:	Perceived behavioural control over resources
POS:	Point of sales
REA:	Resource event agent
SN:	Subjective norm
TPB:	Theory of Planned Behaviour
VIF:	Variance inflation factor
WLS:	Weight loading sign

Publications

Journals

- Djajadikerta, H., & Mat Roni, S. All dysfunctional behaviours are not created the same: Challenges to the generalisability of security-based research. *Information & Management*. (Journal ranking: ABDC A*-ranked. Status of article: Under second review).

Conferences

- Mat Roni, S., Djajadikerta, H., & Nias Ahmad, M. A. (2014). *Insider misbehaviour: How system complexity and organisational culture affect AIS misuse.* Paper presented at the Regional Conference on Science, Technology and Social Sciences, Cameron Highland, Malaysia.

- Mat Roni, S., Smith, M., & Djajadikerta, H. (2013). *Insider dysfunctional behaviour: Culturally cultivated from within*. Paper presented at the International Conference on Governance, Management & Financial Criminology, University of Waikato, Hamilton, New Zealand.

Chapter One
Introduction

1.1 Introduction

An Accounting Information System (AIS) extends beyond the realms of a financial data process. It is a discipline with a shared identity; either as a subset within Information Systems (IS) or as an accounting tool because of the dominant role of IS and its pervasiveness in the field of accounting (Granlund, 2011; Ismail, 2009; Poston & Grabski, 2000; Sutton, 2006, 2010a; Vaassen & Hunton, 2009). This is due to AIS having originated from parent disciplines of IS and accounting (Gray, Chiu, Liu, & Li, 2014; Poston & Grabski, 2000; Sutton, 2000, 2004b, 2010b).

Earlier studies indicated that threats to AIS were largely attributed to technical breakdowns requiring software patches, updates and technical controls (Calderon, Chandra, & Cheh, 2006; Gaston, 2006); or financial anomalies, necessitating improved accounting procedures (Boritz, 2005; Burchell, Clubb, Hopwood, Hughes, & Nahapiet, 1980; Granlund, 2011; Neu, Everett, Rahaman, & Martinez, 2012). Either way, the interconnecting elements bridging the two disciplines have been inadvertently ignored, and efforts to address threats caused by flawed control of AIS and its environment have been inadequate to address the issues holistically.

At present, data in modern AIS are conditioned through a *resources-events-agents* (REA) model in both financial and non-financial forms. The REA model presents a significant departure from the traditional debit-credit concept. It is on this model that many enterprise systems rely (Worrell, Wasko, & Johnston, 2011; Yeow & Faraj, 2011) to capture meta-information for guiding sound managerial and

strategic decisions and operational controls (Markus & Pfeffer, 1983; Ramadhan, Joshi, & Hameed, 2003).

Modern AIS is largely influenced by REA, where the data originates from a variety of sources, and is transmitted, processed, stored and retrieved by means of numerous interconnected systems and sub-systems (Sutton, 2006, 2010a). This complex bond has numerous vulnerabilities (Ramadhan, et al., 2003) which affect data security and consequently, data integrity (Li, Peters, Richardson, & Watson, 2012). Each stage that the data travels or resides poses a risk of compromise, yet despite numerous calls for deeper examination of internal practices (Doherty, Anastasakis, & Fulford, 2011; Kraemer, Carayon, & Clem, 2009; Spears & Barki, 2010; Williams, 2008), the emphasis of data security and integrity has been on defending against external threats (e.g. in Almalawi, Yu, Tari, Fahad, & Khalil, 2014; Calderon, et al., 2006; Shameli-Sendi, Cheriet, & Hamou-Lhadj, 2014). This study considers the risks posed by both internal and external factors.

The demand for further study of precarious practices in the AIS environment has been motivated in part by the premise that insiders pose greater threats than outsiders (D'Arcy, Hovav, & Galletta, 2009; Doherty, et al., 2011; Furnell & Phyo, 2003). Addressing internal security concerns with external solutions further complicates and obscures the real issues rather than solving them. For this reason, it is critical to examine these phenomena in the context of a thorough understanding of negative behaviours and their potential application to other accounting-related disciplines, in order to reduce and eradicate insider dysfunction.

1.2 Threats to Accounting Information Systems

Despite the challenges of defining AIS, there is general agreement that it includes sources of data, systems and subsystems, which are primarily used to capture economic events. Ismail (2009) contended that there was a paradigm shift in AIS with the emergence of the *events accounting system* (EAS) in 1969 (Lieberman & Whinston, 1975; Sorter, 1969), which was later refined into the *resources-events-agents* concept in information management in 1982 (McCarthy, 1982). In the latter case the discipline was no longer limited to transaction processing, but also encapsulated future economic events (Abernethy & Guthrie, 1994; O'Leary, 2010).

In a similar vein, Benita (2003), Geerts and McCarthy (2002) argued that AIS, with its stringent adherence to principles of debit and credit, is unlikely to adequately (Benita, 2003; Geerts & McCarthy, 2002) address the fast-changing needs (Vasarhelyi & Alles, 2008) of both financial and non-financial information (Dillard & Yuthas, 2006).

Consequently, advancements in IS have caused AIS to evolve dynamically and move into a new paradigm. Although the situation appears straightforward, there is a gap in theoretical knowledge about the new model, as is true of all emerging technologies, where such a paradigm shift presents both opportunities and challenges that require thorough research (Sutton & Arnold, 2011; Worrell, et al., 2011; Yeow & Faraj, 2011). Among the many challenges that have surfaced are undesirable behaviours propagated within organisations by insiders, which lead to data security breaches, and ultimately, losses of all kinds.

In 2006, a team from the Internal Revenue Service in the United States reported a chain of restaurants in Detroit, called La Shish, who had skimmed off more than USD20 million over a four-year period (Furchgott, 2008). The scheme

was executed with the assistance of automated sales-suppression software installed at the restaurants' point of sales (POS) systems. The New York Times reported that the software, also named *zapper*, was being used in Germany, Sweden, Brazil, France, the Netherlands and Australia.

More recently, in March 2011, Albert Gonzalez was sentenced to two concurrent 20-year jail terms for his role in data security breaches (Richardson, 2011). Between 2005 and 2007 Gonzalez sold more than 170 million credit- and ATM-card information that he had stolen from several companies, including the famous Heartland Payment Systems. What is more intriguing is that Gonzalez's primary unauthorised access to the companies' systems was a simple *structure query language (SQL)* injection method.

These cases illustrate different dysfunctional behaviours by two distinct perpetrators: an insider in the former and an outsider in the latter. However, in both cases, the point of entry was a subsystem of the accounting information system.

Various feeder systems and subsystems of the AIS financial data processing core pose a risk of exposure to dysfunctional behaviour by insiders. In the La Shish case, the POS system, where sales data from checkout counters was fed to the main financial data processing nucleus, small zapper software that fits into a USB flash drive was installed by an insider to siphon transactions that met pre-determined criteria. Hence, flawed data, stemming from its origin, was wired and processed by the core processor giving misleading financial outputs.

The risk of a data security breach is not limited to POS systems. Of major concern is the possible security breach of non-financial data stored in numerous corporate servers. In 2010, an alarming 98 per cent of reported data loss was

identified as missing from servers (Baker et al., 2011). Although the loss of non-financial data is difficult to quantify, such losses are significant and likely to induce panic. This realisation has led investors to exercise extreme caution with regard to IT operations (Benaroch, Chernobai, & Goldstein, 2012), even when the risk of a breach is unlikely to materialise. A study by Gatzlaff and McCullough (2010), where significantly negative market reaction was experienced after customers' data were compromised, is one such example. The authors also observed that the negative reaction was stronger towards companies with high growth opportunity. Furthermore, the study revealed that the market tends to react more negatively when companies refuse to provide details of the security breach for fear of a huge monetary loss (Gatzlaff & McCullough, 2010).

Fear of a huge monetary loss resulting from security breaches of data stored in a corporate server was also illustrated in the case of TJ Maxx[1]. Prior to Gonzalez's arrest, a customer's data breach of TJ Maxx incurred the company an estimated USD256 million in costs relating to customer notifications, credit monitoring and court settlements (Kerber, 2007). The negative reaction of the market towards non-financial data security breaches is therefore an indication of the value of the data, which are mainly collected via AIS subsystems.

Although the TJ Maxx case was perpetrated by an external party, Lynch (2006) suggested that more than 50% of data security breaches were attributable to insiders. In contrast to several surveys where insider security malpractices were

[1] TJ Maxx is one of the victimised companies whose customers' data was compromised by Gonzalez. At the time when the company announced the data security breach, it was not clear whether all of the compromised data was attributable to an attack by Gonzalez.

perceived to occur less frequently (Baker, et al., 2011; Richardson, 2011), the threats are equally damaging. Greenemeier (2006) postulated that, despite a perception that insider sources of attack appeared to be secondary, the aftermath was still most costly (Banerjee, Cronan, & Jones, 1998; Peltier-Rivest & Lanoue, 2011).

1.3 Background, Problem Statements and the Orientation of the Study

According to (Martinez-Moyano, Conrad, & Andersen, 2011; Pfleeger & Caputo, 2012), combatting threats in AIS by focusing solely on technical aspects or accounting procedural controls (Otley & Fakiolas, 2000) is not sufficient. As early as the 1970s, researchers such as Hopwood (1972) and Otley (1978), to name a few, found that even with tightly monitored accounting procedural controls, dysfunctional behaviour of subordinates was still prevalent, and even induced by the control mechanisms themselves. This is partly due to the limitations of the accounting data to serve a managerial purpose, and partly because of a lack of understanding of dysfunctional behaviours of individuals and organisational performance (Jaworski & Young, 1992).

Similarly, the work of Shabtai, Bercovitch, Rokach, and Elovici (2014), Jans, Lybaert and Vanhoof (2010), and Debreceny and Gray (2010) on data mining techniques are useful for addressing internal fraud in AIS. However, the techniques are limited to post-event technical analysis rather than effectively deterring dysfunctional behaviour or providing a comprehensive understanding of the issues. Calls for behavioural studies in AIS and IS in general are prevalent in the literature (e.g. Boss, Kirsch, Angermeier, Shingler, & Boss, 2009; Crossler et al., 2013; Hu, Dinev, Hart, & Cooke, 2012; Vance, Lowry, & Eggett, 2013; Warkentin & Willison, 2009). The initiatives demonstrate a diversity of emphases, such as IT dominance on

behaviour (Sutton, 2000, 2010a); reliance behaviour (Hampton, 2005; Mascha & Smedley, 2007); and acceptance behaviour (Hwang & Grant, 2011; Kwahk & Ahn, 2010). It should be noted that while studies which broaden our understanding of the cognitive aspects of dysfunctional behaviours, particularly those originating within the organisation, will be beneficial (Dinev, Goo, Hu, & Nam, 2009), single-discipline studies do not facilitate a holistic comprehension of the "bond" that nurtures such actions. This is because individuals behave differently when taken out of their context (Sutton, 2000). Understanding the bond and its interconnected elements will provide more comprehensive insights into insider dysfunctional behaviours, and result in the most effective deterrents. This is particularly true in complex organisations where AIS support disparate tasks.

Given that tasks within organisations vary significantly, particularly in their information-generating cores, it has become the norm for organisations to make extensive use of enterprise-wide systems with sophisticated technologies. Therefore, AIS (the technology) and its users (the operators) are regarded as two interconnected elements that make the entire system functional or dysfunctional. The interaction between these two elements constitutes a distinct bond between the technology and the users. For this reason both elements are better studied together, to take into consideration advancements in related disciplines (Merchant, Van der Stede, & Zheng, 2003) rather than focussing on them separately. In order to penetrate the layers that make up the bond, a guiding theory is required to underpin the study.

Many psychological, organisational and social theories (e.g. Moody & Siponen, 2013; Pfleeger & Caputo, 2012; Posey, Roberts, Lowry, Bennett, & Courtney, 2013) have been used in IT, accounting and AIS studies to enhance our

understanding of behaviour and technology. However, scholars such as Hanseth, Aanestad and Berg (2004) argued that these approaches neglected an important element – the technology itself. This is because the studies drew upon borrowed theories from other disciplines that isolated the technology, despite being applied in the AIS environment. The notion of socio-technical systems (Kwahk & Ahn, 2010) as suggested in actor network theory (ANT) is therefore relevant to put into perspective the behavioural aspects of managing organisations effectively (Abernethy & Brownell, 1997). ANT is guided by the principle that there is neither human-only nor technical-components-only network systems (Hanseth, et al., 2004). Since ANT assumes no a priori human, social and technology impacts but insists on parallel co-existence of these elements, this theory presents an appropriate framework for understanding the origins of dysfunctional insider behaviour in the AIS environment.

The threats to AIS from legitimate users are many and varied, and in order to fully realise the benefits of AIS, dysfunction emanating from within must be adequately addressed. In the early era of electronic data processing (EDP) and the introduction of management information systems (MIS), confusion arose from the interconnections between the two and resulted in "people problems" being scantily addressed (Dickson & Simmons, 1970). Dickson and Simmons (1970) contended that the problems ranged from *avoidance* (or refusal to use the system) to *projection,* that places blame on the system, and ultimately to *aggression,* including sabotage. In support of these tenets Abu-Musa (2006) further outlined eight common insider behaviours of serious potential concern to the security of AIS. These behaviours start at the input stage, such as an erroneous data entry, and continue through to output

level with for example, a misdirection of prints. As the scale and magnitude of insider dysfunctional behaviours vary in their nature, consequences and intentions, discerning them in an appropriate setting is compelling.

Malicious or otherwise, insiders are not only legitimately connected to AIS; they also have a better understanding of the ways in which the entire system and internal controls work. These individuals sit behind organisational firewalls (Warkentin & Willison, 2009), have escalated user privileges, and comprise the weakest link in securing organisational AIS assets (Crossler, et al., 2013). They are also aware of valuable target locations (Probst, Hansen, & Nielson, 2007), giving them a huge advantage over external cybercriminals (Nicholson, Webber, Dyer, Patel, & Janicke, 2012). Malicious users exhibit a different attack signature than outsiders (Beautement & Sasse, 2009); they have system privileges that can be escalated without setting off an intrusion detection system (IDS) (Tapiador & Clark, 2011) making the threat of a data breach very real. Good AIS defence mechanisms are not the only answer to the issue (Martinez-Moyano, et al., 2011; Pfleeger & Caputo, 2012; Tapiador & Clark, 2011; Williams, 2008). Coupled with mounting evidence of insider attacks and misuse of corporate AIS or IT in general, the need to look at the behavioural aspects of insiders as an internal source of threat was prompted. Mapping dysfunctional behaviour in the AIS environment to better comprehend how it happens and what factors contribute to such negative behaviour has become crucial. To further strengthen the theory of interconnections proposed in ANT, a prominent behavioural theory, *theory of planned behaviour (TPB),* has been used in this study to chart possible links to dysfunctional behaviour.

To add further complexity, the "people" problem is not confined to individuals. Other factors also contribute to the problem. As technology becomes an inseparable part of society (Hanseth, et al., 2004), ANT evolves and revolves around the socio-technical, emphasising the dominant interaction between humans and technology. Accordingly, this study was designed around TPB and ANT, with a myriad of socio-technical facets to map behaviour beyond a purely cognitive perspective. Within the context of insider dysfunctional behaviours in AIS, this study incorporates the interface of human behaviour, technology and their interconnections, to better grasp the interactions of these varied, non-priori elements.

The vast literature on AIS is either IT- or information-system (IS) specific; or focuses exclusively on accounting, managerial and/or financial reporting. As far as behavioural aspects are concerned, the literature on accounting information systems generally focuses on the human-computer interaction (e.g. Abernethy & Bouwens, 2005; Hwang & Grant, 2011; Kwahk & Ahn, 2010; Selamat & Jaffar, 2011), and factors contributing to or deterring the use of AIS (Davern & Wilkin, 2010; Selamat & Jaffar, 2011).

Researchers have examined the fraudulent activities and misuse associated with IT/IS in general, and there is a scarcity of studies focussing on AIS-specific negative behaviour. Furthermore, these studies on IT/IS emphasise security breaches originating from outside the organisation rather than those emanating from within (Furnell & Phyo, 2003; Magklaras & Furnell, 2002, n.d.; Phyo & Furnell, n.d.; Velpula & Gudipudi, 2009). Since insiders are equipped with access and prolific AIS resources, the risk of malfeasance is concerning.

IT/IS literature is abundant with studies on insider security-related behaviour (e.g. Baruch, 2005; Boss, et al., 2009; Greenemeier, 2006; Hu, et al., 2012; Siponen, Adam Mahmood, & Pahnila, 2014; Vance, et al., 2013), yet little attention has been given to distinguishing one type of negative behaviour from another (Crossler, et al., 2013; Posey, et al., 2013). Although studies of behaviour at an aggregated level provides general insights, they do not explain behavioural variability across situations (Ajzen, 1991). The issue with aggregation is further compounded when it comes to insider threats where the absence of behaviour disaggregation leads to sample contamination and statements of limited practical use. Crossler et al. (2013) and Posey, et al. (2013) raised this concern, because studies emphasising insider security awareness may not address issues related to those who engage in acts of malicious intention. These authors suggested that "the knowledge gained from focusing on a single behaviour or subset of behaviours is not necessarily generalisable to the grand structure of behaviours" (Posey, et al., 2013, p. 1190). Guo (2013) reiterated this in his study on security-related behaviours in IS, which reported inconsistent and contradictory results, partly due to diverse interpretations of such behaviours ("many of the concepts overlap with each other on some dimensions and yet are different on others" (Guo, 2013, p. 242), and partly because factors that explain IS security compliance do not necessarily account for policy violations.

The extant literature suggests that several gaps exist in AIS governance, most notably in the theoretical foundation that provides an understanding of how individual, contextual (organisational culture) and technological factors (AIS) interact to give rise to dysfunctional behaviour, and methodological deficiencies in

the analyses of insider malpractice at macro and micro levels. These gaps in the literature, together with mounting evidence of insiders' misuse of AIS assets, were the main drivers for the current study examining AIS-specific dysfunctional behaviour within organisational settings.

1.4 Research Questions

In addition to the limited literature on insider dysfunctional behaviours, a review of the issues that generate negative effects in the AIS environment provided the impetus for this study to broadly factor in elements that influence behaviour. Whilst there are numerous studies on employee dysfunctional behaviours, comprehensive studies that encapsulate individual, organisational and technical factors are limited, and consequently, many questions remain unanswered. In this study the questions are centred on *how* and *why* unwarranted behaviours persist despite procedural and technical controls. The monitoring mechanisms that have been put in place are also examined.

Scholars in IS security have investigated the behavioural aspects of insiders to provide insights into harmful practices in relation to organisational IS assets. This is evident in previous research into IS security compliance/non-compliance behaviour (Boss, et al., 2009; Ifinedo, 2012, 2014; Myyry, Siponen, Pahnila, Vartiainen, & Vance, 2009; Siponen, et al., 2014), IS misuse (Glassman, Prosch, & Shao, in press; Grant, 2010; Moody & Siponen, 2013; Siponen, Vance, & Willison, 2012; Vance, et al., 2013), and studies on computer abuse (Baruch, 2005; Lowry, Posey, Roberts, & Bennett, 2014; Posey, Bennett, & Roberts, 2011). Furthermore, investigations into IS security largely focused on non-malicious and non-compliance behaviour (Warkentin & Willison, 2009; Willison & Warkentin, 2013), highlighting

the need to investigate volitional malicious actions more deeply. Studies by Moore, Cappelli, and Trzeciak (2008) on acts of sabotage, and those by Baskerville, Park, and Kim (2014) on deliberate computer abuse, began to address this gap.

However, there is a need to look at common behavioural traits at the higher-order structure, and differences at the subset level. Accordingly, this study investigated how predictors of behavioural intention, termed *dysfunctional behaviour*, differs at aggregated and subset levels. It addressed the methodological issues raised by scholars (e.g. Crossler, et al., 2013; Guo, 2013; Posey, et al., 2013; Warkentin & Willison, 2009) and advances our knowledge of behavioural intention across different types of insider dysfunctional behaviours. Within the context of AIS, research question 1 was as follows:

Research question 1: How are different types of insider dysfunctional behaviours related to or different from one another?

Research question 1 is concerned with the individual level. It looked at how insiders articulate their cognition to result in misbehaviour. Analysing the behavioural types, allows the study to deeply examine the constructs that shape the decision to engage in negative behaviours. In addition to the typological analysis, an investigation on the constructs and the path that leads to the intention to misuse explain the much-needed *why* factor, which is lacking in the development of theories in the AIS discipline (Sutton, 2004b). In this regard TPB is acknowledged for its predictive capacity and was used as the basis for charting insider dysfunctional behaviour.

Although TPB is lamented for its cognitive assimilation constructs, the theory critically analyses behaviour at an individual level. Despite the fact that TPB incorporates the *subjective norm,* which affects a subject's articulation of others' views on an intended behaviour, other influential external elements are not factored in. This led to the second question in the study, aimed at identifying significant external triggers for such behaviours, real or intended.

Research question 2: What are contextual factors influencing the predictors of behavioural intention?

AIS security issues stemming from negative insider behaviours are not limited to individuals' traits and personalities, although these have been found to be statistically correlated (Grant, 2010). The literature also acknowledges that the people problem is not limited to the inner persona (Dickson & Simmons, 1970), but extends to situational facets (Fox & Spector, 1999) with which individuals interact. All these elements contribute to assimilation of the behaviours.

Attempts to diffuse insider threats are largely influenced by generally accepted practices. These materialise in the form of acceptable IT/IS security and asset usage policies, and training and awareness programs that become a template from one organisation to another. Despite heavy investment in this area misbehaviour still persists, leaving organisations vulnerable to losses resulting from such actions. What is needed is a radical revamp of the approach to managing insider threats. However, any attempt to address insider threats has to be grounded on a

sound approach, preferably, based on an empirically tested model. Therefore, the third question of this study was:

Research question 3: From a socio-technical perspective, how can insider threats be managed?

1.5 Objectives

In order to answer the above research questions, the following objectives formed the foundations of the study:

1. To categorise insider dysfunctional behaviour into a relevant taxonomy.
2. To investigate the influence of contextual factors on the predictors of intention to engage in dysfunctional behaviour in the AIS environment.
3. To analyse the influence of different types of dysfunctional behaviours.

1.6 Significance of the Study

The importance of this study is linked to its anticipated contribution. Rather than measuring intention to comply with IS security policy and inferring that an absence of compliance demonstrates non-compliance and therefore dysfunction, the current study focuses directly on dysfunctional behaviour in AIS. The absence of compliance intention does not necessarily imply dysfunction, because the latter can be attributed to failure of the instrument, which has primarily been designed to measure compliance intention and not dysfunctional behaviour. This is well

documented in the many studies by Greene and D'Arcy (2010), Ifinedo (2012, 2014), and Rhee, Kim, and Ryu (2009), in which their instruments clearly encompass a spectrum of one's cognitive assessment on intention to comply with organisational IS security policy. In the study by Greene and D'Arcy (2010), none of the questions measuring intention to comply with security policy contained any element of dysfunctional behaviour. This does not indicate that their instrument is inaccurate, but rather that the instrument is accurate only within the context of their study. Therefore, although such studies provide greater insights into compliance intentions and behaviours, they do not describe how dysfunctional behaviour is formed. This is where the current study makes a valuable contribution by directly investigating dysfunctional behaviour in AIS.

Acquiring data about dysfunction by asking respondents about their intentions to engage in negative behaviours presents an enormous challenge for researchers. Despite a firm policy on anonymity that governed this study, it was difficult to extract an honest and reliable response. To address this dilemma, vignettes were used in this study to create scenarios that were carefully adapted from D'Arcy and Hovav (2009) to provide a comfortable psychological separation between the perpetrators described in the vignettes and the respondents.

While numerous theories and pragmatic approaches in the literature were designed to address insider threats in the AIS environment, only limited studies have simultaneously analysed all three factors: the individual, technical and organisational elements. As for its parent disciplines, "AIS research borrows (theories) substantially from economics, psychology, sociology, and philosophy, but only limited effort has been put into developing theory within an AIS context" (Sutton, 2004a, p. 283).

Many of the existing theories in AIS contribute to *what* and *how*, with noticeably fewer addressing the *why* dimension (Sutton, 2004a). This has resulted in the failure of IS security campaigns in organisations, stemming from the inability of management to understand the human aspects of the IS security culture (Lacey, 2010).

In addition to addressing these shortcomings, this study contributes to the AIS discipline in several ways. Firstly, it maps the link between insiders' dysfunctional behavioural intentions and its antecedents (together with their possible constructs). Through the lens of *actor network theory (ANT)* and the *theory of planned behaviour (TPB),* further examination of possible constructs were explored and empirically tested.

Second, the study contributes an empirically tested dysfunctional behaviour taxonomy overlaid on top of computer skills and intention vectors, adapted from the work of Stanton, Stam, Mastrangelo, and Jolton (2005). This taxonomy not only provides a structured approach to aggregate and disaggregate dysfunctional behaviour categories, but also helps to explain different correlation strengths and significances of given behaviours between intention and contributing variables at both macro and micro levels. The approach addresses issues of *what* and *how* in AIS theory development with reference to insider dysfunctional behaviours. It is also a preliminary attempt to alleviate the methodological concerns raised by Crossler, et al. (2013), Guo (2013) and Posey, et al. (2013) that insider dysfunctional behaviour must be studied in its grand structure for a general understanding of how behaviours form, and at its subset level for more detailed exploration.

The formation of insider dysfunctional behaviours can be simplistically explained by a causal model proposed and empirically tested by Jaworski and Young (1992). The model is comprised of six constructs, including dysfunctional behaviour, whereby the elements can be grouped into a contextual cluster, mediator and behavioural components. The literature suggests varying degrees of correlation among the assemblages, giving rise to the notion that there is another set of variables in action that moderates the relationship. Therefore, the current study has been organised in a way that reflects the formation of dysfunctional behaviours, taking into consideration the relationship among the disparate components. This is illustrated in Figure 1 below.

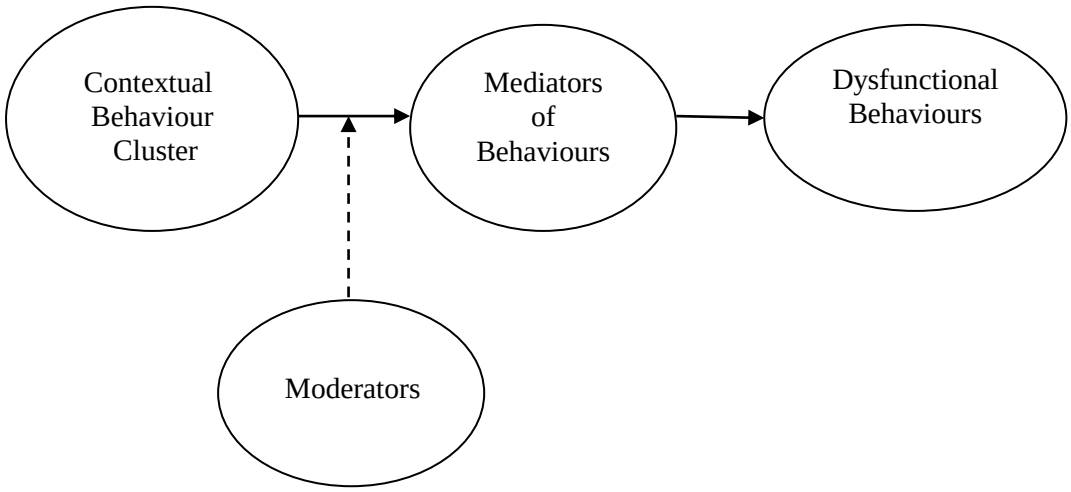


Figure 1: Contextual Cluster, Mediators, Dysfunctional Behaviours and Moderators.

In Figure 1 the dysfunctional behaviour of insiders is theorised to regress with a contextual behaviour cluster in which attitude, subjective norms and perceived behavioural control form subdivisions within this group. In Figure 1 the hypothesis

is that the relationship between the contextual cluster and the actual behaviour is mediated by an intention. It is further proposed that another set of variables, represented by moderators, also influences the relationship. A more detailed breakdown of the components and the relevant variable classes are discussed in section 2.6 of this study.

Whilst behavioural intentions can be formed as a result of attitude, subjective norms and perceived behavioural control, the actual behaviour may not materialise until an opportunity arises and an adequate resource is obtained (Ajzen, 1991; Ajzen & Madden, 1986). Ajzen and Madden (1986) suggested that the opportunity is an external factor which affects behaviour by increasing a sense of perceived behavioural control. The opportunity and the resources, which manifest in various shapes and forms, thus exert an influence on the connection between the intention and its antecedents. This is aligned with actor network theory propositions where the network encompasses many actants, all requiring investigations.

This study adds another dimension to the body of knowledge by defining an appropriate set of actants that form the network of insider dysfunctional behaviours in an AIS context. By empirically and simultaneously examining all three dimensions (individual, organisation and technology levels) of the dysfunctional behaviours, this study contributes to theory development in AIS by invoking the most substantive, yet less researched *why*.

From a practical perspective, the current study bridges the gap between the context of AIS control measures and the actual needs of AIS defence mechanisms. Since issues of security and control measures are not exclusively technological, the behavioural aspects of those connected to AIS and the associated risks should form

the basis of a managerial decision about which resources are worth protecting and how to protect them from internal attack or simple misuse. This is supported by propositions in ISO/IEC 27000 series and the COSO's risk-based, integrated internal control framework, where security and internal control measures lean more towards meeting managerial objectives rather than shortfalls in technology. Both control frameworks also support the actor network theory and suggest that security related issues in IT/IS particularly, are socio-technical and multifaceted.

The model proposed in this study is intended to impact the way in which organisations conduct their AIS security training and awareness programs. By dissecting appropriate and relevant aspects of insider dysfunctional behaviours, more rigorous and effective approaches to security can be devised. Rather than relying on widely-practiced strategies, an empirically tested model of insider dysfunctional behaviours will provide a better solution in the form of a major revamp of the security policies.

Chapter Two
Literature review

2.1 Introduction

Insider dysfunctional behaviour in accounting information systems poses a real threat to the functioning of an organisation. Despite reports and surveys that indicate a declining trend in internal sources of attack (Doherty, et al., 2011; Leach, 2003; Stanton, et al., 2005), threats loom as large as before, since insiders are a weak link in the information security net. This study focuses on aspects of insider dysfunctional behaviours in accounting information systems (AIS), such as an attack on the system (Lynch, 2006), a password-sharing culture (Abu-Musa, 2006; Collins, 2008; Stanton, et al., 2005), intentionally inputting wrong data, and other instances of non-compliance with security policies, all of which represent some of the many negative actions that do not conform to management-approved conduct.

Insider dysfunctional behaviours in the AIS environment encapsulate more than technology-based control measures. It includes an understanding of the key drivers and the intricate network in which these drivers interact to prompt the cognitive dysfunction. More attention is required to better address the issues. Although the risks may not be completely alleviated, mitigation to an acceptable level should be a managerial priority. Contextual facets of the theory of planned behaviour (TPB) and propositions in actor network theory (ANT) and the accounting information system itself, can therefore shed some light on the tenets of cognitive malfeasance in AIS.

2.2 Accounting Information Systems

Accounting information systems is a discipline in its own right, and is traceable back to the information technology (IT) and accounting fields (Sutton, 2004b, 2010b). It is evident from the literature that AIS shares commonalities with its parent disciplines in terms of theories and approaches, yet in a practical sense it is the need for business information that sets AIS apart. This has prompted IT to become an enabling tool for the accounting discipline by collecting and processing business information.

In its initial stages, AIS was a highly structured system aligned with the concept of conventional paper-based accounting systems, and centred mostly on transaction processing cycles and capturing only accounting data. This can be traced back to early computerised accounting applications such as *Noah 1* released in 1977, *Champion* in 1981, *MYOB* in 1989, and *Peachtree* that began in the mid-1970s (Cohn & Bellone, 1997). Limited by hardware capability and high costs, these early AIS applications, with the exception of Champion, were structured according to batch-processing principles to replace journal entries that would otherwise have been done in a conventional bookkeeping record. Technological advancements and increased affordability of both hardware and software have allowed conventional accounting information systems to remove the former constraints. Today AIS is more holistic or enterprise-wide, includes both financial and non-financial information, and captures internal and external data as well as future-oriented data (Abernethy & Guthrie, 1994). These modern features encourage organisations to make full use of AIS capabilities, as evidenced by an estimated annual compound growth in the enterprise resource planning (ERP) global market of 6.7 percent, which stood at US$18 billion in 2007 ("Market Studies," 2007).

Although AIS is not extensively studied by comparison to the information systems field (Granlund & Mouritsen, 2003), the importance of AIS is widely acknowledged in the literature (Granlund, 2011; Granlund & Mouritsen, 2003). Sound AIS alignment (Ismail & King, 2005), good task-technology fit (Benford & Hunton, 2000) and company-wide implementation of AIS (Fayard, Lee, Leitch, & Kettinger, 2012; Grande, Estébanez, & Colomina, 2011) were not only found to be positively correlated with firm performance, but also improve firms' financial indicators in the long run. AIS and the technology that powers it mould the corporate culture, support and shape both technical and strategic decisions (Nicolaou, 2000) and even redesign entire internal control structures of organisations (Ramadhan, et al., 2003). AIS has therefore become an integral part of organisations (Mauldin & Richtermeyer, 2004; Mauldin & Ruchala, 1999; Sutton, 2010a) which, if properly aligned, is worthy of the investment.

Despite its usefulness, insider threats are of particular concern in the AIS field. On the pretext that AIS is shrouded by the dominance of IT and accounting, pertinent issues have been addressed from the perspective of one of these disciplines, with a technical and/or procedural emphasis. Although the literature provides useful insights, there are a myriad of AIS facets that have not been closely studied to obtain a better understanding. Against this backdrop, the current study sought to fill the gaps in the literature by addressing insider threats in the AIS environment.

2.3 Dysfunctional Behaviour

Studies on behaviour in information systems (IS) in general have advanced our understanding and ability to deal with the risks posed by insiders. A vast amount of literature has examined negative insider behaviour from the perspective of IS

security compliance/non-compliance (Barlow, Warkentin, Ormond, & Dennis, 2013; Furnell & Rajendran, 2012; Harris & Furnell, 2012; Padayachee, 2012b). Computer misuse (Liao, Luo, Gurung, & Li, 2009; Vance, et al., 2013), and computer abuse (Baruch, 2005; Lowry, et al., 2014; Posey, et al., 2011) can be aggregated as IS security deviant behaviours (Burns, 2013; Cheng, Li, Li, Holm, & Zhai, 2013).

While deviant behaviour is understood within the context of volitional malicious (Burns, 2013; Wall, 2013) and non-malicious (Burns, 2013) behaviours, this aggregated behaviour typology does not differentiate between similar yet fundamentally disparate behaviour. An example of this would be intentional AIS record modifications within one's authorised workspace, as opposed to record changes that require escalated user privileges. The former action requires less computer skill, while the latter requires more computer knowledge to penetrate internal firewalls and remove the digital footprint of such actions from an organisation's server logs. Control remedies, such as instituting supervisory authorisation prior to record changes, do not fully address acts of unauthorised record changes requiring high computer competency and in turn, protective control technologies to detect such attempts. Deviant behaviour therefore provides a foundation from which to understand negative insider behaviour at the aggregated level, but suffers from typological deficiencies at the subset level, because behaviours are only categorised on the basis of intention (i.e. malicious and non-malicious).

The interpretation of Jaworski and Young (1992) emphasises the aspect of "knowingly performed" and supports the idea that the behaviours in focus are executed within the consciousness of the performer. This is further supported by

Furnell and Phyo (2003), who suggested that motive or intention is one of the best ways to categorise IT misuse. However, it should be noted that intention does not necessarily mean malicious intent. Even an act carried out in good faith is considered dysfunctional when that behaviour goes against management-sanctioned conduct.

An early attempt to disaggregate seemingly similar behaviours in IS was undertaken by Davis (2001), who modelled two pathological internet use/misuse scenarios by referencing their symptoms and effects. Davis's work not only provides a general basis for dysfunctional behaviour categories, but also allows scholars to understand how the intricate connections of psychopathology (e.g. depression and social anxiety) as well as situational factors, reinforce users' cognitive dysfunction leading to internet use/misuse. Magklaras and Furnell (2005) extended this concept by including computer skills as part of their proposed user sophistication model which advanced the identification and classification of dysfunctional behaviour. Guo (2013) proposed eight dimensions[2], including intention and computer skills, to identify subsets of dysfunctional behaviour.

An examination of the two dimensions of intention and computer skills found that one of the many comprehensive attempts that pave the way to aggregation and disaggregation of insider behaviour had been demonstrated by Stanton, et al. (2005). These authors listed 94 behaviours which were subsequently categorised into 6 types using a 2-vector plane – the level of computer skills (low to high) and a continuum of intention (malicious to neutral to good) in a given behaviour. These 6

[2] Eight dimensions are (1) intention (focuses on volitional/non-volitional action), (2) malicious/non-malicious, (3) level of computer skills and knowledge, (4) type of perpetrator, (5) job relatedness, (6) direct or indirect damage to organisations, (7) requiring action or absence of actions by employees, and (8) actions are subject to policies or laws.

categories included 4 risky behaviour types, *intentional destruction, detrimental misuse, dangerous tinkering,* and *naïve mistake*, and 2 acceptable practices (*aware assurance* and *basic hygiene*). Table 1 summarises a description of these behaviours.

Table 3

Categories of Behaviour (Stanton et al., 2005)

Behaviour	**Description**
Intentional destruction	Requires high technical expertise together with a strong intention to harm organisational IS assets.
Detrimental misuse	Requires minimal technical expertise with minimal intention to do harm through actions such as annoyance, harassment, and rule breaking.
Dangerous tinkering	Requires technical expertise but with no clear intention to do harm to organisational IS assets.
Naïve mistake	Requires minimal technical expertise with no clear intention to harm organisational IS assets.
Aware assurance	Requires technical expertise together with a strong intention to do good by preserving and protecting organisational IS assets.
Basic hygiene	Requires no technical expertise but includes clear intention to preserve and protect organisational IS assets.

In this study, dysfunctional behaviour has been defined as a motivated behaviour, detrimental to an organisation, team, individuals and/or external stakeholders (Griffin, O'Leary-Kelly, & Collins, 1998)[3], and requiring a certain level of computer skills. It is described as negative behaviour knowingly performed

[3] The work of Griffin et al. (1998) was taken into consideration although their study looked at the behaviours from a general workplace perspective. The authors methodologically classified the behaviours as dysfunctional when there was an existence of dysfunction in the context, intent, motive and consequences. The approach they used to arrive at their categories is relevant to this study.

(Jaworski & Young, 1992) without proper alignment to the interests of related parties. Dysfunctional behaviours are therefore defined as detrimental to related parties, or represent a quantifiable (monetary) or non-quantifiable (unjust satisfaction) personal benefit at the expense of others. In particular, such behaviour violates certain norms, and in its various forms, subsequently impairs the functioning of others (Felps, Mitchell, & Byington, 2006). The current study uses this definition to examine dysfunctional behaviour in the context of a motivation (intention) to perform an action that requires computer skills.

Amongst many negative psychological connotations, Jensen and Patel (2011) argued that counter-productive work behaviour can either be directed at the organisation or individuals within the organisation. In an extreme case, fraudulent behaviour materialises as an example of counter-productive performance. Jaworski and Young (1992) looked deeper into the prospect of employee dysfunctional behaviours motivated by self-interest, where the behaviours violated control procedures but were not targeted at either the organisation or individuals. Rather, they were executed to meet specific job performance indicators through *gaming*[4] or *strategic information manipulation*[5]. In either case the motive remains the same, that is, to fulfil personal interest regardless of the negative consequences to the organisation or individuals within the organisation.

---

[4] In a *gaming* process, an employee chooses to maximise a performance indicator which is measured by a superior regardless of a detrimental effect of such action in the long run.

[5] One of the popular methods of strategic information manipulation is the income-smoothing technique. Through this scheme, the natural flow of information is altered without having to change the actual value of the data. Some of the incomes are matched against expenses incurred in periods which result in performance tailored to the preference of the perpetrators.

In examining the consequences of such behaviour, the magnitude of effect of the dysfunction is further compounded within teams. The negative behaviour of a member of a team can be detrimental to the functioning of the whole group (Felps, et al., 2006). Although visibly negative behaviour can be corrected by supervisory or managerial remedial action, less visible or discreet dysfunctional behaviour, such as fraud, presents a greater challenge for both teammates and management. One of the many difficulties facing management is to take the necessary corrective action against such inconspicuous behaviour in order to deter the behaviour, but in a sophisticated digital world operating around a spinal column of accounting information systems, many fraudulent acts go unnoticed for several years.

In contrast to the most obvious negative behaviours, a less dramatic example is the misuse of an AIS facility. This type of negative activity, both with or without apparent malicious intent, can be detrimental if it goes undeterred. Misdirection of a printout (Abu-Musa, 2006) and password-sharing practices can be viewed as simple errors of judgement. However, the consequences are confounding. In the case of the National Health Service (NHS) in the United Kingdom in 2007, a simple error of judgement involving the sharing of passwords led to an unsolved patient's death (Collins, 2008). What is more intriguing is that a year prior to this case, the same author highlighted serious instances of improper access to patient health records, mostly involving password-sharing practices (Fleming, 2006). The situation was neither detected nor sanctioned by management until investigation of the 2007 case was concluded as unsolved. It transpired that the doctor, whose account was used by another individual to access the patient's record, misdiagnosed the patient. Although the NHS case is not directly related to AIS, it is a good

illustration of how practices, even without malicious intent, can negatively impact an organisation.

2.3.1 Taxonomy of Dysfunctional Behaviour in AIS

Human behaviour is the result of complex cognitive assimilation of a decision-making process. Understanding the behaviour and how it is triggered presents great challenges. Such complexity has prompted some scholars to isolate behaviours (in Abu-Musa, 2006; Dickson & Simmons, 1970; Jaworski & Young, 1992) in order to better analyse and make sense of a given dysfunctional behaviour and its triggers.

Indiscriminate use of methodology has attracted criticism, and although it has merits, suffers from deficiencies and contamination (Gupta & Jenkins Jr, 1991). Separating the negative behaviour from its relevant spectrum can lead to a loss of meaningful detail in exchange for an explanation (Gupta & Jenkins Jr, 1991) to substantiate interconnections (Jensen & Patel, 2011) between the triggers and possible interdependencies (Dalton & Todor, 1993) between various dysfunctionalities with a similar continuum. This is particularly true when the same treatment, applied to similar audiences, results in different observations.

Moreover, ignoring disparities that exist between the dysfunctional behaviours within the same spectrum can contaminate the criterion (Pelled & Xin, 1999). Certain dysfunctional behaviours are either alternatives or interdependent of each other. Observing two similar, yet finely separated negative behaviours as a unitary element can result in good comprehension, but suffers from deprived explanatory power due to contamination. Nevertheless, studying behaviour at its

aggregate level can provide general disposition (Ajzen, 1991) which helps us to understand how the dynamics of the behaviour work.

Balancing the need to understand the dynamics of insider dysfunctional behaviours in AIS and the explanatory power resulting from the observation therefore requires careful consideration. In this study, four negative behaviours were carefully categorised with regard for their diversity, into relevant continuums based on a behaviour taxonomy introduced by Stanton, et al. (2005). Selected studies have been summarised in Table 2 to show how dysfunctional behaviour was analysed, putting to rest the methodological concerns raised by Gupta and Jenkins Jr (1991), Guo (2013), Posey, et al. (2013), Crossler, et al. (2013), and Warkentin and Willison (2009).

In seeking to explain the antecedences and formation of the behaviours, various studies have analysed dysfunctional behaviours in the AIS environment in terms of types of threat (e.g. in Leach, 2003), types of perpetrator (e.g. in Anderson, 1980), information processing stage (e.g. in Abu-Musa, 2006) or intention (e.g. in Griffin, et al., 1998; Magklaras & Furnell, 2002). Interestingly, in a general workplace setting, Griffin et al. (1998) also categorised dysfunctional behaviours based on injury effects. These authors suggested that dysfunctional behaviour can be categorised as *injurious to individuals* or *injurious to organisations*.

Table 4

Selected Studies on Insider Dysfunctional Behaviour

Authors	Behaviour Themes	Number of Vignettes	Behaviour being Studied	Stanton et al. Taxonomy
Hovav and D'Arcy (2012)	Information system misuse	4	Email misuse	Detrimental misuse
			Unauthorised access via found password	Detrimental misuse
			Unauthorised software installation	Dangerous tinkering
			Unauthorised record change	Intentional destruction
D'Arcy and Hovav (2009)	Information system misuse	2	Unauthorised access	Detrimental misuse
			Unauthorised data modification	Intentional destruction
Vance, Siponen, and Pahnila (2012)	Security (non) compliance behaviour	6	Reading confidential documents	Naïve mistake
			Failing to report computer virus	Naïve mistake
			Using unencrypted portable media	Naïve mistake
			Failure to lock (log off) PC	Naïve mistake
			Sharing passwords	Naïve mistake
Myyry, et al. (2009)	Security (non) compliance behaviour	1	Password sharing	Naïve mistake
Son (2011)	Security compliance behaviour	0	Regular scan for viruses	Basic hygiene
			Compliance with security policy with regards to email	Basic hygiene
			Compliance with security policy with regards to use of internet and network	Basic hygiene
			Installations of operating system patches to prevent unauthorised access	Aware assurance

Authors	Behaviour Themes	Number of Vignettes	Behaviour being Studied	Stanton et al. Taxonomy
Boss, et al. (2009)	Security compliance behaviour	0	Keeping up to date with latest security threats	Basic hygiene
Lee and Larsen (2009)	Security compliance behaviour	0	Adopt anti-malware	Basic hygiene
Ifinedo (2012)	Security compliance behaviour	0	Intention to comply with information system security policy	Basic hygiene

Since dysfunctional behaviour covers a whole range of negativity in the workplace, categorising them is challenging. Nonetheless, commonalities have been found amongst these behaviours that indicate a notion of similarity and suggest the different dysfunctional behaviours share a common two-part vector. At the individual level, the observed intentional behaviour can be benevolent or malicious (i.e. intention vector), while at the organisational level the behaviour can be either harmful or harmless (i.e. severity vector). However, using these two vectors to categorise these behaviours presents a complex and chaotic taxonomy, despite the apparent fit with a socio-technical network as postulated in *actor network theory* (ANT). This is due to the nature of the latter vector, the perceived severity, where the actual aftermath is rather obscured and can exceed an individual's or organisation's preliminary assessment of the outcomes of a given dysfunctional behaviour. Aligned with this notion is the finding of Ifinedo (2012), where the perceived severity resulting from an action did not warrant compliance with good security practices amongst employees in the IS environment.

Whilst the perceived severity is appealing, it does not provide sufficient evidence to support the dysfunctional behaviour taxonomy. Ajzen (1991), and Ajzen and Madden (1986) suggested that control over an action affects both intention and the actual behaviour. Therefore, both perceived and actual behaviour control carry an empirical weight for engaging in dysfunctional behaviour. This is further supported by the findings of Ifinedo (2012), Schultz (2002), and Magklaras and Furnell (2005), that self-efficacy is strongly correlated with negative behaviour and/or behavioural intention. A comprehensive study of vectors, carried out by Stanton et al. ((2005)), resulted in the identification of (IT) skills and intention vectors. It is within these vectors that this study is situated, to explain the bond and its interconnected elements in the framework of ANT and TPB constructs.

Table 3

Four-quadrant Dysfunctional Behaviours

	Computer Skill	
Intention	Malicious-high skill	Malicious-low skill
	Neutral-high skill	Neutral-low skill

At its rudimentary level, dysfunctional behaviour can be classified into a four-quadrant matrix depending on the level of computer skills and the nature of the intention, i.e. whether the behaviour requires low or high AIS skill and whether it was performed with a neutral or malicious intent. This is illustrated in Table 3. Using the four-quadrant matrix, dysfunctional behaviour was operationalised through the lens of a taxonomy established by Stanton et al. (2005), as illustrated in Figure 2.

Stanton et al. analysed 94 employee behaviours which were modal-grouped into 6 categories based on their commonalities, including 2 groups of accepted practices (which are excluded in the current study). Table 3 and Figure 2 both show, at the very extreme end (malicious – high-skill quadrant), the first behaviour category as *intentional destruction.*

This behaviour category requires high IT skills and suggests a malicious intention. The second category, (malicious – low-low quadrant) is *detrimental misuse*, and requires novice skills with a presence of malicious intention. The third (neutral – high skill) and fourth (neutral – low skill) categories are *dangerous tinkering* and *naïve mistake* respectively, both with questionable motives (unclear intention).

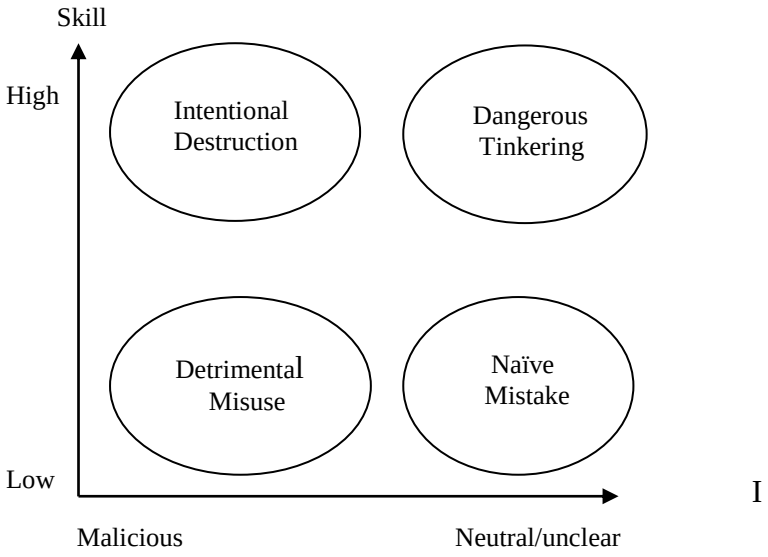


Figure 2: Two-factor Taxonomy of Insider Dysfunctional Behaviour. Adapted from Stanton, et al. (2005).

2.4 Actor Network Theory

Actor network theory (ANT) emphasises the associations of related sets of components. At its rudimentary level ANT is comprised of an *actant* (actor) and a *network*. The actant can take the form of a person, an object, an activity, or other elements that change a state of affairs (Dolwick, 2009) without necessarily being the source of the change. The network on the other hand, is a tie or bond that influences the dynamics of relationships between the actants (Worrell, Wasko, & Johnston, 2013).

In contrast to conventional theories that explain what and how things work, ANT places more emphasis on describing the bond that makes up a phenomenon (Dolwick, 2009; Hanseth, et al., 2004). This is because research in information systems should not only emphasise technological or social factors, or the two alongside each other, but should focus on incidences that exist when the two systems interrelate (Lee, 2001). More importantly, ANT asserts that every network is heterogeneous. This assumption gives researchers free rein to develop a conceptual framework pertaining to an observed phenomenon, but also gives rise to an issue of selection, so that researchers are compelled to carefully define an appropriate set of actants that play a major role in the observed phenomenon.

The literature emphasises three major elements in complex insider dysfunctional behaviour that contribute to security threats in AIS: psychology, organisation and technology. Various studies have examined these three factors in isolation, with only limited attempts to scrutinise them simultaneously. The information security dilemma cannot be adequately approached with a technology solution alone, since both socio-organisational and sociological regulations are also important (Padayachee, 2012a; Roy Sarkar, 2010). In complex technology scenarios

comprised of environment and people, a single-sided approach to coping with threats can resolve vulnerabilities in one aspect, but cause security concerns in other aspects (Sveen, Torres, & Sarriegi, 2009; Van der Stede, 2000). Failure to understand dynamic information security interdependencies can result in poor coordination among those responsible for the tasks.

In light of this issue, the current study was designed to better explain insider dysfunctional behaviours and the risks of insider threats, by simultaneously examining the cognitive constructs of individuals, organisational culture and AIS technology. The 'open' theory of ANT combined with an in-depth cognitive view of TPB, allowed for examination of three-level factors (individual, organisation, and technology).

2.4.1 Individual Level

Operators of technology represent the most important, as well as the weakest link in the security of AIS assets (Crossler, et al., 2013). Insiders operate technology with volitional controls to use at their discretion, and articulations of their behaviour can strengthen or weaken the defence mechanisms. Understanding these articulations allows a more robust and holistic approach to safeguarding AIS assets.

The "people problem" in the IS environment described by Dickson and Simmons (1970) highlighted the critical requirement to look deeper into insider behaviours. Despite the implementation of relevant security policies, individuals nevertheless act in contradictory ways which are detrimental to others and organisations. Complex assimilations of insider (mis)behaviour contribute to more

than 50% of security breaches (Lynch, 2006) and hardly changes, even when training makes them aware of existing policies pertaining to acceptable use (Grant, 2010; Wolf, Haworth, & Pietron, 2011) of these AIS assets.

Examining personality traits only focuses on the fringe of dysfunctional behaviours. The demographic parameters of insiders (Grant, 2010) and security awareness programs (Wolf, et al., 2011) were found to be statistically significant for dysfunctional behaviours, but presented limited accord to account for the misbehaviour. What is needed is a deeper look into the cognitive aspects of individuals, which manifest themselves into detrimental actions. The theory of planned behaviour is recognised for its ability to predict human behaviour at an aggregate level, and the use of this theory enabled a more nuanced analysis of the factors that compel individuals to engage in dysfunctional behaviours in the AIS environment.

2.4.2 Organisational Culture

Organisational culture forms an association with employee behaviour (Jacobson & Joanne, 2009; Musa, 2011) and influences the way people act and react (Lacey, 2010) by sustaining the performance of work customs with an established norm of proper and improper behaviours (Dent, 1991). The organisational culture binds its members with a complex pattern of beliefs, expectations, ideas, values, and attitudes that manifest themselves into actions (Pratt & Beaulieu, 1992). It can therefore be presumed that common practices in the AIS environment are attached to and shaped by the culture within the organisation. The previously mentioned NHS case in the UK is an example of how password-sharing practices was viewed as a

legitimate trade-off to accomplish tasks (Möller, Ben-Asher, Engelbrecht, Englert, & Meyer, 2011; Post & Kagan, 2007) even though such actions were not permitted in the organisation's security policy.

TPB recognises the role that organisational culture plays in individuals' behaviour, however, the influence of culture is limited to the subjective norm construct that measures others' perceptions of oneself rather than reflecting an absolute culture domain. Statements such as "most people who are important to me would probably think I should report..." (Randall & Gibson, 1991, p. 116) and "most people who are important to me think that I should..." (Ajzen, n.d.-b, p. 5) clearly demonstrate that instruments used to measure the subjective norm emphasise the importance of others' views to individuals about the intended action. While these statements have merit as a direct measurement of the subjective norm, they do not encompass the organisational culture in its entirety. The subjective norm of TPB does not provide the relative weights to factor in organisational culture in shaping behaviour. The findings of Chang (1998) and Randall and Gibson (1991) further demonstrated that subjective norms exert a moderate influence over intention when TPB is used for testing for (un)ethical behaviour. Unlike attitude, subjective norm tends to present a mixed pattern for the prediction of behaviour (Ajzen, 1991). The inclusion of organisational culture as a separate construct therefore, allows more direct measures of its influence over behaviour, and provides deeper insight into insider dysfunctional behaviours in the AIS environment.

Organisational culture forms a contextual variable (Borchert, 2011) that facilitates insider behaviours with limited negating effects on behavioural dysfunctionalities (Jacobson & Joanne, 2009). Analysing dysfunctional behaviours

through the cognitive assimilation of performers suggests that the organisational culture does not form a direct relationship with the intention and the subsequent dysfunctional behaviour. Rather, it is postulated to moderate the effects of the intention's antecedents (attitude, subjective norms and perceived behavioural control) upon the intention and/or negative behaviour.

Organisational culture is also part of a formal control (Musa, 2011) in the form of security and acceptable IT/IS usage policies embedded as an internal control mechanism. This mechanism binds members of the organisation to conform to approved standards of conduct. A poor internal control structure, particularly in the computer environment, results in poor firm performance; both at operational and financial reporting levels (Stoel & Muhanna, 2011). Therefore, the existence of these policies becomes a dimension of interest in measuring the effects of organisational culture on dysfunctional behaviour.

Further, to overcome unwarranted actions against AIS requires a set of controls that extends beyond technology-based measures, such as user privilege control, network access control, and other data-protection mechanisms. It is a board-management-staff-affected process through which an organisation can achieve its desired goals ("IC - Integrated Framework summary: COSO," 1992). Within this scope, the current study takes into account the internal control systems that go beyond management-sanctioned, technology-based control measures, many of which are based on prescribed information security and management as per ISO 27000 series and the COSO-ERM framework, incorporated by organisations as a part of their (security) culture. A strong and well-observed security culture in organisations can mitigate, if not eliminate, the risks associated with AIS. Perpetrators'

behavioural control of IC-fortified AIS is weakened in situations where the cost of executing dysfunctional behaviours is higher than the perceived benefits of successful penetration.

However, any control measure (including prescribed procedures and policies) is only as strong as its weakest point. In large organisations the resources to implement internal control mechanisms are more cost effective and readily accessible than for small and medium-sized entities (SME). Resources such as manpower, finance and expertise are real limiting factors for SMEs and can hinder implementation of a sound internal control structure (Jiang & Li, 2010). These limiting factors perpetuate weak links in the chain of internal control mechanisms. Given that effective deterrents can increase perceived threats of punishment for unwarranted behaviour (D'Arcy, et al., 2009), it is logical to assume that weak internal controls can induce dysfunctional behaviour, simply because there are more opportunities for exercising dysfunctional behaviour.

Even good internal control systems will not prevent dysfunctional behaviour in situations where top management chooses to override it. Such overrides take place when there is ineffective monitoring by those entrusted with it. At the top level of an organisational hierarchy for example, the board of directors supposedly oversees executives whose duties are to serve the shareholders' interests. However, board of directors' oversight can be conscientiously impeded by executives who are able to influence the former because they are more involved in daily operations and can induce influence over the appointment of the directors (Choo & Tan, 2007; Daily, Dalton, & Cannella Jr, 2003). Choo and Tan (2007) argued that this

'executives-tipped' balance of oversight power explains why the directors tacitly tolerate even serious dysfunctional behaviour, including fraud, amongst executives.

Similarly, a harmless practice such as password sharing to expedite certain routine transactional processes also presents a weak link in internal control measures. Paino, Ismail and Smith (2010) found that employees resort to a certain degree of dysfunctional activities in order to cope with time-budget pressures. Such actions may not be entirely motivated by malicious motives, but are practised to ensure smooth running of a routine operation or to cope with time and budget pressures used as indicators of performance within organisations.

The trade-off between security and convenience in practice is very real. A survey of 300 IT professionals by Lieberman Software Corporation in 2011 shows that 42% of respondents acknowledged their organisation practiced password and access sharing (Lieberman, 2011). Some scholars (e.g. Singh, Cabraal, Demosthenous, Astbrink, & Furlong, 2007) found that the seemingly harmless practice of sharing passwords was seen as necessary to get the job done in some cases, yet it can cause organisations to lose control over their assets (Patrick, 2008) and even face legal action (see Mook, 2012). Ironically, such uncalled-for practices can generate unwanted security risks in AIS which is what the control measures have primarily been designed to prevent. This trade-off induces a heightened sense of perceived behavioural control that compels perpetrators to exercise more severe dysfunctional behaviours.

2.4.3 Measuring Organisational Culture

The nature of organisational culture is complex, and measuring it presents an enormous challenge for researchers. The approach and subsequent analysis must

be exercised with due care. Preceding the measurement, Bellot (2011), Witte and Muijen (1999) and Schein (1990) raised several considerations for researchers to address. These include the culture to be measured, the level from which the data is to be collected, the dimensions of the culture and the methodology to be used. Each of these parameters has a profound impact on the accuracy and validity of the measurement tools and the subsequent analysis.

The issue of which culture to measure in order to determine the organisational culture stems from the interconnections and infusion of national culture (Hofstede, 1998a, 1998b), sectoral or industrial influence (Chatman & Jehn, 1994; Gordon, 1991), professional affiliation effects (Bloor & Dawson, 1994) and sub-cultures nurtured within departments (Cooper, 1994; Hofstede, 1998b) which may differ from the culture at the organisational level. Infusion of these varied cultures into the organisational culture may lead investigators to assess sub-cultures rather than the culture at the firm level. The national culture for example, is well known to affect practices in organisations (Birnberg & Snodgrass, 1988), while sectoral or industrial norms largely influence organisational behaviours regardless of the national culture. Professional bodies to which members of an organisation are affiliated also exert an influence over organisational practices, particularly when individuals in the organisation are expected to adhere to certain codes of conduct to retain their membership. In so doing, the external professional body forms a sub-culture that discerns itself in organisational practices through its membership affiliation. In a large corporation the organisational culture becomes compartmentalised within each department and develops its own unique sub-culture.

Therefore care must be taken when assessing organisational culture to ensure that it includes a composition of all the various sub-cultures.

For the current study, the culture of interest is that which manifests itself in the prevailing norms of organisations. The nature of the sample, which was limited to medium-sized entities, reduced the contamination issues of sub-cultures. Medium-sized entities are sufficiently large for culture to develop, yet not too dispersed in terms of divisions for disparate sub-cultures to proliferate. Unlike larger organisations where complex structures and management tiers dominate, the effects of culture in medium-sized entities are more visible (Peel, 2006). Therefore, according to Hofstede (1998a), measuring the culture of an organisational unit rather than individuals is appropriate in medium-sized entities, because the firm's culture closely resembles practices across all divisions.

Organisational culture characterises the organisation in which it is manifest through the individual members of the organisation and their actions (Hofstede, 1998a; Schein, 1990). The level at which organisational culture is measured depends on the uniqueness and focus of each study. Measuring the organisational culture at the firm level is adequate for certain studies, but may not be appropriate for others where varied departmental practices are an indication that a unique sub-culture exists (Cooper, 1994) within that particular department. The selection of an appropriate level to measure culture must be based upon the requirements of the study. Chatterjee Lubatkin, Schweiger and Weber (1992) and Hu et al. (2012) adopted an individual unit of measurement with a greater focus on top management. Their decision to use this sample was made on the grounds that the top management sub-culture is a reasonable manifestation of the firm's overall culture, based on the

importance of the roles and influence of the managerial level in shaping and establishing the culture of a given organisation (Deal & Kennedy, 1988; Schein, 1990).

However, the assumption does not address conflicting sub-cultures in various departments of an organisation which are incongruent with the top management group. Henri (2006) pointed out that no organisation is likely to develop just a single culture; rather an organisation is built upon a continuum of cultural dimensions (Quinn, 1988) which are anchored in a combination of values (Dent, 1991; Lacey, 2010; Pratt & Beaulieu, 1992). Regardless of the organisational hierarchy, scholars agree that the organisational unit is an appropriate unit of measurement from which to collect data for aggregation at the firm level (Hofstede, Neuijen, Ohayv, & Sanders, 1990), supplemented with analysis that controls for inter- and intra-group differences (Muijen et al., 1999; Witte & Muijen, 1999) in the cultural units' aggregate scores (Hofstede, 1998a).

Apart from the type of culture to be measured, the unit of measurement and the levels of assessment, researchers are also presented with another important consideration: selecting the culture dimensions to be assessed. The literature is strewn with many culture dimension sets, each with its own merits. Among these, five are frequently cited and include Hofstede (1998a, 1998b; Hofstede, et al., 1990) (6 dimensions), Chatterjee et al. (1992) (7 dimensions), Quinn (1988) (4 dimensions), Van Muijen et al. (1999) (4 dimensions in 2 domains) and Schein (1990) (7 dimensions). Of these five dimension sets, Van Muijen et al. (1999) distinguished between the value (evaluative) and practice (descriptive) domains. These dimensions are summarised in Table 4.

While the dimensions in Muijen's approach remained the same for the two domains, the idea of distinguishing between the values that anchor members of an organisation and actual practice adds further value to the dimension sets. Although many scholars argue that the value drives the action, situational adaptations supersede the a priori values, as evidenced in the 2009 case of the National Health Service in the United Kingdom and the findings of Shafer (2008). Even in organisations where there is consensus on values, inconsistent behaviours can still materialise (Schein, 1990). Using the value as an explanation for the behaviour rather than a subject to be explained tends to ignore the influence of historical and environmental effects on practices (Herbst & Houmanfar, 2009).

Regardless of whether the practices of members in an organisation are temporarily stable due to situational adaptations or stem from the culture of the organisation, such manifestations exhibit the practice norms. These practices are cultivated by the evaluative domain, comprised of complex patterns of beliefs, ideas, expectations and attitudes (Pratt & Beaulieu, 1992) that influence members to behave or misbehave (Dent, 1991). When the culture is defined as artefacts (e.g. Henri, 2006; Schein, 1990), observable through the expression of actions, conversations, rules and the physical environment, the descriptive (practice) domain of Muijen et al.'s (1999) approach is relevant to this study and warrants consideration.

The final consideration that incites many scholarly arguments is the method by which the organisational culture is assessed. Bellot (2011) and Jung et al. (2009) laid down a comprehensive analysis of the methods used to measure organisational culture. Two approaches are: the qualitative, which involves observations and in-

depth interviews, and the quantitative, in the form of questionnaires, checklists and structured interviews. Both have their own merits and shortcomings. The former method offers a richness of data but suffers a comparability issue (Bellot, 2011) because the framework is unstructured. Qualitative approaches also tend to impose the researcher's view rather than the respondents' perceptions (Hofstede, 1998a).

Table 4

Culture Dimensions

Authors	**Culture Dimensions**
Hofstede (1998a, 1998b; Hofstede, et al., 1990)	Power distance Individualism versus collectivism Masculinity versus femineity Uncertainty avoidance Long term versus short term Indulgence versus restraint
Chatterjee et al. (1992)	Innovation and action orientation Risk-taking Lateral integration Top management contact Autonomy and decision making Performance orientation Reward orientation
Quinn (1988)	Internal focus External focus Flexibility Control
Muijen et al. (1999)	Support orientation Rules orientation Goal orientation Innovation orientation All dimensions are assessed at both practice and value domains
Schein (1990)	The organisation's relationship to its environment The nature of human activity The nature of truth and reality The nature of time The nature of human nature The nature of human relationships Homogeneity versus diversity

A quantitative approach on the other hand, provides good quantification of data that allows for comparisons across organisations, industries and nations with substantial psychometric quality (Cameron & Quinn, 2011). However, the true value of this approach is limited to the amount of contextual information that it can offer.

2.4.4 AIS Technology

AIS technology is driven by the need for organisations to capture, process and communicate business information to both internal and external users. In the early era of AIS, the technology was confined to the development and deployment of accounting software and transaction-processing functionalities.

Scholars and users alike recognise the challenges that come with AIS, particularly security issues. Numerous studies have approached these issues by insisting on technical solutions through an emphasis on confidentiality, integrity, and availability of the data and systems (Dunkerley, 2011). These studies focused on security of AIS assets in three broad areas: access to the system, communication channels (Dunkerley, 2011; Musa, 2011) and post-event analysis of potential fraud signatures through a data mining technique (Debreceny & Gray, 2010; Jans, et al., 2010). Similarly, studies on communication channels to secure AIS have centred on technical issues by providing useful solutions for pre-despatch data encryptions, digital signatures and firewalls. System security also accentuated fortification from within the software itself. Bug fixes and constant update patches have become a technical norm to mitigate threats in modern AIS.

Lynch and Gomaa (2003) proposed that a predictable intrusion detection system (IDS) increases the likelihood of attack on a computer system. While the core of the internal control system of AIS is fortified against attack, the IDS in a

predictability context, depends on the perpetrator's familiarity with anticipating the workings of the system's defence mechanisms. It is this familiarity that propels individuals to engage in dysfunctional behaviours, ranging from simple technical tinkering with the system to fraud and acts of sabotage. The predictability of IDS thus contributes to increased familiarity, and places individuals in a position of having more control over the outcomes of their actions (Lynch & Gomaa, 2003).

2.5 Theory of Planned Behaviour

The theory of planned behaviour (TPB) creates a nexus for explaining behaviour. It posits that *intention* captures motivational factors to perform behaviour and is strongly correlated with actual behaviour (Ajzen, 1991). The theory recognises that intention is an immediate determinant of actual behaviour, that the predictive power of TPB is related to conceptually independent determinants of this mediator and the influence of other non-motivational elements such as opportunities, resources and controls over the outcomes of such behavioural performance. A*ttitude (ATT), subjective norm (SN)* and *perceived behavioural control (PBC)* exert an influence on volitional behavioural performance through intention (Ajzen, 1991; Ajzen & Madden, 1986; Rhodes & Courneya, 2003). The inclusion of PBC also encompasses non-volitional behaviours that extend beyond the influence of *attitude* (ATT) and *subjective norm* (SN). Table 5 highlights findings of selected work in the organisational field and IT/IS discipline. These studies show a mixture of significant correlations of the TPB constructs.

According to Ajzen (1991), the relative influence of ATT, SN and PBC have on intention varies across behaviours and situations. In some cases (e.g. in Chang, 1998; Randall & Gibson, 1991) intention is mostly affected by ATT and SN

with PBC only imposing a moderate influence. An explanation for this phenomenon lies in the context of the observed behaviour that a volitional behaviour does not require critical resources and opportunities. As such, PBC only plays a limited role in the formation of the intention. Nonetheless, all three predictors still make significant independent contributions towards the prediction of behaviours.

The validity of TPB has also been challenged by some scholars who share a common observation of the effects of *prior experience* upon future behaviour. In a variety of studies, past behaviour is a determinant for future intention and/or actual behaviour. The extent to which past behaviour influences the current intention and/or actual behaviour remains a matter of great debate. If the said behaviour is repetitive in nature, such action is said to be performed under the control of habitual forces rather than a decision-making hegemony (Smith et al., 2008) as proposed by TPB. This is illustrated in the studies of Hodgson (2010), Smith et al. (2008), Ouellette and Wood (1998); and Rhodes and Courneya (2003).

While authors such as Hodgson (2010) and Smith et al. (2008) argued that prior experience moulds habitual behaviour thereby undermining the cognitive aspects of TPB to predict intention and subsequent behaviour, Ajzen (1991, 2002b) proposed that the relationship between past experience and habitual behaviour is a demonstration of temporal stability. This means that regardless of whether the behaviour is a result of a frequent routine or controlled effort, both are under the influence of cognitive factors and are not an automatic response or semi-consciously performed. As long as intention and perceived behavioural control remain constant, the performance of the latter behaviour is thus unchanged (Ajzen, 2002b).

Table 5

Summary of Selected Previous Studies of the Intention's Determinants

Behaviour	Performance Benchmarking (Hill, Mann, & Wearing, 1996)	Support for Organisational Change (Jimmieson, Peach, & White, 2008)	Online Music Piracy (d'Astous, François, & Montpetit, 2005)	Use of Technology (Venkatesh, Morris, Davis, & Davis, 2003)		Unethical IT Use (Chatterjee, 2008)
				*	**	
Attitude (ATT)	0.41	0.23	0.33	0.52	0.22	0.362
Subjective Norm (SN)	0.41	0.28	0.25	0.05^	0.25	0.276
Perceived Behavioural Control (PBC)	0.11^	0.18	0.34	0.24	0.19	0.295

Note: ^ Not significant. * Voluntary use. ** Mandatory use. Unless indicated, the values are based on the respective study's significant correlation coefficients.

2.6 Theoretical Framework and Hypotheses Development

It is clear from the literature that the cognitive constructs of TPB are able to predict behaviour at the individual level. Different correlation strengths of these constructs on intention, as shown in Table 5, indicate that the paths by which these constructs affect intention (hence the actual behaviour) are also moderated by external elements with which the individual interacts. In the context of dysfunctional behaviours within the AIS environment, organisational culture and AIS technology are therefore proposed to mediate the effects of the determinants of intention. The interaction of these constructs is mapped in Figure 3.

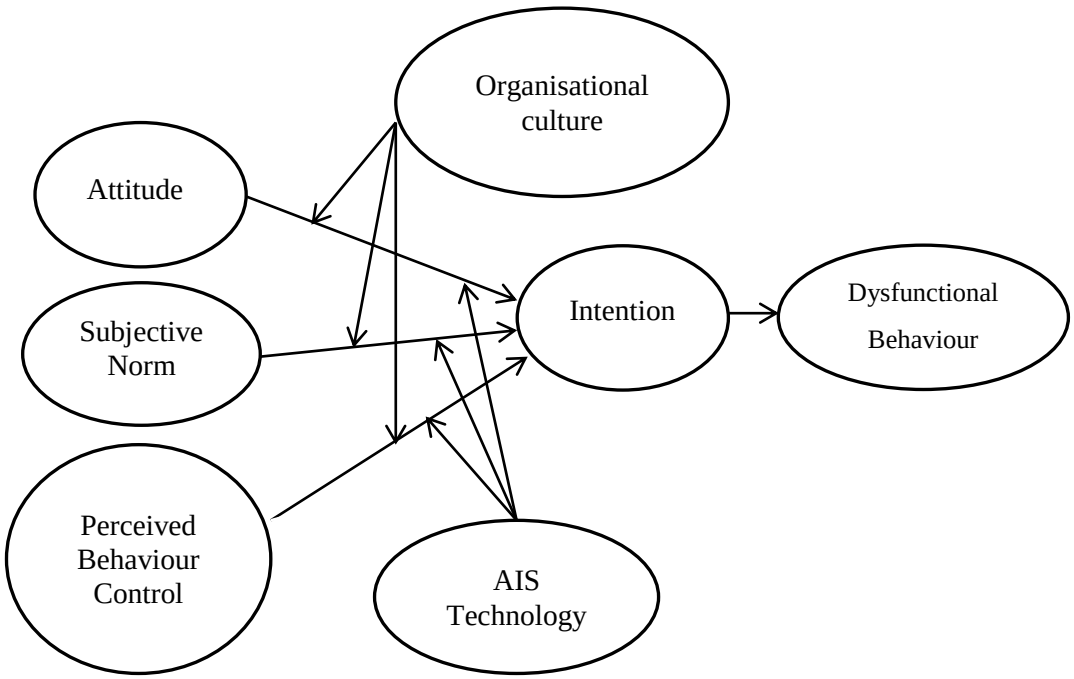


Figure 3: The interaction of Organisational Culture, AIS Technology and the TPB Constructs[6]. Adapted from Ajzen (1991).

2.6.1 Intention as a Predictor of Actual Behaviour

Intention is a good predictor of actual behaviour in both volitional and non-volitional settings, (Ajzen, 1991; Ajzen & Madden, 1986; Chang, 1998; Randall & Gibson, 1991). Intentions drive individuals to behave the way they do. The supposition is that intentions "…capture the motivational factors that influence a behaviour; they are indications of how hard people are willing to try, of how much of an effort they are planning to exert, in order to perform the behaviour."(Ajzen, 1991, p. 181).

[6] Given intention is found to be a good predictor of actual behaviour, intention-dysfunctional behaviour path is not examined in the scope of this study.

The essence of the intention-behaviour relationship is that the stronger the intention, the more likely the person will engage in the behaviour. This is illustrated in the many scholarly works of such as (e.g. in Venkatesh, Morris, Gordon, & Davis, 2003; Workman, 2005), that recorded a significant correlation between intention and actual behaviour. The longitudinal study by Venkatesh et al. (2003) further validated the influence of intention over actual behaviour in both voluntary and mandatory use of technology. In this respect, regardless of controllability, i.e., voluntary or mandatory behaviour, the use of intention as proximal behaviour can be justified.

2.6.2 Predicting the Intention: The Effects of Attitude, Subjective Norm and Perceived Behaviour Control

Attitude and subjective norm are two constructs that reflect an individual's dispositional judgment of behaviour with respect to their own and others' views. The attitude towards the behaviour (ATT) is one's evaluation of the tendency towards the intended behaviour (Ajzen, 1991; Ajzen & Madden, 1986); while the subjective norm (SN) represents social pressures that influence an individual to perform or not to perform a behaviour (Ajzen, 1991; Ajzen & Madden, 1986). The effect of social pressures is assimilated within the performer's salient belief, this is actualised into SN and later translated into intention and subsequent behaviours.

SN tends to correlate differently across different scenarios. Venkatesh et al. (2003) found that SN does not exert any significant influence over intention in the voluntary use of technology, but exhibits different correlations in a mandatory usage setting (see Table 5). One explanation for this variation can be found in the study of

Workman (2005), where SN and ATT together induced an individual to engage in misuse in a technology[7] practice. Where social pressure increases but the attitude towards using the technology is poor, there is a tendency to misuse technology. This aligns with the findings of Hansen, Møller Jensen, and Stubbe Solgaard (2004), Heinze and Hu (2009), Jimmieson, Peach, and White (2008), Yan and Sin (2013), that attitude and subjective norm significantly affect intention. The effects of attitude and subjective norm are hypothesised as follows:

H1: Attitude has a significant positive effect on intention.

H2: Subjective norm has a significant positive effect on intention.

In non-volitional behaviour, where complete control over the behaviour does not exist, the performer is likely to hold back on the intended action until sufficient resources and opportunities are available (Ajzen, 1991; Ajzen & Madden, 1986). This prompted the inclusion of the perceived behavioural control (PBC) construct into TPB to account for the (perceived) control over actual behaviour. The more the performer perceives to have control over the behaviour, the more inclined he/she is to engage in such behaviour.

PBC refers to the performer's perception of the ease or difficulty of performing the behaviour of interest (Ajzen, 1991). In essence, PBC explains the extent to which a performer views that an intended action requires effort. Such effort

[7] Workman (2005) found a curvilinear effect on intention when SN and ATT are analysed simultaneously through a hierarchical regression using quadratic terms. The study was conducted on the (mis)use of an expert decision support system (EDSS). The implication is that when a user interacts with an environment where the EDSS is largely used, the user is found to be pretending to use the technology, but ignoring all the benefits and outputs suggested by the system.

requires skills and resources to perform the behaviour which reflects the performer's internal locus of control (Rotter, 1960, 1966). Ajzen (2002a) added that intention is also dependent upon anticipated outcome contingencies, reflecting external locus of control. Ifinedo (2014) and Workman, Bommer, and Straub (2008) found that external locus of control and self-efficacy (internal locus of control) positively and independently relate to IS security compliance intention. These findings suggest that the more individuals perceive the outcome is within their control, the stronger their intention will be. In the context of insider dysfunctional behaviour, this is illustrated in the work of Cheng, et al. (2013) and Li, Zhang, and Sarathy (2010), where an increased probability of punishment discouraged potential IS abuse, although this was limited to the perception of punishment severity (the cost of security policy violation), rather than the certainty of being caught for such a violation.

These perspectives give rise to the notion that PBC is not a single construct, but rather a two-factor construct comprised of internal and external loci of control, where the perception of control over resources reflects the internal locus and the perception of control over outcome mirrors the external locus. Hence, this study hypothesises that:

H3a: Perceived control of behavioural outcomes has a significant positive effect on intention.

H3b: Perceived control of resources to engage in behaviour has a significant positive effect on intention.

Despite being supported by the theory of planned behaviour (TPB) the value of this theory has been challenged (e.g. Celuch, Goodwin, & Taylor, 2007;

Chang, 1998; Zolait, 2011). The antecedences of intention in TPB (attitude, subjective norms and perceived behavioural control) were found to be relatively unstable in many studies. A review of 185 independent studies by Armitage and Conner (2001) revealed that although TPB accounted for 39% of variances in intention, the subjective norm was found to be a weak predictor of intention. This is aligned with the findings of Chang (1998), but contradicts the work of Yan and Sin (2013) and Hansen, et al. (2004), where reference to others (subjective norm) was found to be a significant predictor of intention[8]. Similarly, Celuch, et al. (2007) and Zolait (2011) found that perceived behaviour control satisfies a two-factor, rather than a single construct.

Disparate findings in the many studies of TPB are attributable to a variety of reasons, such as the quality of measurement tools (Armitage & Conner, 2001), the type of behaviour, and the conditions in which the behaviour of interest is being reviewed. Where predictive efficacy of an established predictor-criterion relationship varies, there is an indication of a third variable that systematically changes the form or strength of the predictor-criterion relationship (Davis, 2004; Goltz & Smith, 2010; Sharma, Durand, & Gur-Arie, 1981; Walsh, Evanschitzky, & Wunderlich, 2008). Inclusion of this third variable, known as the moderating variable, can further enhance understanding of the phenomenon being studied (Walsh, et al., 2008) and explain a predictor-criterion relationship that seems to defy conventional wisdom, as highlighted by Posey, et al. (2011), Moore, et al. (2008), and Stanton and Stam (2006). In a computerised system, Posey, et al. (2011), Moore, et al. (2008), and

[8] Hansen, et al. (2004) found that attitude and subjective norm are strong predictors of intention. However, perceived behaviour control exhibits a non-significant effect on intention.

Stanton and Stam (2006) argued that, in certain circumstances, adding more stringent security controls to a system fails to suppress insider dysfunctional behaviour. In fact, the added security appears to foster system misuse. It is therefore critical to look at the moderating effects of third variables. In the current study, organisational culture and system complexity were identified as the moderating variables.

2.6.3 Moderating Effects of Organisational Culture

Musa (2011) argued that organisational culture is part of a formal control brought about by implementation of acceptable security and IT/IS usage policies. This creates a social bond (Cheng, et al., 2013; Lacey, 2010) between employees and the organisation and forms strong social ties that help to reduce deviations from conventional norms (Hu, et al., 2012; Lowry, et al., 2014; Terry, Hogg, & White, 1999). However, this bond is contingent to actual practices in the organisation. For example, non-compliance practices in the work environment are often viewed as an acceptable norm (see Lieberman, 2011) when such actions are routinised and widely performed, because it creates a culture of non-compliance in the organisation. In contrast, when policy-compliance practices are customary, any violation of established policies has a negative connotation that affects the individual's pre-dispositional cognitive assimilation. The effects of ATT, SN and PBC on intention are thus influenced by organisational culture in a way that can weaken or strengthen its effects, depending on the strength of the culture which is contingent to policy-compliant or non-compliant norms. Therefore, this study hypothesises that:

H4a: The relation between attitude and intention will be moderated by organisational culture, such that when organisational culture is strong, the relation between attitude and intention will be weaker than when organisational culture is weak.

H4b: The relation between subjective norm and intention will be moderated by organisational culture, such that when organisational culture is strong, the relation between subjective norm and intention will be weaker than when organisational culture is weak.

H4c: The relation between perceived control of behavioural outcome and intention will be moderated by organisational culture, such that when organisational culture is strong, the relation between perceived control of behavioural outcome and intention will be weaker than when organisational culture is weak.

H4d: The relation between perceived control of resources to engage in behaviour and intention will be moderated by organisational culture, such that when organisational culture is strong, the relation between perceived control of resources and intention will be weaker than when organisational culture is weak.

2.6.4 Moderating Effects of AIS Technology

Fortification of AIS technology by way of data storage, communication channels and software protections (through updates and patches) has become customary in attempts to alleviate risks. The use of an intrusion detection system (IDS) and the maintenance of user logs, either embedded within the AIS software or installed as part of the system's firewall, forms a set of defence mechanisms.

However, a predictable working pattern of AIS is likely to prompt insiders to behave dysfunctionally (Lynch & Gomaa, 2003; Lynch, 2006) because the outcomes of an input can be predicted with high precision.

In contrast, complex AIS can reduce the likelihood of dysfunctional behaviour. This is because system complexity introduces uncertainties (Alvarado-Valencia & Barrero, 2014) and interference (Post & Kagan, 2007) that act as barriers, thereby securing the AIS. These barriers create cognitive dissonance ("Cognitive dissonance," 2008) which affect attitudinal change and subjective norm, as well as reducing employee efficacy in exerting sufficient control over the resources to engage in dysfunctional behaviour; and limits their ability to anticipate an outcome of their behaviour. Therefore, the following hypotheses were tested to confirm the moderating effects of AIS complexity on the dispositional determinants of intention.

H5a: The relation between attitude and intention will be moderated by complexity of AIS technology, such that when complexity of AIS technology is high, the relation between attitude and intention will be weaker than when complexity of AIS technology is low.

H5b: The relation between subjective norm and intention will be moderated by complexity of AIS technology, such that when complexity of AIS technology is high, the relation between subjective norm and intention will be weaker than when complexity of AIS technology is low.

H5c: The relation between perceived control of behavioural outcome and intention will be moderated by complexity of AIS technology, such that when complexity of AIS technology is high, the relation between

perceived control of behavioural outcome and intention will be weaker than when complexity of AIS technology is low.

H5d: The relation between perceived control of resources to engage in behaviour and intention will be moderated by complexity of AIS technology, such that when complexity of AIS technology is high, the relation between perceived control of resources and intention will be weaker than when complexity of AIS technology is low.

The following chapter provides an overview of the research methodology used in this study, and describes the research design, instrument development, the sample and the sampling techniques, data collection and analysis procedures.

Chapter Three
Research methodology

3.1 Introduction

This research was a quasi-experimental quantitative research study, using a series of vignettes supplemented by a questionnaire to explore the research questions. The approach fitted the nature of the study that focused on prohibited behaviours in the accounting information system (AIS) usage policy of a corporation. The use of vignettes provided sufficient distance between the respondents and potential reprimand for their unwarranted actions (Crossler, et al., 2013), and at the same time, illuminated important features of sensitive information through depersonalisation (Schoenberg & Ravdal, 2000).

The procedures used to achieve the objectives of the study are detailed in the following sections. This chapter describes the research design, instrument development, sample and sampling technique, data collection and analysis procedures. The data analysis procedure has been arranged into two main sections: the preliminary data analysis, which includes the preliminary procedures to ensure the dataset was ready for statistical analysis and exploratory factor analysis, and the second section, which involves a two-stage structural equation modelling procedure as proposed by Anderson and Gerbing (1988), to assess the measurement model and the structural model. Each section is further described below.

3.2 Variables and Measurements

Four vignettes were constructed to incorporate the dysfunctional behaviours and relevant variables, particularly the exogenous constructs. The vignettes were based on the work of D'Arcy (2007), supplemented with references to dysfunctional

behaviour taxonomy as laid down by Stanton et al. (2005). This combination enabled a clearer picture of intensity and relevance of behaviours and associated variables.

The variables of theory of planned behaviour (TPB) were measured according to instruments developed by Azjen (1991), Chatterjee (2008), Thompson, Higgins and Howell (1991) and Venkatesh et al. (2003). These instruments were chosen because they exhibit high composite reliability values (ranging from 0.928 to 0.967) and convergent validity values (factor loading between 0.718 to 0.959) across the items measuring TPB constructs (e.g., Chatterjee, 2008). The items were further referenced to TPB scale development guides provided by Ajzen (n.d.-a, n.d.-b).

Organisational culture was measured according to instruments developed by van Muijen et al. (1999). AIS complexity was evaluated by adapting the instruments of Thompson et al. (1991) and Venkatesh et al. (2003) with some modifications to the wording to suit the context of the study.

3.2.1 Dysfunctional Behaviours

Stanton et al. (2005) presented a 6-modal[9] group taxonomy of behaviours in IS. These were: *intentional destruction*, *dangerous tinkering*, *detrimental misuse*, *naive mistake*, *basic hygiene* and *aware assurance*. In combination, these modal groups consist of 94 different employee behaviours, mapped against 2 vectors: *intention* and *computer skill*. Intentional destruction sits at one extreme end of the vector plane, and is associated with high malicious intention requiring relatively high

9 The term 'modal' is a category designation used by Stanton et al. to assign each behaviour to one of the six categories based on the greatest number of respondent (see Stanton, et al., 2005, p. 127)

computer skills. This type of behaviour includes intentional actions, such as deletions and modifications of data without appropriate or sufficient approval from authorised personnel. On the other hand, detrimental misuse normally requires less technical expertise, but includes harmful intention. Unauthorised access to records and escalated access privilege are two examples of how junior employees gain access to data for which they have no authority.

In contrast, naïve mistake implies no clear malicious intention and usually requires less computer skills. Password-sharing practices and leaving a workstation without logging out properly are two dysfunctional behaviours in this category. Similarly, dangerous tinkering is postulated not to have clear malicious intentions, however, this category normally demands high computer skills. Unauthorised installation of software and reconfiguration of network access for the purpose of making job tasks easier, without approval, are deemed to require relatively high computer skills without a clear malicious intentions.

Based on this taxonomy, 4 vignettes, comprised of 4 different themes, were adapted from the work of D'Arcy (2009); each fitted into Stanton's first 4 modal groups respectively. The last two groups of the taxonomy, basic hygiene and aware assurance were excluded, because the scope of this study was limited to dysfunctional behaviours[10]. Table 6 summarises the vignettes, the associated themes and the typologies of the taxonomy belonging to each vignette.

[10] Basic hygiene and aware assurance categories are security-compliance behaviours. Basic hygiene (low computer skill – good intention) includes employee compliance to computer security policy to maintain the confidentiality of their password. Aware assurance (high computer skill – good intention) looks into employee actions such as system penetration test.

Table 6

Vignettes and Behaviour Taxonomy

Vignette	Theme	Typologies in Taxonomy
Vignette 1: By chance, Catherine discovered a password that allowed her to access a restricted area of the payroll system of the company. This allowed her to see the salary paid to other employees. At the same time, she was preparing to ask for a raise. Prior to meeting with the management, she accessed and viewed the salaries of others in similar a position to hers. She used this information to determine how much increment to ask for.	Unauthorised access	Detrimental misuse
Vignette 2: Hashim prepares payroll records for the company's employees and therefore has a good access to the timekeeping and payroll system. He periodically changes the amount of hours-worked record of other fellow friends of him by rounding up their total overtime hours such as 39.5 hours to 40 hours.	Unauthorised modification	Intentional destruction
Vignette 3: Lee is given a laptop by the company that he can use while in the office as well as on the move. However, the laptop does not have software that allows him to tap into the production planning system that he is authorised to access through other computer terminals. He believes that software will make his work more efficient and effective. A request to the IT department to purchase the software is denied because it is too expensive. To solve the problem, Lee obtains an unlicensed copy of the software and personally installed into the laptop.	Unauthorised software installation	Dangerous tinkering
Vignette 4: Linda works in the marketing department and therefore has access to the company's customer account database. One day at the office, Linda's co-worker in the same department asked to borrow her password in order to access the customer database because she forgot her password. The system administrator who was in charge in resetting the password was on sick leave. Linda gave her password to the co-worker for her to access the customer account database.	Password sharing	Naive mistake

3.2.2 Intention, Attitude, Subjective Norm & Perceived Behavioural Control

Intention, attitude, subjective norm and perceived behavioural control are latent constructs that form the building blocks of TPB. These four constructs were

measured using scales adapted from Azjen (1991), Chatterjee (2008), Thompson et al. (1991) and Venkatesh et al. (2003). All items were measured on a 7-point Likert scale where 1 corresponded to "strongly disagree" and 7 corresponded to "strongly agree".

Table 7

Intention, Attitude, Subjective Norm and Perceived Behavioural Control

Constructs	Scales
INTENTION (Chatterjee, 2008; Venkatesh, Morris, Gordon, et al., 2003)	Int1: I intend to carry out a similar action in future. Int2: I predict I will carry out a similar action in future. Int3: I plan to carry out a similar action in future. Int4: If you are in X's situation, how likely are you to perform a similar action? Int5: All things considered, would you take the same action as X did?
SUBJECTIVE NORMS (Ajzen, 1991; Chatterjee, 2008; Venkatesh, Morris, Gordon, et al., 2003)	Sn1: People who influence my behaviour think that I should carry out such action. Sn2: People who are important to me think that I should carry out such action. Sn3: My fellow colleagues would themselves have carried out this action if they had been in my place.
ATTITUDE (Chatterjee, 2008; Venkatesh, Morris, Gordon, et al., 2003)	Att1: Carrying out such action is good. Att2: Carrying out such action is valuable.
PERCEIVED BEHAVIOURAL CONTROL (PBC-OutC) Perceived control over the outcomes of behaviour. (Thompson, et al., 1991; Venkatesh, Morris, Gordon, et al., 2003)	Pbc1a: Carrying out such action can decrease the time needed for my important job responsibilities. Pbc2a: Carrying out such action can significantly increase the quality of output of my job. Pbc3a: Carrying out such action can significantly increase the quantity of output of my job.
PERCEIVED BEHAVIOURAL CONTROL (PBC-Res) Perceived control over the resources to engage behaviour. (Ajzen, 1991)	Pbc1b: I have the resources necessary to carry out such action. Pbc2b: I have control over carrying out such action.

In previous studies, perceived behavioural control was viewed as a single construct. In this study however, perceived behaviour control was divided into two separate constructs from which the perception of control stems: one's (perceived) control over resources to engage in a given behaviour (Ajzen, 1991; Ajzen & Madden, 1986), and control over the outcome of such behaviour (e.g., Jensen & Patel, 2011; Phau & Ng, 2010). The constructs and their respective sets of scales are summarised in Table 7.

3.2.3 Organisational Culture

Organisational culture was measured according to the 4 dimensions (see Muijen, et al., 1999) of support, innovation, practice and performance. While van Muijen et al. evaluated the dimensions in 2 domains, descriptive (practice) and evaluative (value), the current study emphasised the descriptive side of the analysis. The actualisation of organisational values in members of the organisation is visible in the practices arising from group interaction (Bellot, 2011; Da Veiga & Eloff, 2010). Therefore the descriptive evaluation, which focuses on practice rather than values, presents an appropriate measurement of culture (Jung, et al., 2009). Table 8 depicts the dimensions and the scales used in the current study.

3.2.4 Accounting Information System (AIS) Technology

Features of accounting information systems (AIS) can change the way people behave towards the technology (e.g. Eggert & Serdaroglu, 2011; Harrison & Datta, 2007; Jon, Carter, & Zmud, 2005; Kim, Mannino, & Nieschwietz, 2009b).

Table 8

Dimensions of Organisational Culture

Dimensions	Scales
Support Dimension	**In regard to the support in your organisation, how many people...** Spp1: with personal problems are helped? Spp2: who wish to advance by promotion are supported by their superiors? **In regard to the support in your organisation, how often...** Spp3: is constructive criticism accepted? Spp4: do managers express concern about employees' personal problems? Spp5: are new ideas about work organisation encouraged? Spp6: do management practices allow freedom in work?
Innovation Dimension	**In regards to the innovation in your organisation, how often...** Inv1: does your organisation search for new markets for existing products? Inv2: is there a lot of investment in new products? Inv3: do unpredictable elements in the market environment present good opportunities? Inv4: does the organisation search for new opportunities in the external environment? Inv5: does the company make the best use of the employee skills to develop better products /services? Inv6: does the organisation search for new products/services?
Practice Dimension	**In regards to the practices in your organisation, how often...** Prc1: are instructions written down? Prc2: are jobs performed according to defined procedures? Prc3: does management follow the rules themselves?
Performance Dimension	**In regards to the goal / performance of employees in your organisation, how often...** Pfm1: is competitiveness in relation to other organizations measured? Pfm2: is individual appraisal directly related to the attainment of goals? Pfm3: does management specify the targets to be attained? Pfm4: is it clear how performance will be evaluated? Pfm5: are there hard criteria against which job performance is measured? Pfm6: is reward dependent on performance?

Note: The dimensions and scales are adapted from the work of van Muijen et al. (1999)

The more complex a system is, the less likely that it will be used (Kim, Mannino, & Nieschwietz, 2009a), and the higher the possibility of misuse (Shang, 2011; Workman, 2005). The effects of AIS technology on the predictors of intention

to engage in a dysfunctional behaviour can therefore be measured according to the complexity of the system.

While some scholars measure system complexity in terms of the system's attributes and specifications (e.g. Meyer & Curley, 1991; Meyer & Curley, 1995), an equally quantitative evaluation is via a mental model of users (Fioretti, 1999), because they have to exert sufficient effort to deal with such complexity (Fioretti & Visser, 2004; Hampton, 2005). Regardless of intricate technicality at the back-end, the front-end affects the perception of an easy-to-use system (Shang, 2011) because such interaction defines the amount of cognitive resources and skills required (Dong-Han, Jinkyun, & Wondea, 2011; Speier, 2006) to execute the actions.

Measuring the system's complexity from the cognitive aspect of the user rather than the system's attributes therefore presents a valid methodological approach, and questions of relevance and volitional control over the use of (or reluctance to use) AIS in this study's sample of companies, was no longer an issue. The mental model of the users formed a good construct against which the effects of their intentions could be measured via their cognitive representation of the system's complexity. As for the other latent constructs, AIS complexity was measured according to 4 scales, adapted from the instrument developed by Thompson et al. (1991) and Venkatesh, et al. (2003). This is illustrated in Table 9.

3.3 Sample

The sample of interest was middle managers of medium-sized enterprises (SMEs) in Malaysia. The list of companies was obtained from SME Corp of Malaysia, a central agency for SMEs, commissioned by the Malaysian government to formulate policies and coordinate programs for other agencies relevant to SMEs.

Table 9

Accounting Information System (AIS) Complexity

Construct	Scale
AIS complexity (Thompson, et al., 1991; Venkatesh, Morris, Gordon, et al., 2003)	Cpx1: My interaction with the system is clear and understandable. Cpx2: I find the system is easy to use. Cpx3: Using the system takes too much time from my normal duties. Cpx4: Using the system involves too much time doing mechanical operation (e.g. key in data)

A stratified sampling method was used to find clusters of companies in three sectors: service, retailing and manufacturing. These sectors were chosen for their volume of transactions and the extensiveness of AIS, suitable for quasi-experiments. Medium-sized companies were chosen for this study because they are sufficiently large to have developed a unique organisational culture, but not too large that the culture has become disparate from one department to another (Dent, 1991).

The middle manager group was selected as they had AIS user privileges or systems access which was not available to other operators, which presented an opportunity to misuse the system.

3.4 Data Collection

Two approaches were used for collecting data: a printed copy and an online version via a software program called Qualtrics. Companies previously shortlisted by the stratified random sampling method were further scrutinised for their respective email addresses. Those with registered email addresses ending in domain names "tm.net.my" and "jaring.net.my" were excluded from the email list because they

were default email accounts allocated to individuals or companies in Malaysia upon a successful application for internet access. In practice, this type of email address is not well monitored. Instead, printed copies of the questionnaire were mailed to these potential respondents together with reply-paid envelopes.

In order to mitigate against potential fatigue and sensitisation by repeated exposure to the instruments in a single study session (Chatterjee, 2008), each respondent was presented with one vignette so that both the printed and online versions contained only one vignette per response. Follow-up procedures in the form of one-time reminders were sent to all respondents two weeks after the initial contact. Data collection and reminder procedures were carried out in a way that maintained the anonymity of the respondents.

The data-collection phase commenced in February 2013 and ran for a period of 5 months. A total of 1000 printed copies were mailed and 380 email invitations were sent.

3.5 Pilot Study

The instrument was pre-tested on a smaller scale through email invitations. A two-stage pilot study was conducted using 4 vignettes per set in stage 1, and a single vignette per set in stage 2. Eight responses were collected from the preliminary pilot test and a further 38 (out of 40 sets distributed) were collected from the second stage conducted in Malaysia. Two questionnaire sets were not returned.

In stage 1, the overall content of the instrument was tested at a free accounting software workshop held at Edith Cowan University, on the Joondalup campus in December 2012. A further 6 online questionnaires containing all four vignettes were emailed to local (Australian) businesses. All 8 responses were used to evaluate the contents, structure and wording of the questionnaire. The comments and

responses were subsequently incorporated into the second stage, which comprised a single-vignette response per set. The responses from the second phase were used to test for instrument reliability. This two-stage pilot study is summarised in Table 10.

Table 10

Two-stage Pilot Study

	Number of vignettes per question set	Objectives	Number of valid responses (total)	Place of study
Stage 1	4	To test the overall structure of the instrument.	8 (8)	Perth region, Australia
Stage 2	1	To test item reliability and the structure of the revised instrument.	38 (40)	Northern region, Malaysia

The pilot study was necessary to test for the structure, contents and reliability of the instrument in relation to the local setting, particularly power distance, which is higher in a developing nation than in a developed country (Siew Imm, Lee, & Soutar, 2007). The dysfunctional behaviour modal group presented by Stanton et al., (2005) and included in the vignettes was tested in the pilot study to accommodate any cultural differences that may affect the behavioural taxonomy.

As a result of the pilot study (stage 1), two additional questions were added. These were: "If you were in X's situation, how likely would you be to perform a similar action?[11]" and "All things considered, would you take the same action as X

[11] *X* refers to the person in the vignette.

did?"[12] These two questions were designed to enhance the measurement of intention to engage in dysfunctional behaviours and resulted in 5 items for measuring intention, as shown in Table 7.

Principal axis factoring (PAF) with direct oblimin rotation (Schmitt, 2011) was also conducted on the pilot data. This exploratory factor analysis (EFA) was included to see whether the items in the instrument loaded into the component which they were predicted to measure. The results showed that the items had a set of satisfactory loadings on the components they were designed to measure, with no item load less than .50 on their respective parent construct.

Table 11

Reliability of Instruments in Pilot Study

	Scales	Cronbach's alpha	Cronbach's alpha on standardised items	*N* of items
Organisational Behaviour	Support	.956	.958	6
	Innovation	.969	.969	6
	Practice	.978	.978	3
	Performance	.968	.968	6
AIS	Complexity	.749	.773	4
Individual Factors	Intention[13]	.976	.976	5
	Attitude	.915	.915	2
	Subjective norm	.958	.957	3
	Control over outcome	.960	.962	2
	Control over resources	.897	.897	3

[12] ibid.
[13] Inclusive of 2 additional items suggested after Stage 1 of the pilot study.

As summarised in Table 11, the pilot study also showed that the instrument was sufficiently reliable for the actual study, with Cronbach's alpha ranging from .773 to .978, which is above the suggested minimum threshold of .70 (Nunnally & Bernstein, 1994).

3.6 Data Analysis Methods

In the first section, preliminary data analysis (PDA) was conducted to prepare the dataset for the main analysis. In the second section, exploratory factor analysis was run to determine appropriate factor-indicator segments. Partial least square structural equation modelling (PLS-SEM) was later used to build the second-order factor of organisational culture in section 3, and to analyse the full structural model in section 4 of the data analysis (Hair, Black, Babin, & Anderson, 2010). Figure 4 gives a brief overview of the data analysis sections and relevant procedures, with further details are provided in the following sections.

Generally, SEM is regarded as a suitable approach for finding a causal network (Chatterjee, 2008; Chin, 1998a; Rodgers & Guiral, 2011) for analysis in an experimental or quasi-experimental research design. PLS-SEM was preferred for this study because it places less emphasis on measurement scales, sample size and data distribution forms (Wold, 1985), as well as being prediction oriented (Hair, Ringle, & Sarstedt, 2011; Taskin, 2011). PLS-SEM also has an ability to mitigate issues of inadmissible solutions and factor indeterminacy (Fornell & Bookstein, 1982) with its underlying iterative algorithm, based on a series of ordinary least square (OLS) (Chin, 1998b). Hair, et al. (2011) also recommended PLS-SEM for situations where a latent variable comprises fewer than three items. These properties give PLS-SEM an advantage over covariance-based SEM. Given that the current study emphasises

the predictive ability of specified sets of constructs rather than confirming a theory, and two latent constructs (attitude and control over resource) were measured with only two items, PLS-SEM was deemed an appropriate method.

The PDA section involved an analysis and treatment of missing values (Allison, 2003; Brick & Kalton, 1996; Graham, 2012; Karanja, Zaveri, & Ahmed, 2013), tests for method bias (to test if mail and email data collection methods presented bias), common-method bias (Bagozzi & Yi, 1990; Doty & Glick, 1998; Podsakoff, MacKenzie, & Podsakoff, 2012), and non-response bias (Baruch & Holtom, 2008; Choung et al., 2013).

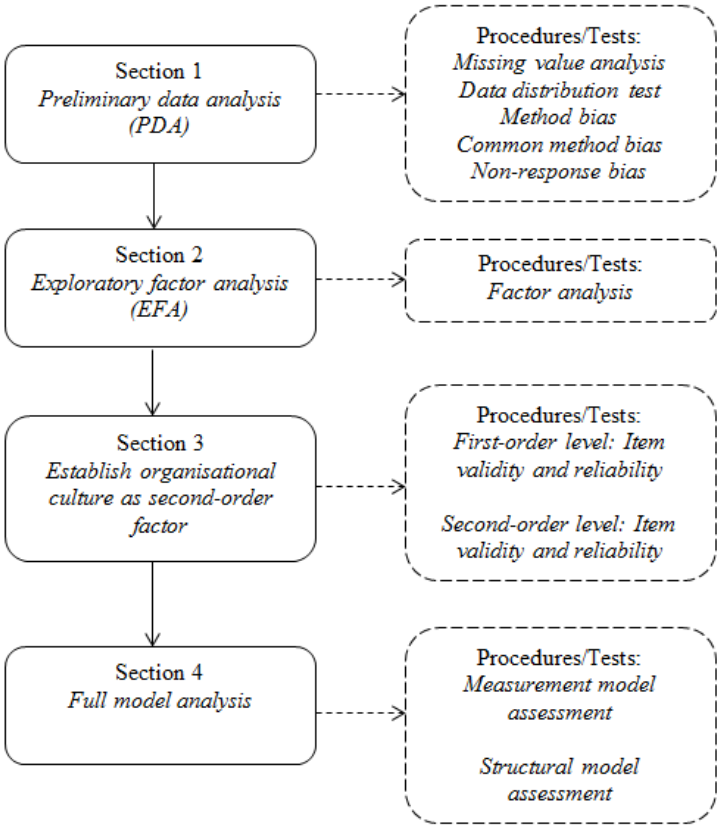


Figure 4: Data Analysis Sections.

A data distribution test was performed to determine which statistical approaches were suitable. If the data were normally distributed, the differences between early and late respondents, data collected by mail and email, and differences in intention of the four vignettes used, could be tested using parametric tests such as *t*-test (Allen & Bennett, 2010). However, non-parametric tests, such as Mann-Whitney U and Kruskal-Wallis, are more appropriate when the data are not normally distributed (Field, 2013; Pallant, 2010) or where data transformation generally results in a complicated interpretation of parameter estimates (Tabachnick & Fidell, 2007; Wang, 2012).

In the second section of the analysis, EFA was conducted to determine the latent constructs, which the instrument was designed to measure. Although the instrument used in this study was adapted from reliable studies, EFA was still required, especially in light of conflicting findings regarding perceived behavioural control as a single- or two-component construct (Ajzen, 2002a; Terry & O'Leary, 1995).

In the third section, data analysis was undertaken to build organisational culture (CULTURE) as a second-order latent variable. This was done by establishing reliability and validity at first-order factor and second-order factor, as proposed by (Chin, 1998a). The first-order factor measured 4 dimensions of organisational culture: innovation, practice, support and performance. Once the first-order factors were established, these latent constructs were used as the 4 indictors of CULTURE. The validity and reliability of CULTURE were again assessed (at second-order level) and generated a full model as shown in Figure 5.

In the final section of the analysis the full model was analysed. A 2-stage SEM approach (Anderson & Gerbing, 1988; Hair, et al., 2011) was used, which required an assessment of the measurement and structural paths of the research model. Tables 13 (page 88) and Table 14 (page 90) summarise the criteria used for the measurement and structural assessments.

As illustrated in Figure 5, the full research model depicts intention (INTENT) as a criterion variable; attitude (ATT), subjective norm (SN), perceived behaviour control over outcome (PBC-Out), and perceived behaviour control over resources (PBC-Res) as predictor variables; system complexity (COMPLEX) and organisational culture (CULTURE) as moderating variables; and vignette (VIGNETTE) as a control variable.

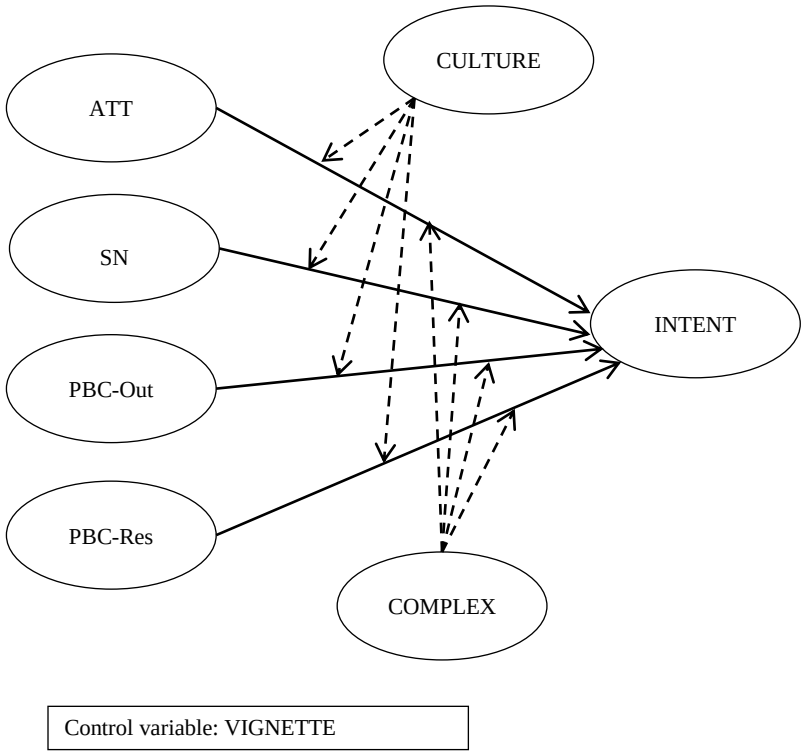


Figure 5: Full Model.

Consistent with the approach of Greene and D'Arcy (2010), Leonard, Cronan, and Kreie (2004), and in line with Ajzen's (2002a) proposition on heterogeneous behaviour types, an analysis of the full model was undertaken at aggregated level of behaviour and its subset level. Once the measurement model was found to be sufficiently robust, PLS-SEM was run for a combined dataset and separately for each type of dysfunctional behaviour. This approach provided a general understanding of dysfunctional behaviour at the grand structure, and illustrated how each predictor differs across behavioural typologies, while also addressing the methodological concerns raised by scholars (e.g. Crossler, et al., 2013; Guo, 2013; Posey, et al., 2013; Warkentin & Willison, 2009). For each data analysis section, purposes and procedures relating to the data analysis are highlighted in Table 12.

3.7 Primary Software Used

SPSS version 22 was used for the preliminary data analysis, while WarpPLS 4.0, a partial least square structural equation modelling (PLS-SEM) statistical program, was used to analyse the measurement and full structural model. Relative to covariance-based SEM, PLS-SEM offers many advantages, including less fatal errors in model identification and lower sensitivity to sample size (Hair, Black, Babin, Anderson, & Tatham, 2006). Hair, et al. (2006), and Hair, Ringle, and Sarstedt (2011) suggested that compared to covariance based SEM, PLS-SEM provides more reliable estimates for models comprising single- or two-item latent constructs. The robustness of PLS-SEM in providing reliable estimates have also

been evidenced in situations with non-normal data distribution (Reinartz, Haenlein, & Henseler, 2009; Ringle, Sarstedt, & Straub, 2012).

PLS-SEM was preferred for this study for the reasons outlined above. The ability of WarpPLS to provide visual moderating effects on the relationship between the latent constructs made this particular program useful for the current study.

An additional feature of the software which further enhances the current study is its ability to automatically test for correct hypothesised causality flow (a test of Simpson's paradox[14] issue) and provide *p*-values for factor loadings, thereby eliminating the need to check for *t*-statistics to determine the significance of factor loadings (Kock, 2013). The factor loadings, cross-loadings and *p*-values provided by the software also added to the assessment of the measurement model before analysing the structural path.

[14] Simpson's paradox or Yale paradox happens when the hypothesised causality flow is on opposite direction of what is indicated by statistical results. Kock (2013, 2015) suggests *weight loading sign* (WLS) be used to check for potential causality issues. A negative WLS indicates a causality issue in the path modelling. In this study, WLS for all paths in the full model showed positive values, indicating that Simpson's paradox was not a concern.

Table 12

Data Analysis Sections and Procedures

Section	Purpose	Procedure
Preliminary data analysis (PDA).	To prepare data for subsequent analysis	Missing value analysis using expected maximisation method (Karanja, et al., 2013; Little, 1988; Rubin, 1976). Common method bias using Harman's single factor score (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003; Podsakoff, et al., 2012; Siponen, et al., 2014). Data distribution test (normality test) using Kolmogorov-Smirnov and Shapiro-Wilk tests. Non-response bias test by splitting dataset into early and late respondents and later the difference was tested using Mann-Whitney U test (see Fullerton, Kennedy, & Widener, 2013; Leslie, 1972; Mehta & Hall, 2014; Wallace & Sheetz, 2014). Data collection method bias (mail and email) test using Mann-Whitney U test (Allen & Bennett, 2010; Field, 2013).
Exploratory factor analysis (EFA).	A preliminary procedure to determine items for each latent construct.	Factor analysis using principal axis factoring (Allen & Bennett, 2010; Hair, et al., 2010; Pallant, 2010; Schmitt, 2011)
Establish higher-order construct of organisational culture (CULTURE).	To establish CULTURE as second-order factor to be used as a moderating variable in the final model.	Assessments of reliability and validity at both lower-order and higher-order factors (Chin, 1998a).
Full model analysis.	The main analysis which includes all variables.	A 2-stage PLS-SEM approach was used (Anderson & Gerbing, 1988; Hair, et al., 2011).

3.8 Preliminary Data Analysis

In survey research bias complicates interpretation and limits the usefulness of the findings. Bias can stem from instrument design, the participants, or the way the research is administered, resulting in missing values and systematic variations in measurement approach. Procedural and/or statistical controls (see Doty & Glick, 1998; Podsakoff, et al., 2003) are required to detect the presence of bias, and where present, to control its effects on the statistical results. This section discusses the treatment and procedures used to address missing values and any potential bias.

3.8.1 Treatment of Missing Values

Missing values can hinder certain statistical procedures and distort the survey estimates (Bennett, 2001; Brick & Kalton, 1996). In survey-based studies this can occur at unit and item levels. Unit-level missing values is a result of the respondents' failure or refusal to respond to the survey (also known as a non-response), while at item level, this happens when respondents do not answer certain question(s) in the survey instrument (Karanja, et al., 2013). Missing values can potentially reduce statistical power and artificially increase standard errors of statistical procedures (Rigdon, 1998).

Missing values can take the form of missing completely at random (MCAR), missing at random (MAR), or not missing at random (NMAR) (Little, 1988). Little suggested that MCAR occurs when the "missingness" does not depend on the value of other variables in the dataset. On the other hand, MAR refers to a missing pattern that is traceable or predictable from other variables (Bennett, 2001). When the missing data is not missing at random and is directly related to the

requested data, this is called NMAR. Identification of missing data patterns is crucial to decide on the most suitable treatment for imputing the missing values.

Issues concerning missing values prompted the American Psychological Association (APA) Task Force on Statistical Inference (Wilkinson, 1999) to urge researchers to report on the presence and treatment of missing data. In particular, Hair, et al. (2010) reiterated the importance of recognising missing data patterns at item level, and choosing relevant remedial actions on the basis of maintaining original data distribution.

Using a 20% missing-value criterion as suggested by Karanja, et al. (2013), 19 cases with missing values were included in the data analysis. Twenty percent of missing data was the maximum cut-off rate that subsequent statistical remedies could effectively impute without altering the original data distribution (Hair, et al., 2006) or yield problematic parameter estimates (Scheffer, 2002).

Expected maximum (EM) method was used to deduce the most likely values for the missing data. This method was chosen because EM provides unbiased parameter estimates (Bennett, 2001) for MCAR missing data patterns (Karanja, et al., 2013). For EM to provide reliable estimates, Little's missing-completely-at-random test (Little, 1988) was conducted to see if the missing values were indeed MCAR. This brought an objective approach to the missingness pattern analysis.

EM is primarily based on Rubin's (1976) inference framework which is still used today (Schafer & Graham, 2002). The algorithm of this framework consists of 2 steps: expectation (E-step) and maximisation (M-step). In the E-step, the algorithm imputes "best-guess" values based on the distribution of missing data values and existing data points; while the M-step maximises the likelihood of obtaining new

parameter estimates using the values produced in the E-step (Bennett, 2001). This procedure is repeated until changes in the parameter estimates from one iteration to another is negligible (converged).

3.8.2 Common Method Bias

Common method bias (CMB) is the magnitude of the discrepancies between the observed and true relationships between the constructs of interest (Doty & Glick, 1998). In CMB, variations in the constructs are attributable to the measurement method rather than the construct's measurement, and undermine the true relationships between the latent variables. Following the guidelines of Podsakoff, et al. (2003) and Podsakoff, et al. (2012), both procedural (using psychological separation technique) and statistical (using Harman's single factor score) methods were used to control and detect CMB (see Siponen, et al., 2014).

In terms of procedural control, four vignettes were embedded in the survey instrument as a psychological separation technique. This technique was used to put a comfortable distance between the respondent and the person engaging in dysfunctional behaviour. The psychological separation was also chosen because the criterion variables in this study could not be sourced from other avenues for the given predictor variables.

Harman's single-factor score technique was later used to statistically check for the presence of CMB. Consistent with Schmitt (2011), a principal axis factoring (PAF) extraction method was used, whereby all manifest variables were constrained to a single common factor. Based on unrotated factor solution, the presence of CMB in the data can be detected if the procedure yields one general factor accounting for

majority (i.e. more than 50%) of variance (Doty & Glick, 1998; Hu, et al., 2012; Podsakoff, et al., 2012).

3.8.3 Data Distribution

Although PLS-SEM does not necessitate datasets to be normally distributed, a data distributional test is nevertheless needed to determine subsequent methods of analysis. For example, a dataset which does not conform to normal distribution assumptions requires a non-parametric class of tests. Although data transformations are recommended (Field, 2013) to achieve normality, these transformations can change data space, which complicates interpretation of the results (Pallant, 2010; Tabachnick & Fidell, 2007). Pallant (2010) therefore recommended non-parametric tests be used, which are comparable to parametric tests, because in such cases "…non-parametric tests may have greater power than the corresponding parametric test" (Howell, 2013, p. 659).

Both Shapiro-Wilk and Kolomogorov-Sminov tests were conducted to check if the dataset conformed to normality assumptions. Where datasets were found to be non-normally distributed, tests for significant differences in early and late responses (used to test for the presence of non-response bias), and differences in intention between groups were checked using non-parametric tests. Depending on the number of the sample group to be tested, Kruskal-Wallis (for more than 2-sample groups) and Mann-Whitney U (for 2 samples groups) were appropriate to test for group differences respectively.

3.8.4 Non-response Bias

Non-response bias (NRB) is a form of missing values at unit level. Van der Stede, Young, and Chen (2005) emphasised that the sample size is more critical than NRB, particularly when the response rate is high (Leslie, 1972; Mao & Palvia, 2008). For example, Mao and Palvia (2008) had a response rate of more than 80% where NRB could be safely ignored. In accounting however, the response rate is usually 25% or lower (Smith, 2011), which dictates that NRB be adequately addressed (Gorla & Somers, 2014), as in Lin and Huang (2010).

In order to address NRB the dataset was split into two subsets: early and late responses. Late responses were treated as a proxy for non-responses and were later compared to see if there was any significant difference between the two data subsets (see Fullerton, et al., 2013; Leslie, 1972; Mehta & Hall, 2014; Wallace & Sheetz, 2014). The split datasets were subjected to a Mann-Whitney U test. NRB is not a concern when the test yields no significant differences between two datasets, as was the case in this study.

3.8.5 Data Collection Method Bias

In order to detect bias in the data-collection methods, a Mann-Whitney U test was performed on each variable to find significant differences between the responses received via email and those received by mail. A significant result requires statistical control because there is evidence of systematic method bias, while a non-significant result is an indication that the responses from two data-collection methods are similar.

3.8.6 Exploratory Factor Analysis

Exploratory factor analysis (EFA) was conducted using SPSS version 22. The extraction method was principal axis factoring (PAF) with direct oblimin (orthogonal) rotation (Schmitt, 2011). Orthogonal direct oblimin rotation was used because the method represents reality in a behavioural study where factors are allowed to correlate, and reduces potential under-factoring while yielding a similar pattern matrix as other oblique rotations such as quartimin and promax (Treiblmaier & Filzmoser, 2010). Items with minimum factor loadings of .50 on their respective parent construct and lower cross-loading on other constructs were maintained (see Hair, et al., 2006; Siponen, et al., 2014). This was further checked against Eigenvalues and scree-plots (Allen & Bennett, 2010; Pallant, 2010) to determine the appropriate number of factors to be retained.

Kaiser-Meyer-Olkin (KMO) and Bartlett's tests of sphericity were also used to check that the factor solutions were appropriate. KMO values close to 1 indicate relatively compact patterns of correlation, a sign that the factor analysis provided distinct and reliable factor solutions (Pallant, 2010). Kaiser (1974) suggested KMO values of .50 or more are acceptable, while Field (2013) considered values between .70 and .80 as good.

Bartlett's test on the other hand, checks whether a variable's correlation matrix is an identity matrix, which means all correlation coefficients are zero (Field, 2013). Given that certain relationships between variables are anticipated, Bartlett's test has to be significant ($p < .05$) to be acceptable (Allen & Bennett, 2010). Once these qualities are established, the factor solutions can be used for further analysis.

3.9 Partial Least Square Structural Equation Modelling (PLS-SEM) Stage 1: Assessing the Measurement Model

WarpPLS 4.0 was used as the primary PLS-SEM software to analyse both the measurement and the structural model, to establish second-order factor (CULTURE), and to analyse the full model for this study. The measurement model was assessed according to criteria drawn from the work of Geffen and Straub (2005), suggestions by Anderson and Gerbing (1988), Chin (1998b), and Hair, et al. (2011). These criteria require statistically acceptable levels of discriminant validity and convergent validity, achieved through average variance extracted (AVE) assessments and inter-construct correlation, item loadings and cross-loadings with their respective *p*-values. Effectively the methods and criteria represent an instrument's validity assessment and thus forms the basis for measuring model adequacy (Moqbel, 2012).

Multicollinearity was also checked to ensure the quality of the measurement model, and reflective latent constructs were determined at this stage to ensure the validity of the structural model parameter estimates in stage 2.

3.9.1 Reliability and Validity

Item reliability was assessed according to individual item standardised loading on parent factor. Hair, et al. (2010) suggested that an item is reliable when the loading is equal to or more than .50. At the latent construct level, Cronbach's alpha and composite reliability, with a threshold set to .70 (Fornell & Larcker, 1981; Ifinedo, 2014), were used to assess reliability. An instrument which registers a value above the minimum .70 cut-off provides a consistent measurement (Rizzuto, Schwarz, & Schwarz, 2014; Tavakol & Dennick, 2011) and is therefore considered reliable. However, Hair, et al. (2011) supported the use of composite reliability over

Cronbach's alpha in PLS-SEM for measurement model assessment. This is because "…composite reliability does not assume all indicators are equally reliable, …rather (the method) prioritises indicators according to their reliability estimate" (Hair, et al., 2011, p. 145). In this study, both Cronbach's alpha and composite reliability were reported.

As reliability does not necessarily convey validity, the square-root of AVE and factor loadings were used to test for validity (Chin, 1998b; Hair, et al., 2011). Validity is concerned with the inter-relatedness of the items measuring intended latent traits or constructs. An item is valid if it meets both convergent validity and discriminant validity assessments.

Theoretically, an item is said to have sufficient convergent validity when it measures the latent construct for which it was designed. In order to meet this criterion, convergent validity for the items in this study was assessed through their factor loadings. Items with high loading (> .50) on its parent construct (Hair, et al., 2010; Kline, 2010; Schumacker & Lomax, 2012) and with low cross-loading on other factors support good convergent validity. Kock (2013), and Schumacker and Lomax (2012) proposed that these loadings be assessed for statistical significance (*p*-values ≤ .05) because the *p*-value is used as a validation parameter in confirmatory factor analysis. In addition, Fornell and Larcker (1981) suggested an AVE cut-off point of .50 for good convergent validity.

An item is said to have adequate discriminant validity when it does not measure a construct other than that for which it was designed. Failure to establish sufficient discriminant validity can lead to a questionable conclusion, such as whether a hypothesised structural path in a research model is real or the result of

statistical discrepancies (Farrell, 2010). Consistent with Farrell (2010), Fornell and Larcker (1981), Hair, et al. (2006), and Kock (2013), AVE was also used to assess discriminant validity in the current study. In its basic form, AVE dictates the average variances that a latent construct is able to explain by its observed variables (Farrell, 2010; Hair, et al., 2006). For good discriminant validity the square-root of AVE for each latent variable has to be higher than the correlation of the construct with other latent variables (Fornell & Larcker, 1981; Kock, 2013).

Collinearity amongst the variables was also assessed. Although Hair, et al. (2011) suggested that collinearity is not an issue with a reflective model (with the exception of a formative measurement), and partial least square (PLS) algorithm is sufficiently robust to deal with collinearity (Kroll & Song, 2013; Westlund, Källström, & Parmler, 2008), multicollinearity can still dramatically reduce estimators' efficiency (Kenett & Salini, 2011). For this reason, vertical (or predictor-predictor latent variable collinearity), and lateral Collinearity (or predictor-criterion collinearity) were both assessed through average variance inflation factor (AVIF) and average full collinearity variance inflation factor (AFVIF). Kock and Lynn (2012) proposed AVIF and AFVIF cut-off points of 3.3 as ideal and 5 as acceptable. They concluded that, where values exceeded these limits, it is an indication of multicollinearity in the instrument and re-examination of the indicators' (observed variables) factor loadings is required. However, a more relaxed cut-off point of lower than 10 is also acceptable in a multivariate analysis (Hair, et al., 2010). The reliability and validity criteria used in this study are summarised in Table 13.

3.9.2 Reflective Latent Constructs

Prior to testing a model in PLS, the nature of the latent constructs must be determined, i.e. whether they are reflective (i.e. changes in the latent constructs are reflected in their indicators) or formative (i.e. changes in the latent constructs are caused by their indicators). PLS-SEM uses slightly different methods to produce outer model estimates (measurement model) for reflective and formative latent constructs. For a reflective latent construct, PLS-SEM computes *outer loadings* between the latent construct and its indicators, with the latent construct as an independent variable and the indicators as dependent variables. In a formative latent construct, *outer weights* are calculated using the indicators as independent variables and the latent construct as the dependent variable. Incorrect specification of the latent construct can undermine its content validity, misrepresent a structural model, and result in less useful theories for both researchers and practitioners (Coltman, Devinney, Midgley, & Veniak, 2008).

The nature of a construct can be established through theoretical and empirical assessment of its properties. In regard to theoretical assessment, a construct is said to be reflective when it exists independently of the indicators measuring them, when causality flows from the construct to the indicators, and the indicators are interchangeable, i.e. adding or dropping an indicator does not change the conceptualisation of the latent construct (Bagozzi, 2007; Chin, 1998b; Jarvis, Mackenzie, Podsakoff, Giliatt, & Mee, 2003; Rodgers & Guiral, 2011).

From an empirical perspective, reflective constructs can be determined by the intercorrelation and validity of indicators according to Cronbach's alpha and AVEs (Coltman, et al., 2008). The indicator-construct causality flow can be further

checked using weight-loading signs (WLS). A negative WLS indicates a Simpson paradox, which means a hypothesised indicator-construct link is impossible or reversed (Kock, 2013; Wagner, 1982). The latent constructs in this study were assessed using the above approaches to determine whether they were reflective or formative. Table 13 summarises the criteria used for assessment in the measurement model.

Table 13

Measurement Model Criteria

Assessment	**Criterion**	**Note**	**Reference**
Item Reliability	Individual item standardised loading on parent factor.	Min. of .50	Hair et al. (2010)
Convergent Validity	Individual item standardised loading on parent factor, and loadings with sig. *p*-value	Min. of .50 $p < .05$	Hair et al. (2010) Gefen and Straub (2005)
	Composite reliability	> .70	Fornell and Larcker (1981) Nunnally and Bernstein (1994) Hair et al. (2010)
	Average variance extracted (AVE)	> .50	Hair et al. (2010) Urbach and Ahlemann (2010)
Discriminant Validity	Square-root of AVE	More than the correlations of the latent variables.	Hair et al. (2010)
Reliability	Cronbach's alpha	> .70	Nunnally and Bernstein (1994) Urbach and Ahlemann (2010) Hair et al. (2010)
	Variance inflation factor (VIF)	< 10 < 5.0 < 3.3 (ideal)	Hair et al. (2010) Kock and Lynn (2012)

Nature of Construct	Formative / reflective	Theoretical assessment Indicator inter-correlation Weight loading sign	Chin (1998a) Coltman, Devinney, Midgley, and Veniak (2008)

3.10 Partial Least Square Structural Equation Modelling (PLS-SEM) Stage 2: Assessing the Structural Model

Once the effect was established and the measurement model was found to be adequate, the structural model was assessed. The criteria used to assess the structural model are described in the following sections. Table 14 provides a summary.

3.10.1 Coefficient of Determination, R^2

Breiman and Friedman (1985), and Chin (1998b) suggested that the R^2 criterion is critical to evaluate a structural model. R^2 measures the amount of variation in dependent latent variables that have been accounted for by predictor latent constructs (Mohamadali, 2012). R^2 values of .75, .50 and .25 (and lower) are considered substantial, average and weak respectively (Hair, et al., 2011).

3.10.2 Predictive Relevance, Q^2

Predictive relevance, Q^2, measures how well-observed values are reconstructed by a given model and its parameters (Chin, 1998b). This is because Q^2 "…builds on a sample re-use technique, which omits a part of the data matrix, estimates the model parameters, and predicts the omitted part using the estimates"

(Hair Jr, Sarstedt, Hopkins, & Kuppelwieser, 2014, p. 113). Q^2 becomes larger when the difference between predicted and original values gets smaller, hence the model's predictive relevance.

3.10.3 Effect Size, f^2

Cohen (1988), Hair Jr, et al. (2014), and Lowry and Gaskin (2014) insisted that researchers report on effect size to measure the relative impacts of predictor variables on criterion variables. While the impact can be statistically significant (i.e. *p*-value $\leq$ .50), it can also be too weak from a practical standpoint (Kock, 2013). Cohen (1988) considered f^2 values of .02, .15 and .35 to be small, medium and large respectively.

3.10.4 Path Coefficient

Path coefficients in a model indicate the magnitude and direction of relationships. Many PLS-SEM software programs only provide path coefficients, *t*-statistics and standard errors, while *p*-values of the path coefficients are generally left to the researcher to estimate. WarpPLS however, provides the path coefficients together with associated *p*-values, which are more meaningful for hypothesis testing (Kock, 2013). In this study, the path coefficients were assessed according to their values and associated *p*-values. Chin (1998a) proposed standardised coefficients of .20 as a minimum accepted value, with a preferred value of .30. Table 14 summarises the criteria used to assess the structural model.

Table 14

Structural Model Assessment Criteria

Criterion	Note	Reference
Coefficient of determination, R^2	.67 substantial .33 average .19 weak	Chin (1998b)
Predictive relevance, Q^2	> 0 Stone-Geisser test	Geisser (1975) Stone (1974)
Effect size, f^2	.02 small .15 medium .35 large	Cohen (2013)
Path coefficient	Magnitude Sign p-value Standardised coefficient .20 acceptable .30 ideal	Hair et al. (2010) Chin (1998a)

3.11 Organisational Culture Variable

Organisational culture (CULTURE) was included in the final model as a higher-order latent variable. This was done to assess reliability and validity at both sub-scale (lower-order) and higher-order levels (Chin, 1998a) using similar criteria to the measurement model assessment summarised in Table 12. As postulated by Hair et al. (2006), higher-order factors provide several advantages, including increased parsimony and reduced complexity of a research model, by illuminating only relationships of interest.

Given the objective of this study was to look at the interaction effects of organisational culture with individuals' behavioural predispositions, the use of a higher-order latent variable in this context was appropriate.

3.12 Control Variable

As this study uses four different vignettes, the differences between dysfunctional behaviour dimensions in each vignette can influence the hypothesised relationships amongst the latent variables. This is because one type of behaviour can form an alternative of or be reciprocal to other actions (see Dalton & Todor, 1993), which should prompt control of the behaviour type in the structural analysis. Similar methodological concerns were also raised by Crossler, et al. (2013), Guo (2013), and Posey, et al. (2013). Accordingly, the differences in the vignettes were tested and controlled to eliminate potential bias from extraneous variables (see Kock, 2011). This procedure allows for proper observation of the true relationship in a given model (Mehta, 2001; Pole & Bondy, 2010). A Man-Whitney *U* test was conducted to test for differences, and VIGNETTE was introduced into the full model as a control variable.

3.13 Full Model Analysis

A full model analysis (with "vignette" as a control variable) was run on the combined dataset (N = 387) to provide a general understanding of dysfunctional behaviour at grand structure (see Ajzen, 2002a). A separate PLS-SEM was later conducted to investigate how the effects of predictors of intention differ across the subsets of dysfunctional behaviour. This illuminated the influence of behaviour dimensions (malicious-neutral intent, and low-high computer skill) on the strength of the structural paths in the model.

Chapter Four
Results

4.1 Sample Descriptive Statistics

Out of 1380 surveys mailed and emailed, 387 useable responses were collected, representing 23% from email (89 responses out of 380 email invitations[15]) and 30% from mail (298 returned from 1000 mailed[16]). The overall response rate was 28%, which is considered satisfactory for a survey-based study. Baruch and Holtom (2008) conducted an extensive review of 1607 journal articles and found that an average response rate for an organisational research survey was 36%, with a standard deviation of 18.8. Other studies suggested mailed survey response rates could be as low as 21%, and even 10% for email-based surveys (see Bye, Horverak, Sandal, Sam, & van de Vijver, 2014; Hu, et al., 2012). The data collection took place over a 5-month period beginning in February 2013. A description of the responses is shown in Table 15.

4.2 Preliminary Data Analysis

4.2.1 Treatment of Missing Values

Using a 20% cut-off point for missing values (see Karanja, et al., 2013), 19 cases were included in the analysis and an expected maximisation (EM) procedure

[15] 91 responses were recorded for the email-based survey. Two responses were excluded from the subsequent analyses because substantial data were missing (see Brick & Kalton, 1996; Hu, et al., 2012).

[16] 321 responses were received through the mailed survey. 23 responses were considered invalid because of a large percentage of missing data (see Bennett, 2001) that can bias the final results.

was used to impute missing values. The results showed that the missing value pattern was one of missing completely at random (MCAR), as supported by Little's non-significant MCAR test (χ^2 = 707.52, *df* = 654, *p* = .072). The imputed values could therefore be used in subsequent analyses.

Table 15

Sample Descriptive Statistics

	Vignette 1 Detrimental misuse	Vignette 2 Intentional destruction	Vignette 3 Dangerous tinkering	Vignette 4 Naïve mistake	Total
Male	31	42	40	28	141
Female	74	70	58	44	246
Total	105	112	98	72	387
Age group:					
20 - 30	72	70	54	42	238
31 - 45	33	40	40	30	143
> 45		2	4		6
	105	112	98	72	387

4.2.2 Data Distribution Test

At univariate level data violates the assumption of normality as shown by Shapiro-Wilk and Kolomogorov-Smirnov tests, *p*-value < .05. Although data can be transformed to approximate normal distribution, the procedure can result in a complex interpretation of statistical results (Pallant, 2010; Tabachnick & Fidell, 2007). Therefore, Kruskal-Wallis and Man-Whitney *U* were used to test for group differences in the preliminary data analysis stage. These tests are equivalent to *t*-test in parametric procedures.

4.2.3 Test for Common Method Bias

Harman's single-factor score was used to test for the presence of common method bias (CMB) (see Podsakoff, et al., 2003; Podsakoff, et al., 2012; Siponen, et al., 2014). By constraining (unrotated) factor extraction to one factor, the common method bias is said to be present if the variance accounted for by a single factor is higher than 50% (Doty & Glick, 1998; Hu, et al., 2012; Podsakoff, et al., 2012). In this study the results showed a single factor solution accounted for only 26% of the total variance, suggesting that CMB was not a concern.

4.2.4 Test for Non-response Bias

A Mann-Whitney *U* test was performed on split datasets (early and late responses) for every variable in the current study (see Fullerton, et al., 2013; Leslie, 1972; Taskin, 2011; Wallace & Sheetz, 2014). The results showed no significant difference between early and late responses for each variable, thereby confirming that the non-response bias (NRB) was not a concern.

4.2.5 Data Collection Method Bias

The dataset was again subjected to a Mann-Whitney U test to find if the data collection methods (email and mail) presented systematic differences between any of the variables. The dataset was split between email (n = 89) and mail (n = 298), and a Mann-Whitney *U* test was run on each variable. The results indicated no significant difference between responses received by email and by mail for every

variable, and consequently, data collection method bias did not pose a concern in this study.

4.2.6 Exploratory Factor Analysis

Exploratory factor analysis was conducted using principal axis factoring (PAF) with direct oblimin rotation (Schmitt, 2011; Treiblmaier & Filzmoser, 2010). Data factorability was found to be adequate with *KMO* = .86, and significant Bartlett's test of sphericity, $p < .001$, (Allen & Bennett, 2010; Field, 2013; Kaiser, 1974). Ten factors were identified as underlying latent constructs from 40 items based on Eigenvalues (Allen & Bennett, 2010; Field, 2013), and an assessment of the scree-plot (Cattell, 1966) shown in Figure 6. With the exception of *support5* and *performance1*, items with minimum factor loadings of .50 on their respective parent construct and lower cross-loadings on other constructs, were maintained (see Hair, et al., 2006; Siponen, et al., 2014). Items *support5* and *performance1* had loadings of less than .50 as shown in Appendix 1, and were dropped from subsequent analyses. The factor analysis was run again without these two items (*support5* and *performance1*).

A final 10-factor model accounted for 67.05% of variances, as shown in Table 16. These factors included the 4 dimensions used to measure organisational culture which are support (5 items), innovation (6 items), practice (3 items) and performance (6 items). The other 6 factors are AIS complexity (4 items), intention (5 items), attitude (2 items), and subjective norm (3 items), and perceived behavioural control (PBC) was split into two constructs. The preliminary result is consistent with Ajzen (2002a), and Pavlou and Fygenson (2006), that PBC is comprised of two separate constructs, although it can be unitary at a higher-level factor. This is further

supported by the notion of locus of control in PBC, which is a relative measure of control an individual has over resources to perform the behaviour, and includes self-efficacy (see Celuch, et al., 2007; Curtis & Payne, 2008; Heinze & Hu, 2009) and control over the outcomes of the behaviour, proxied as anticipated benefits (see Kim, Hornung, & Rousseau, 2011). A closer look at the items revealed that *control1*, *control4* and *control5* were related to the resources available to the respondents, while *control2* and *control3* focussed more on the outcomes of a given behaviour. Therefore PBC was maintained as two constructs, namely *perceived control over resources* (PBC-Res – 3 items) and *perceived control over outcomes* (PBC-Out – 2 items). This structure was further confirmed in the measurement model assessment section, where reliability, convergent and discriminant validities were analysed.

Table 16

Total Variance Explained

Factor	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total
1	10.862	27.155	27.155	10.639	26.598	26.598	8.354
2	7.900	19.751	46.906	7.518	18.796	45.394	5.539
3	2.217	5.543	52.45	1.911	4.777	50.171	1.947
4	1.747	4.366	56.816	1.405	3.514	53.684	6.915
5	1.602	4.005	60.821	1.217	3.043	56.727	2.316
6	1.388	3.471	64.292	1.058	2.644	59.372	5.109
7	1.299	3.246	67.539	0.931	2.328	61.699	3.423
8	1.097	2.743	70.281	0.816	2.041	63.74	3.774
9	1.094	2.486	72.767	0.73	1.824	65.564	6.830

10	1.056	2.390	75.157	0.596	1.490	67.054	3.385
11	0.802	2.004	77.161				
12	0.75	1.874	79.035				

Results are truncated.

4.3 Organisational Culture Variable

Following suggestions by Chin (1998a), organisational culture (CULTURE) was assessed at both sub-scale and higher-order levels. The results showed that practice, performance, innovation and support were reliable and valid at their respective item levels, and were sufficient indicators of CULTURE at a higher-order factor. This was evident from loadings and cross-loadings of item measures in Appendix 2 and subscales in Appendix 3. The reliability and validity estimates are summarised in Table 17.

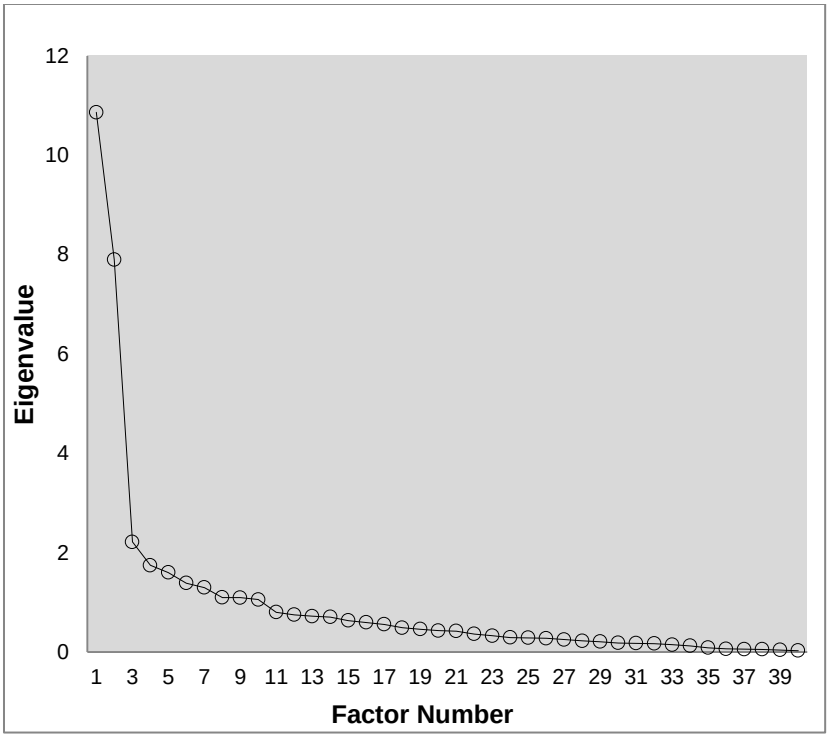


Figure 6: Scree Plot.

As shown in Table 17, items for 4 constructs of CULTURE at sub-scale level exhibited sufficient reliability with loadings of more than .50 on their respective sub-scales. Each sub-scale's reliability was confirmed by Cronbach's alpha of more than .70 and VIF of less than 5. Convergent validity for each construct (subscale) was supported by significant loading ($p < .05$), composite reliability of more than .70, and AVE of more than .70. Discriminant validity was supported by the square-root of AVE for each subscale, which was more than their respective inter-construct correlation as shown in Table 17.

Table 17

Parameter Estimates for Organisational Culture (CULTURE)

		Subscale			
	CULTURE (4)	**Support (5)**	**Practice (3)**	**Perform-ance (5)**	**Innovation (6)**
Composite reliability	.863	.823	.876	.899	.883
Cronbach's alpha	.787	.730	.787	.859	.841
AVE	.612	.584	.703	.641	.557
VIF	1.285	1.474	1.839	2.067	1.737
Loadings on CULTURE*		.711	.785	.840	.787
Maximum cross-loading at higher-order^		.224	.256	.186	.096
Indicator loadings		.603 to .772	.776 to .878	.761 to .851	.699 to .773
Maximum Indicator cross-loadings		.439	.235	.215	.272

Number of items for each construct is shown in ( ). AVE = average variance extracted, VIF = variance inflation factor. *Loadings of subscales on CULTURE. ^Cross-loadings on other constructs.

At a higher-order level the 4 constructs showed sufficient item reliability with each subscale loading on CULTURE higher than .50. CULTURE also exhibited an adequate convergent validity with the subscale variables showing low cross-loading on other constructs (see Appendix 3) and significant loading on CULTURE ($p < .05$). Composite reliability (> .70) and AVE (> .50) further supported convergent validity. The square root of AVE, which was more than the inter-construct correlation (Table 19) and VIF of less than 5 (Table 17) indicated discriminant validity of the second-order construct.

Table 18

First-order Level AVEs and Inter-construct Correlations

	Support	Innovation	Practice	Performance	COMPLEX	INTENT	ATT	SN	PBC-Out	PBC-Res
Support	(.696)									
Innovation	.404	(.746)								
Practice	.434	.454	(.839)							
Performance	.440	.590	.558	(.801)						
COMPLEX	.252	.150	.300	.306	(.745)					
INTENT	.114	.123	-.106	.079	-.086	(.924)				
ATT	.167	.186	.011	.104	-.055	.770	(.975)			
SN	.159	.148	-.088	.109	-.069	.772	.772	(.954)		
PBC-Out	.075	.167	-.054	.101	-.100	.711	.642	.681	(.980)	
PBC-Res	.082	.149	-.119	.112	-.062	.643	.574	.636	.806	(.872)

Square-root of AVE is in () on the diagonal

4.4 Control Variable

The Kruskal-Wallis test showed that intention (INTENT) was significantly different among the four categories of behaviour: dangerous tinkering (*mean rank* = 249.68), naïve mistake (*mean rank* = 169.06), detrimental misuse (*mean rank* = 157.41) and intentional destruction (*mean rank* = 195.62, χ^2 = 39.37, *df* = 3, *N* = 387, $p < .001$, Cohen's $f = .34$). This indicates significant effects of behavioural dimensions, and as a result, these effects (introduced by each of the 4 vignettes) were controlled by introducing a VIGNETTE variable as a control variable in the full model. Using this method eliminated potential confounding effects of different types of dysfunctional behaviour on the outcome (Mehta, 2001; Pole & Bondy, 2010), and allowed for unbiased causal inferences in the model.

Table 19

Second-order Level AVEs and Inter-construct Correlations

	COMPLEX	INTENT	ATT	SN	PBC-Out	PBC-Res	CULTURE
COMPLEX	(.745)						
INTENT	-.086	(.924)					
ATT	-.055	.770	(.975)				
SN	-.069	.772	.772	(.954)			
PBC-Out	-.100	.711	.642	.681	(.980)		
PBC-Res	-.062	.643	.574	.636	.806	(.872)	
CULTURE	.323	.066	.148	.103	.093	.072	(.782)

Square-root of AVE is in ( ) on the diagonal.

4.5 Model Validation Stage 1: Assessing the Measurement Model

Prior to the structural model assessment, measurement of the full research model was checked for reliability and validity. The criteria used are shown in Table 13 (page 88) and the results are described in the following sections.

4.5.1 Reliability and Validity

The results indicated sufficient item reliability with individual item loading above .50, as shown in Appendix 3. Convergent validity of the latent variables in the model was confirmed by significant item loadings ($p < .05$) (shown in Appendix 3), composite reliability of more than .70, and average variance extracted (AVE) in excess of the minimum threshold of .50 (shown in Table 20). The square root of AVE for each latent variable also exceeded the inter-construct correlations as shown in Table 19. Reliability of the variables was further supported by Cronbach's alpha of more than .70 and a variance inflation factor (VIF) of less than 5.

Parameter estimates in Tables 19 and 20 also confirm the initial results of the exploratory factor analysis, suggesting that PBC is a two-factor construct. In addition to these parameter estimates, average block variance inflation factor (AVIF) and full collinearity VIF (AFVIF) were also checked. AVIF and AFVIF were used to assess if the additional component of PBC added either lateral or vertical collinearity to the model (Kock, 2011; Kock & Lynn, 2012), which can result in unreliable estimates in the final analysis. This is particularly important in the light of a relatively high inter-construct correlation between two PBC constructs ($r = .806$), shown in Table 19. In line with Greene and D'Arcy's (2010) approach when inter-construct correlation reaches .80, VIF and AVIF were checked to ensure the 2-factor PBC was uniquely identifiable, and the effects of each construct on the criterion

variable was adequately discernable without the threat of multicollinearity. While AVIF checks for vertical, i.e. predictor-predictor collinearity; AFVIF checks for multicollinearity. Using a cut-off point of 3.3 (an ideal value) and 5 (an acceptable value) for both AVIF and AFVIF (Kock & Lynn, 2012), the full model with two-factor PBC was found to be free of collinearity issues (*AVIF* = 3.151, *AFVIF* = 3.809).

Table 20

Cronbach's Alpha, Composite Reliability and AVE

Construct	Composite reliability	Cronbach's Alpha	AVE	*N* items
CULTURE	.863	.787	.612	4
COMPLEX	.832	.731	.555	4
INTENT	.967	.957	.853	5
ATT	.974	.947	.950	2
SN	.968	.951	.911	3
PBC-Out	.980	.958	.960	2
PBC-Res	.905	.841	.761	3

ATT = Attitude, SN = Subjective norm, PBC-Out = perceived behavioural control over outcome of behaviour, PBC-Res = Perceived behavioural control over resources to engage behaviour, INTENT = Intention, CULTURE = organisational culture, AVE = Average variance extracted.

4.5.2 Assessment of the Nature of Latent Constructs

4.5.2.1 Theoretical Assessment of Reflective Latent Constructs

Following the theoretical assessment criteria of (see Bagozzi, 2007; Chin, 1998b; Jarvis, et al., 2003; Rodgers & Guiral, 2011), attitude (ATT), subjective norm (SN), perceived behaviour control over outcome of behaviour (PBC-Out), and

perceived behaviour control over resources (PBC-Res) were found to be reflective latent constructs. These latent constructs exist independent of their indicators, which when added or dropped, do not cause variation in the constructs. This was further supported when changes in the constructs were manifested by the indicators, suggesting a causality flow originating from the constructs to their respective indicator sets. This was also true for accounting information systems complexity (COMPLEX), where the measurement items were designed to capture the cognitive aspects that users have to exert to interact with the system (see Dong-Han, et al., 2011; Fioretti & Visser, 2004), rather than measuring the system design and operational attributes.

In regard to organisational culture, the 4 dimensions used (support, innovation, practice and performance) are reflective measurements of the latent construct. These 4 latent variables were measured at descriptive (i.e. practice) rather than evaluative (i.e. value) domain.

Muijen, et al. (1999) made a clear distinction between descriptive and evaluative measurements of culture. A descriptive measurement applies to directly observable manifestations of culture (Deal & Kennedy, 1988) which are reflected by artefacts; while the evaluative domain measures fundamental aspects of the culture which have already been programmed into one's mind (Hofstede, 1998a) to influence culture. Since the current study measured the descriptive domains of support, innovation, practice and performance dimensions, these items were representative of the organisational culture.

4.5.2.2 Statistical Assessment of Reflective Latent Constructs

Coltman et al.'s (2008) reflective construct assessment was used to confirm sufficient indicator loadings (more than .50) on their respective factor (see Appendix 1), construct reliability (Cronbach's alpha >.70), average variance extracted (AVE) (Table 20) for each construct which was higher than the construct correlation with other constructs, and showed positive weight-loading sign (WLS).

4.6 Model Validation Stage 2: Assessing the Structural Model

Based on the results in section 4.5, the measurement model showed good individual item reliability, convergent validity and discriminant validity, with values within the thresholds described in Table 14. The next stage was to examine the structural model to determine its explanatory power, and to test the hypotheses of the study. The effects of the constructs defined in the proposed model were assessed through coefficient of determination (R^2), path coefficient (β), effect size (f^2) and predictive relevance (Q^2). Figure 7 depicts the results and shows that 7 out of 12 hypotheses were supported.

The full model showed 78% variations in INTENT, represented by the combined effect of exogenous variables (R^2 = .783). R^2 of this magnitude shows the model has substantial predictive accuracy according to the standards suggested by Chin (1998b) and Hair Jr, et al. (2014)[17]. Predictive relevance of the model was further cross-validated with a positive Q^2 (Q^2 = .760) as shown in Table 21.

[17] Hair Jr, et al. (2014) suggested R^2 of .75, .50, and .25 as substantial, moderate and weak, respectively. Chin (1998b) on the other hand, considered .67, .33, and .19 for similar levels. Regardless of which standard is used R^2 in the model had substantial predictive accuracy.

Although Q^2 showed good predictive relevance, it did not validate the quality of the prediction (Sarstedt, Ringle, Henseler, & Hair, 2014), which had to be assessed by the path's significance and its magnitude (Hair, et al., 2011; Hair Jr, et al., 2014), as well as effect size (Chin, 1998a; Cohen, 1988; Meehl, 1990). All paths leading from predictors to INTENT in the model were significant, with path coefficients ranging from .093 to .449, providing support for H1, H2, H3a, and H3b. Moderating effects of CULTURE and COMPLEX however, showed mixed results. These are discussed in section 4.6.1 and 4.6.2. The results are summarised in Figure 7 and the relevant parameters are shown in Table 21.

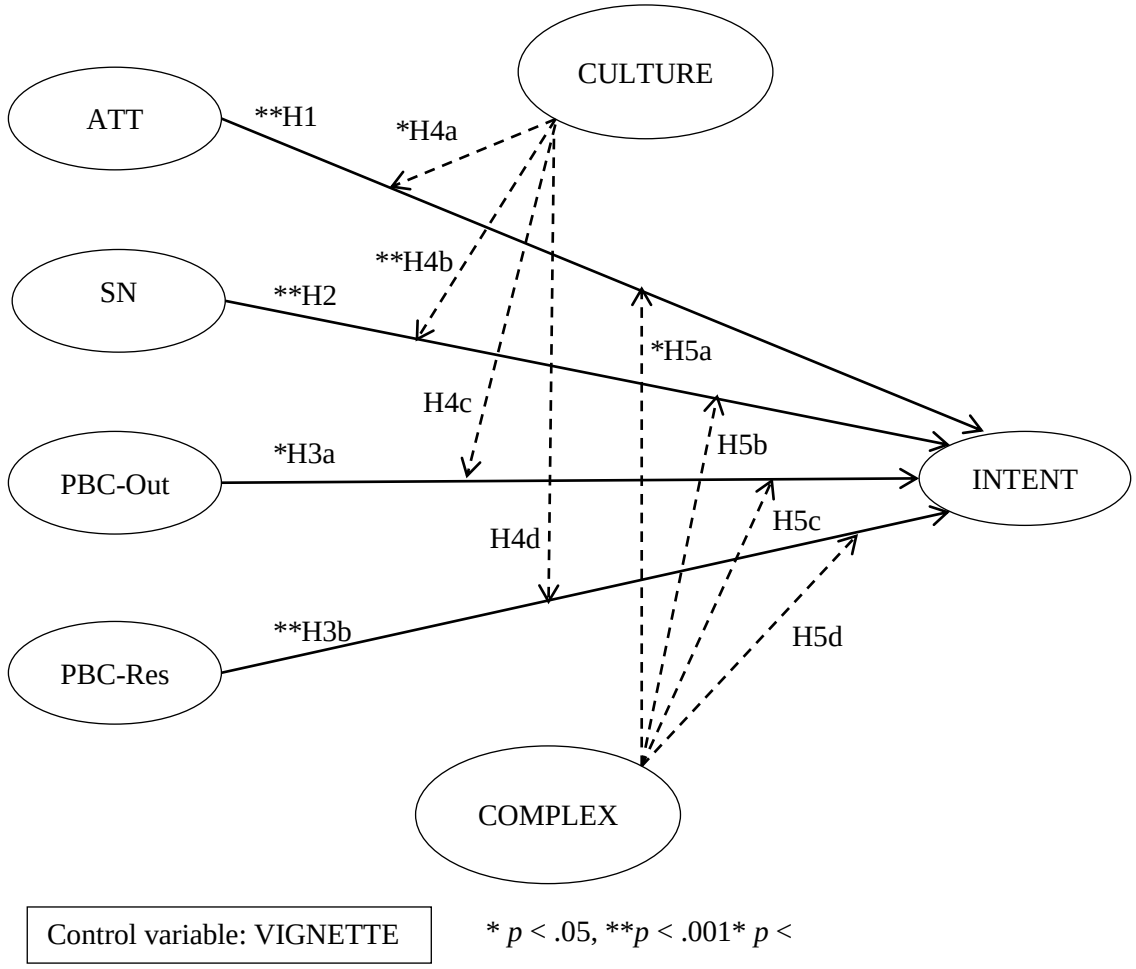


Figure 7: PLS-SEM results.

In Table 21 ATT is the strongest predictor of INTENT, with a path coefficient of .449 (p < .001), which by Chin's (1998a), standards which are considered to be strong. From a practical point of view, the effect size of the ATT-INTENT path further shows that the effect of ATT was large (f^2 = .365). On the other hand, the path coefficient of SN was acceptable, with a medium effect size (β = .228, f^2 = .117), while PBC-Out and PBC-Res both showed a weak influence on INTENT with small effect size (PBC-Out: β = .093, f^2 = .067, PBC-Res: β = .140, f^2 = .090), despite their statistical significance.

Table 21

Structural Model Parameters

Path	***β***	***p*-value**	***f*²**	**Hypotheses**
ATT -> INTENT	.449	< .001	.365	H1: supported
SN -> INTENT	.228	< .001	.177	H2: supported
PBC-Out -> INTENT	.093	.018	.067	H3a: supported
PBC-Res -> INTENT	.140	< .001	.090	H3b: supported
CULTURE moderating effects:				
ATT -> INTENT	.076	.044	.021	H4a: supported
SN -> INTENT	.172	< .001	.051	H4b: supported
PBC-Out -> INTENT	-.004	.462	.001	H4c: not supported
PBC-Res -> INTENT	.014	.374	.005	H4d: not supported
COMPLEX moderating effects:				
ATT -> INTENT	.129	.002	.029	H5a: supported
SN -> INTENT	.025	.284	.004	H5b: not supported
PBC-Out -> INTENT	.048	.141	.012	H5c: not supported
PBC-Res -> INTENT	-.028	.264	.006	H5d: not supported
Control variable: VIGNETTE	-.098	< .001	.031	Not applicable

R^2 = .783, Adjusted R^2 = .776, Q^2 = .760

4.6.1 Moderating Effects of Organisational Culture

Organisational culture (CULTURE) is hypothesised to significantly moderate the effects of attitude (ATT), subjective norm (SN), perceived control of behavioural outcome (PBC-Out), and perceived control of resources (PBC-Res) on intention (INTENT). The results however, only supported H4a (CULTURE on ATT-INTENT, $\beta = .076$, $f^2 = .020$, $p = .044$) and H4b (SN-INTENT, $\beta = .172$, $f^2 = .051$, $p < .001$). From a practical point of view, the magnitude and effect size of these significant moderating effects are small. On closer inspection, the moderating effect on ATT-INTENT revealed that CULTURE moderated this relationship in a similar pattern (Figure 8) for both low (weak) and high (strong) organisational culture. Both lines were curvilinear with identical slopes, indicating that CULTURE tends to increase the effects of ATT on INTENT regardless of CULTURE strength. The moderating effect however, was reversed at one standard deviation away from ATT mean, as indicated by the lines of the ATT upper section in Figure 8. In this instance, irrespective of CULTURE strength, there was evidence of negative ATT impact on INTENT.

CULTURE increased SN effect at every measured point of SN (SN-INTENT, $\beta = .172$, $f^2 = .051$, $p < .001$). However, high CULTURE was different from low CULTURE, where the effect was curvilinear at one standard deviation away from SN mean as shown in Figure 9. This suggests low CULTURE reflects individualism and a detachment from others.

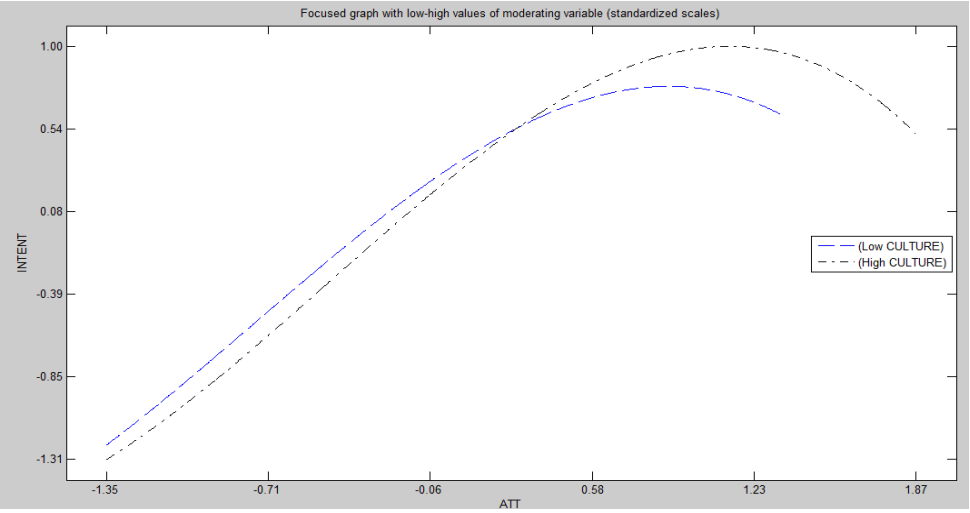


Figure 8: Moderating Effect of CULTURE on ATT-INTENT

Therefore, when organisational culture is weakly associated with an individual, the influence of CULTURE in deterring individuals from engaging in dysfunctional behaviour is marginal. In contrast, in high (strong) CULTURE, the curvilinear relationship showed evidence of CULTURE reducing SN propensity on INTENT. This is reflected in the upper end of the low CULTURE line.

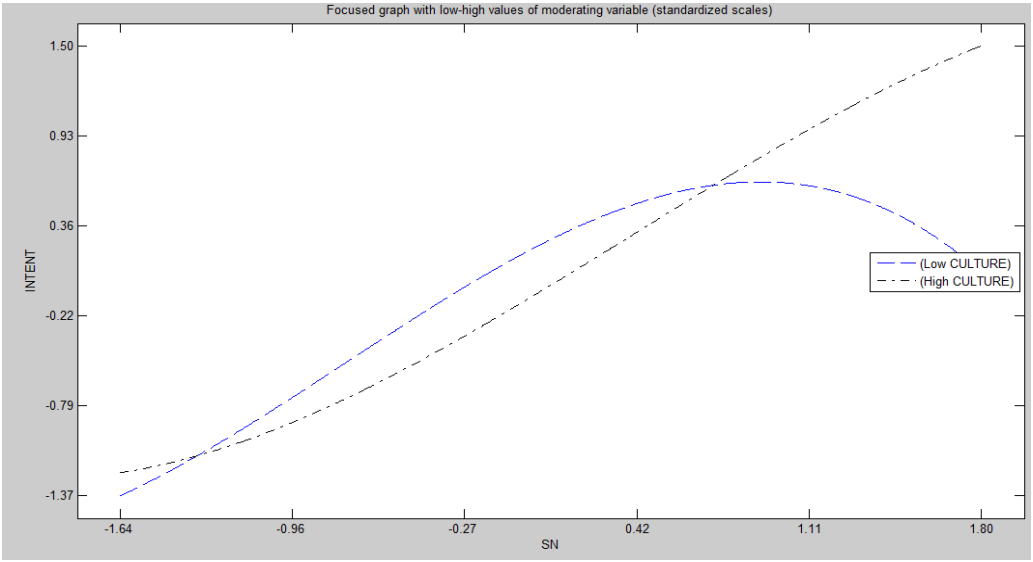


Figure 9: Moderating Effect of CULTURE on SN-INTENT.

4.6.2 Moderating Effects of Accounting Information System Complexity

Systems complexity was hypothesised to moderate all predictor-criterion relationships in the model. However, COMPLEX moderating effect was limited to the ATT-INTENT path in the model, supporting only H5a (ATT-INTENT, β = .129, f^2 = .029, p = .002). H5b (SN-INTENT), H5c (PBC-Out-INTENT) and H5d (PBC-Res-INTENT) were not supported.

Closer examination of the moderating effect of COMPLEX on ATT-INTENT, revealed that for low COMPLEX the effect of ATT on INTENT increased at every measured point. For high COMPLEX however, a curvilinear relationship was observed, with a steeper ATT-INTENT slope at the lower end of ATT, and a reverse effect at approximately one standard deviation away from ATT mean. This indicates that COMPLEX changes the strength and form of the ATT-INTENT relationship. This result is shown in Figure 10.

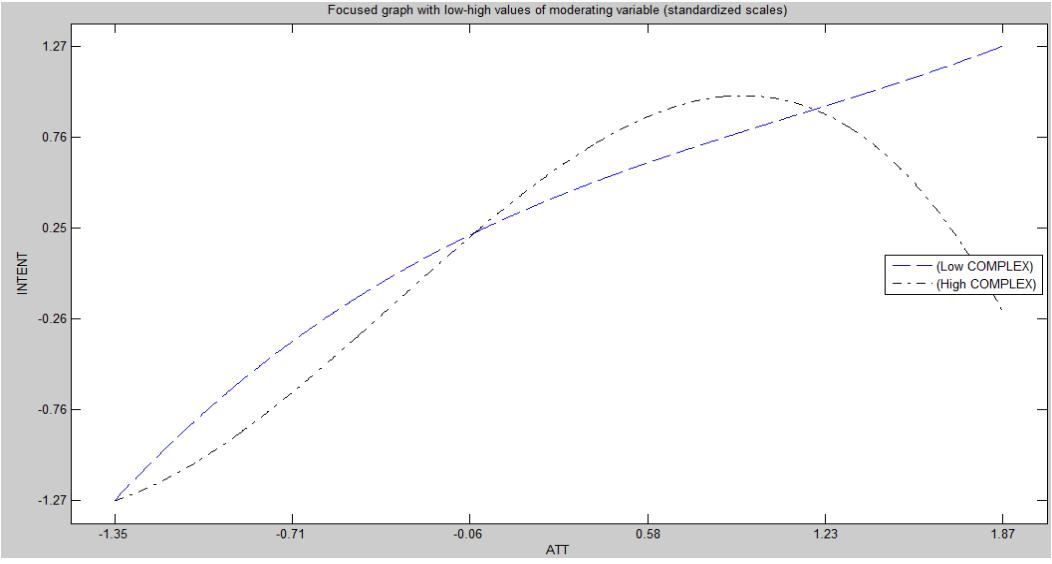


Figure 10: Moderating Effect of COMPLEX on ATT-INTENT.

4.7 Effects of Taxonomic Dimensions

Apart from using aggregate level dysfunctional behaviour to observe general behavioural disposition (see Ajzen, 1991), the research model was also tested on different behaviour categories based on Stanton, et al. (2005) behaviour taxonomy. The procedure was used to examine how taxonomic dimensions, which are a continuum of computer skills (low to high) and level of intention (malicious to neutral), affect each predictor of intention.

The results showed that ATT was a salient predictor across the four categories, as shown by significant ATT-INTENT in all vignettes in Table 22. The SN-INTENT path was significant for vignettes 1 (detrimental misuse), 2 (intentional destruction), and 3 (dangerous tinkering); while vignette 4 (naïve mistake) was non-significant (β = .133, f^2 = .095, p = .062).

Table 22 also shows PBC-Out-INTENT path was significant in vignettes 2 and 4, despite these two behaviours being located at the extreme ends of a two-dimensional taxonomy. Vignette 2, *intentional destruction*, requires high computer skills with malicious intention according to the taxonomy. On the other hand, vignette 4 (naïve mistake) was situated at the low-skill end of the spectrum, hand, vignette 4 (naïve mistake) requires low computer skills and is without clear intention. The PBC-Res-INTENT path was significant in vignettes 3 and 4, both categorised as dysfunctional behaviours with neutral intention

Table 22

Path Coefficients in Vignettes

Path	Vignette 1: *Detrimental Misuse*	Vignette 2: *Intentional Destruction*	Vignette 3: *Dangerous Tinkering*	Vignette 4: *Naïve Mistake*
ATT -> INTENT	.647**	.578**	.791**	.369**
SN -> INTENT	.411**	.352**	.200*	.133
PBC-Out -> INTENT	.028	.144*	-.039	.254*
PBC-Res -> INTENT	.089	.059	.434**	.279**
CULTURE moderating effects:				
ATT -> INTENT	.271**	.170*	.394**	.334**
SN -> INTENT	-.029	.018	-.183*	-.190*
PBC-Out -> INTENT	.021	-.039	.080	.052
PBC-Res -> INTENT	.047	.025	.105	.091
COMPLEX moderating effects:				
ATT -> INTENT	.148*	.176**	-.086	-.058
SN -> INTENT	.051	.282**	.151*	-.031
PBC-Out -> INTENT	-.045	-.080	-.165*	.086
PBC-Res -> INTENT	-.270**	.089	-.169*	.068

* $p < .05$, ** $p < .001$

. CULTURE moderating effect showed mixed results across the four vignettes. While CULTURE significantly moderated the ATT-INTENT path in all vignettes, similar to that at behaviour aggregate level, the moderating effect only exhibited a significant influence on the SN-INTENT path in vignettes 3 and 4 at the behaviour subset level. Vignettes 3 and 4 also showed negative CULTURE moderating effects on the SN-INTENT path. These two vignettes were *dangerous tinkering* and *naïve mistake* respectively, categorised as having neutral intention. CULTURE moderating effects were also non-significant on PBC-Out-INTENT and

PBC-Res-INTENT paths in all vignettes, which was consistent with the results at behaviour aggregate level.

In Table 22 the moderating effect of COMPLEX also illustrates mixed results. Based on Stanton et al.'s (2005) taxonomic dimensions, a pattern was observable in the results. COMPLEX had significant moderating effects on ATT-INTENT in vignettes 1 and 2, which shared a common taxonomic dimension. Both were categorised as malicious, but required different levels of computer skill. Although COMPLEX exhibited a non-significant moderating effect on SN-INTENT path at behaviour aggregate level, vignettes 2 and 3, both located at the upper end of computer skills, showed significant effects. Significant COMPLEX moderating effect was also observed on the PBC-Out-INTENT path in vignette 3; while the PBC-Res-INTENT path was significantly moderated by COMPLEX for vignettes 1 and 3 with negative coefficients.

At the subset level behaviour results were mixed, with some paths showing similar patterns as those at aggregate level, while others did not. Changes in the path coefficients' signs, magnitudes and significances illustrate the influence of dysfunctional behaviour dimensions on predictor-criterion relationships. While the mixed results reveal patterns that can be explained by two dysfunctional behaviour dimensions (level of computer skill and the continuum of malicious-neutral intention), cross-category similarities, such as those shown by the significant moderating effects of COMPLEX on PBC-Out-INTENT for vignettes 2 and 3, was perplexing. This may indicate a limitation of two-dimension dysfunctional behaviour requiring additional taxonomic dimensions, which could be investigated in future research.

Chapter Five
Findings and Discussion

The results of this study partially support the hypothesised relationships amongst the variables. At aggregate level of dysfunctional behaviour, attitude (ATT), subjective norm (SN), and perceived behaviour control over outcome (PBC-Out) and resources (PBC-Res) exhibited significant positive influence on intention (INTENT). However, organisational culture (CULTURE) only showed significant moderating effects on ATT-INTENT and SN-INTENT paths. Furthermore, accounting information systems complexity (COMPLEX) showed significant influence on the ATT-INTENT relationship. At subset level, only ATT showed a consistent influence across all four categories of dysfunctional behaviour. The results are further discussed below.

5.1 Insider Dysfunctional Behaviour

The Kruskal-Wallis test in section 4.4 showed that intention differed across the four types of behaviour. In terms of magnitude and *p*-value, the changes of path coefficients when the research model was applied to each behaviour category (shown in section 4.7) further highlights the influence of behaviour taxonomic dimensions. The findings therefore provide empirical support for the methodological concerns raised by Crossler, et al. (2013), Guo (2013), Posey, et al. (2013), and Warkentin and Willison (2009) by adequately addressing typological differences in AIS behavioural studies.

Behavioural studies in accounting information systems (AIS) have provided us with a good understanding for dealing with risks posed by insiders. Ajzen (1991) proposed an aggregation of different behaviours across different situations to provide

a measure of general disposition, and a more valid measure of underlying behavioural disposition than analysis of any single behaviour. A vast amount of literature has examined negative insider behaviour or information systems (IS) deviant behaviour (Burns, 2013; Cheng, et al., 2013) at the aggregate level. Deviant behaviour is generally viewed and understood through the lens of IS security compliance/non-compliance (Barlow, et al., 2013; Furnell & Rajendran, 2012; Harris & Furnell, 2012; Padayachee, 2012b), computer misuse (Liao, et al., 2009; Vance, et al., 2013), and computer abuse (Baruch, 2005; Lowry, et al., 2014; Posey, et al., 2011). However, this method of aggregation does not address typological differences in deviant behaviour. In order to account for typological disparities, Stanton et al.'s (2005) taxonomy was used in the current study to investigate how predictor criteria behave at both aggregate and subset levels of dysfunctional behaviour.

Using 4 types of risky behaviours, this study introduced dysfunctional behaviour as a concept, defined as higher-order negative behaviour on a continuum of intention (i.e. malicious to neutral) and computer skills (i.e. low to high) which are required to engage in such behaviour (Cheng, et al., 2013; Guo, 2013; Ifinedo, 2014; Magklaras & Furnell, 2001, 2005; Stanton, et al., 2005). Through this concept, dysfunctional behaviour can be understood in its higher-order typology and also at its subset level. At its higher-order level, dysfunctional behaviour aggregates different negative behaviours which pose security risks to organisational AIS assets, and provides a general understanding of dysfunctional behaviour, while at its subset level, a more thorough analysis of each set of behaviours is possible. Based on the dysfunctional behaviour concept and the empirical evidence found this study thus,

answers research question 1, where different types of insider dysfunctional behaviour are related to or different from each other.

5.2 Perceived Behaviour Control

The theory of planned behaviour (TPB) was developed by Ajzen (1991) to improve his previous theory of reason action (TRA). What differentiates TPB and TRA is the inclusion of perceived behaviour control (PBC) in TPB to account for factors beyond one's volitional control. It is argued however, that PBC is composed of two distinct components (Ifinedo, 2014; Kidwell & Jewell, 2003; Terry & O'Leary, 1995; Trafimow, Sheeran, Conner, & Finlay, 2002; Zolait, 2011). The current study also found that PBC comprised two distinct components, although it was not part of the main analysis or related to the research questions, the result was in alignment with the findings of Ifinedo (2014), Pavlou and Fygenson (2006), and Trafimow, et al. (2002).

The argument for PBC as a 2-component construct is partly based on a locus of control (Ajzen, 2002a; Kidwell & Jewell, 2003; Rotter, 1960) which PBC encompasses, that is, either the control is situated within one's internal ability (Bandura, 1978b; Cheolho & Hyungon, 2013), such as skills and resources, or it is externally focused, such as exertion of control over anticipated outcomes (Bandura, 1978a; Rotter, 1966). This corresponds with the view that individuals are more inclined to engage in behaviours they believe are achievable, reflecting external locus of control to execute such behaviour. Ajzen (2002a) however, concluded that PBC at its higher order is a single construct "…and the extent to which they (internal and external controls) reflect one or the other is an empirical question" (Ajzen, 2002a, p. 680). Nevertheless, amalgamating these two distinct constructs into one

can obscure the causes of intention, because each sub-construct may affect intention differently (Trafimow, et al., 2002), particularly when behaviour is perceived to be within one's control and based on internally or externally oriented factors (Kidwell & Jewell, 2003).

Supported by reliability, discriminant validity and convergence validity, PBC in this study was therefore found and maintained as two distinct components, with the presence of theoretical commonality between internal and external locus of control. This is because maintaining lower-order factors in a research model can illuminate aspects of a latent construct which are otherwise hidden if the higher-order factor is used (see Jia, Bhatti, & Nahavandi, 2012; Trafimow, et al., 2002; Zolait, 2011). As PBC in this study was operationalised as perception of control over resources to engage in actual behaviour (PBC-Res) and perception of control over outcome of intended behaviour (PBC-Out), maintaining the lower-order factors as two components can enhance our understanding of the aspects of PBC that affect and are affected by other factors in the research model.

5.3 Contextual Factors Affecting Intention

Employees' interactions with an organisation's AIS are characterised by a myriad of influences (DeSanctis & Poole, 1994) involving human, organisational and technological factors. Managing insider threats solely from the perspective of technology is insufficient, as is looking only at human factors or organisational settings. The human and contextual factors, in this case the organisational culture and technology, must be examined together to provide a holistic view. Research question 2 which seeks to illuminate relevant contextual factors affecting

dysfunctional behavioural intention, is answered in this section where each moderating effect is discussed.

5.3.1 Moderating Effects of Organisational Culture

Organisational culture helps to explain diverse outcomes in information systems-related behaviour (Ahrens & Mollona, 2007; Robey & Azevedo, 1994). Social dimensions in an organisation exert a strong influence over individuals' behaviour, especially when the individual is strongly attached to the referenced group (Cheng & Chu, 2014; Terry, et al., 1999). While organisational culture may not of itself directly affect behaviour, as found by Hu, et al. (2012), interaction effects of organisational culture with attitude and subjective norm produce combined effects on intention. Similarly, employee perception of control over resources to engage in dysfunctional behaviour and relative control over outcomes of such behaviour are also moderated by organisational culture. This is because organisational culture intertwines with the fabric of organisational behaviour as a whole (Ernest Chang & Lin, 2007; Robey & Azevedo, 1994), governing the actions of its members (Tams, 2013). When the culture is shaped to disavow certain types of behaviour, successful engagement in negative behaviour is limited. However, when organisational culture is indifferent to or tolerates malpractice, this can create an environment for dysfunctional behaviour to take place.

The results of this study only partially supported the above assertions. Organisational culture was found to affect attitude- and subjective norm-intention relationships. No significant moderating effect on perceived control over resources and outcome of dysfunctional behaviour was found. The evidence found in this study, that organisational culture moderates the effect of attitude and subjective norm

on intention, aligns with the findings of other recent studies (e.g. Cheng, et al., 2013; Hu, et al., 2012; Ifinedo, 2014). However, such alignment is limited to the extent of significant moderating effects.

It was expected that organisational culture weakens the effect of attitude on intention to engage in dysfunctional behaviour. The positive moderating sign on the other hand, indicates organisational culture can nurture dysfunctional behaviour. This is regardless of the culture strength. As shown by the curvilinear lines in both strong and weak culture, only when attitude is strong that organisational culture can diffuse attitude-intention relationship. When employee's attitude towards dysfunctional behaviour intention is generally indifferent, organisational culture can strengthen positive attitude toward intention of malpractices. A possible explanation for this perplexing finding is a level of employees' awareness of security protocol and repercussion of non-compliance. The employees with low awareness exert attitudinal indifference towards dysfunctional behaviour. This is later strengthened by organisational culture regardless whether the culture is strong or weak. Nevertheless, when the security awareness is high, organisational culture can mitigate a strong attitude toward dysfunctional behavioural intention. Whilst this was not directly examined by the current study, future work should look into this area to advance our understanding on this complex relationship.

Similarly, the effect of organisational culture on subjective norm-intention relationship was found to be positive rather than expected negative. Because subjective norm defines one's reliance on important others on dysfunctional behaviour intention, weakly associated employees with others could lead the employees to look for behavioural cues in organisational culture which eventually

strengthens the effect of subjective norm on intention. This is further compelled by strong output-oriented organisational culture where the employees focus solely on getting a job done with disregard to security policy as seen in NHS case (Collins, 2008; Fleming, 2006).

Further, a lack of empirical evidence to support hypotheses that organisational culture also affects components of perceived behaviour control (PBC) warrants closer examination. A study by Hu, et al. (2012) also acknowledged inconclusive results when it comes to the influence of organisational culture on perceived behaviour control. These authors suggested that other organisational culture attributes be used. An explanation of this perplexing observation lies in the work of Terry, et al. (1999), and Cheng and Chu (2014), who claimed that self-identity is "…a collection of identities that reflects the roles a person occupies in the social structure" (Terry, et al., 1999, p. 228). Both Terry et al., and Cheng and Chu, found PBC influence is strong when a performer of behaviour identifies that his/her relevance or role in a reference group is weak. Therefore, even though organisational culture governs one's actions, the extent to which this factor moderates perception of control on behaviour is subject to an employee's sense of relevance to the organisation. A clear moderating effect of self-identity on PBC can also be seen in the work of Cheng and Chu (2014). However, this valuable work was not conducted within the AIS field, and the current study therefore provides momentum for an important avenue of future research.

5.3.2 Moderating Effects of Accounting Information System Complexity

Accounting information systems (AIS) complexity defines the "…interactions of the person with the environment" (Frese, 1987, p. 321) and

introduces uncertainties (Alvarado-Valencia & Barrero, 2014) that go beyond one's control. AIS complexity was initially hypothesised to significantly moderate the effects of attitude, subjective norms and two components of perceived behavioural control on intention. However, the results of this study showed this was not the case. A significant moderating effect of AIS complexity was only observed in the relationship between employee attitude and intention at aggregate dysfunctional behaviour level.

The absence of significant moderating effect of AIS complexity on perceived behaviour control can partly be explained by the underlying architectural interface design of the software and the computer efficacy of the employees. Software interface design has improved substantially over the decades, making it easier to use. This is coupled with increased computer efficacy among employees in Malaysia, as documented by the Institute for Management Development (IMD) survey. IMD reported a steady increase in IT skill rating[18] from 7.5 in 2008 to 8.0 in 2013 (*IMD world competitiveness yearbook*, 2008; *IMD world competitiveness yearbook*, 2013). Since the current study focuses on cognitive assessment of AIS complexity, the effect of complexity no longer plays a critical role to assert a significant constraint on perceived behavioural control components, nor does it affect employee reliance on reference to others (i.e. subjective norm). Rather, the mental assessment of AIS complexity lies in its effect on shaping attitude towards

[18] IT skill rating is based on a scale between 1 to 10. IMD World Competitiveness Yearbook is a tool to benchmark competitiveness of performance of a country. This annual publication is used by many institutions including governments around the world. Malaysian government also uses this report as part of the country's annual performance report.

dysfunctional behaviour. This supports an individual's *cognitive dissonance* ("Cognitive dissonance," 2008; Festinger, 1962; Gerard, 1994), and *risk homeostasis* (Baniela & Ríos, 2010; Nikolaidis, 2009; Wilde, 1998), which suggest ambiguities resulting from uncertainties create disequilibrium in one's mind, prompting changes in attitude and hence behaviour.

The initial results of this study also revealed that the overall moderating effect of AIS complexity was found to be positive rather than (expected) negative, on the relationship between attitude and intention. This suggests that the more complex AIS is, the more attitude towards system misuse or abuse increases, leading to a higher likelihood that employees will engage in detrimental behaviour. The result of the current study was also consistent with Cheng, et al. (2013) who claimed that certain IS security countermeasures are paradoxical. This was further explained by Nikolaidis (2009) who described the situation as an example of risk homeostasis (Wilde, 1998), where an individual has a certain level of "affordable" risk in which additional security leads to the individual negating the impact of the measure and engaging in risky actions. The more complex a system is in acting as a control mechanism, the more it can be a catalyst for dysfunctional behaviour (Moore, et al., 2008; Posey, et al., 2011; Stanton & Stam, 2006), particularly when such practices are deemed "necessary" to accomplish a given task (Singh, et al., 2007). In the case of the National Health Service (NHS) in the UK (Collins, 2008; Fleming, 2006), the suggestion of Singh, et al. has merits. Password-sharing practices in NHS were deemed necessary to accomplish medical procedures, although such practices were clearly against the organisation's policy. Lieberman (2011) study also showed that 42% of information technology (IT) professionals surveyed engaged in IT practices

that contradicted what was considered acceptable. This was in spite of an initial assumption that IT professionals are well aware of the negative implications of such dysfunctional behaviour. Belanger (2011) reported similar findings in her study, where individuals felt a mandatory password-change policy caused unnecessary interruptions to completing their job tasks, and triggered a negative attitude towards security-compliance policy.

Although systems complexity that reduces or deters an intention to engage in dysfunctional behaviour is preferred, the results of this study suggest that, in a less complex AIS environment, the attitude-intention relationship appears to be positive. In a highly complex accounting information systems environment however, diminishing effect of attitude on intention was observed at the higher end of attitude (curvilinear relationship above one standard deviation away from the mean). Complexity of the AIS system therefore affects attitude towards dysfunctional behaviour in both ways, because "there is an optimal degree of complexity where complexity that is too high stifles performance, and too low complexity does the same thing" (Frese, 1987, p. 326). When AIS complexity is regarded as part of AIS control, the optimal complexity phenomenon explains why information systems control mechanisms help to reduce unwarranted behaviours, as in the studies of Albrechtsen and Hovden (2009), and why the control features themselves induce such behaviour (see Belanger, 2011; Herath & Rao, 2009; Workman, et al., 2008).

5.4 Practical Implications

The findings of this study have implications for managerial practices to bring insider threats to an acceptable and manageable level. Behavioural studies in AIS present findings that provide avenues for understanding commonalities between

human, technology and organisations. Similarly, the findings of the current study imply that, from a socio-technical perspective, optimising the human-technology-organisation interconnection to reduce insider threats can be realised by improving organisational culture, balancing AIS complexity (Wang, Gupta, & Rao, 2015) and job tasks, and focussing efforts on managing programs with sufficient momentum to impact attitudinal change. This is the essence upon which research question 3 is based and subsequently answered through the findings of this study.

Organisational culture can act as a formal control (Ernest Chang & Lin, 2007; Musa, 2011) with "rites and rituals" (Deal & Kennedy, 1988) that bind members to adhere to commonly accepted practices (Goffee & Jones, 1996). Organisations however, will have to cultivate a zero-tolerance approach to dysfunctional behaviour. Where organisational culture sanctions negative activities such practices will prevail, because culture within organisations is affect-neutral (Hofstede, 1998a) in that it represents how things are done rather than a conviction of good or bad practices. In addition, organisations have to maintain a close association with individual employees, and nurture a sense of belonging and strong identity with the group (see Cheng, et al., 2013; Herbst & Houmanfar, 2009; Terry, et al., 1999). Strong self-identification to a particular group leads to social control that governs individuals to behave according to group norms. It is therefore logical to conclude that where organisational culture disavows dysfunctional behaviour and employees identify strongly with the organisation, insider threats are manageable.

Organisational culture is one part of the findings of this study. A balance must also be maintained between the need to secure AIS assets and the urgency of getting tasks done, since added layers of security are usually implemented at the

expense of convenience (Möller, et al., 2011; Sun, Ahluwalia, & Koong, 2011). Less complex AIS creates complacency where dysfunctional behaviour can potentially take place. On the other hand, where AIS is too complex it can foster risk homeostasis through complacency (Nikolaidis, 2009), whereby employees put too much trust in the AIS security system (Rhee, et al., 2009), leading to dysfunctional behaviour, especially in relation to actions with neutral intention, such as password sharing. Striking a balance between the level of security complexity and user convenience is not an easy task. Within the context of dysfunctional behaviour, AIS should be user-centric at both design and implementation stages. Users, job tasks, and data characteristics are all components that should be carefully considered during these stages.

Attitude was found to be a dominant predictor across all four dysfunctional behaviour typologies, so focussing on attitudinal changes is a good way to manage insider threats. Where organisational culture is affect-neutral and has limited or no effect on attitude, factors affecting attitude need to be explored. Perceived severity of sanctions (D'Arcy, Galletta, & Hovav, 2009; Son, 2011) and security training (D'Arcy, et al., 2009; da Veiga & Martins, 2015; Wolf, et al., 2011) are factors that have been found to affect attitude.

Furnell and Rajendran (2012) went further to suggest that workplace atmosphere and workplace-independent factors also influence employee personality. They found these factors included real-life exposure to security incidents, perceived benefits of following good practices and an awareness of external elements, such as legal statutes (data protection acts, and computer security acts) which are contingent on information system assets security. These elements can be incorporated into

security training modules to expose employees to similar external factors with the goal of bringing about changes in their attitudes toward dysfunctional behaviour.

Affecting attitudinal change is difficult, yet it is essential for organisations to put some effort into overcoming apathy in their workplaces. Attitudinal and behavioural changes take time, and plans to initiate change should include adequate time for proposing, implementing and assimilating changes so that they become part of the culture or common practice (Pfleeger & Caputo, 2012). These authors contended that "…if humans using computer systems are given the tools and information they need, taught the meaning of responsible use, and then trusted to behave appropriately with respect to cyber security, desired outcomes may be obtained without security being perceived as onerous or burdensome" (Pfleeger & Caputo, 2012, p. 5).

Chapter Six
Conclusion

In many domains, including accounting and information systems, causal chains follow logical and predictable paths. However, in accounting information systems (AIS), where behaviour is the focus of analysis, predictor-criterion relationships are inexact and terms are defined within the scope of each individual study. These all present challenges to addressing the issues at hand. Since the AIS discipline bridges two major fields: accounting and information systems (IS), solutions for the relevant issues may be sought from its parent fields. Despite advancements in the AIS domain, the discipline is still lacking in theories to explain observed phenomena and problems faced by organisations (Sutton, 2004a, 2006; Sutton & Arnold, 2011; Worrell, et al., 2013), in particular, threats to organisational AIS assets originating from within. In order "…to understand a phenomenon, we need to study that phenomenon from as many perspectives as possible until a consistent pattern arises and theory essentially presents itself" (Sutton, 2000, p. 7). Theories inspire and sharpen empirical investigation, providing a common conceptual framework to integrate diverse findings and potentially deepen our understanding of issues of interest. Developing credible theories therefore helps organisations to take remedial action to alleviate, or at a minimum, bring the risks of insider dysfunctional behaviour to acceptable and manageable levels.

Owing to the IS discipline, academic literature (e.g. Hu, et al., 2012; Vance, et al., 2013; Wall, 2013; Willison & Warkentin, 2013) and professional surveys (e.g. "Key findings from the 2013 US state of cybercrime survey," 2013; Richardson, 2011) acknowledge the IS security risks posed by inappropriate actions of members

of organisation. These are insiders who sit behind the organisations' firewalls (Warkentin & Willison, 2009) with user privileges which are not otherwise granted to external users. Armed with these privileges, insiders remain the weakest link in an effort to secure organisational IS assets (Crossler, et al., 2013), as found in the surveys of (Baker, et al., 2011; Richardson, 2011). Despite rapid advancements in protection technologies, AIS security policies and procedures, and studies on behavioural aspects of AIS security are still limited (Sutton, 2006; Worrell, et al., 2013) "…although the need to consider the more social aspects of IS security has long been recognised" (Warkentin & Willison, 2009, p. 103).

Scholars in AIS security are looking into the behavioural aspects of insiders to provide insights into practices which are harmful to organisational AIS assets. This can be seen in the valuable work on IS security compliance/non-compliance behaviour by (Boss, et al., 2009; Ifinedo, 2012, 2014; Myyry, et al., 2009; Siponen, et al., 2014), IS misuse by (Glassman, et al., in press; Grant, 2010; Moody & Siponen, 2013; Siponen, et al., 2012; Vance, et al., 2013), and studies on computer abuse by (Baruch, 2005; Lowry, et al., 2014; Posey, et al., 2011). However, the investigations largely focused on non-malicious or policy non-compliance behaviour (Warkentin & Willison, 2009; Willison & Warkentin, 2013). While these studies make an important contribution to the body of the literature, examination of different types of harmful insider behaviour, such as volitional malicious actions which pose considerable risks to organisational AIS assets, is at best limited. Studies such as those by Moore, et al. (2008) on acts of sabotage, and Baskerville, et al. (2014) on deliberate computer abuse, address this gap.

An investigation of harmful insider practices, without segregating behaviours according to their appropriate categories, can lead to sample contamination, limiting the practical use and application of recommendations. Guo (2013) found that studies of security-related behaviour in this field sometimes reported inconsistent and contradictory results, partly due to a broad conceptualisation of harmful behaviours with "many of the concepts overlapping each other on some dimensions and yet different on others" (Guo, 2013, p. 242), and partly because factors explaining AIS security compliance do not necessarily account for policy violations. For example, studies that emphasise improving security awareness among insiders are unable to address issues relating to insiders who engage in acts driven by malicious intention (Crossler, et al., 2013; Posey, et al., 2013) "because knowledge created from a focus on a single behaviour or subset of behaviours does not necessarily generalise to the grand structure of behaviours" (Posey, et al., 2013, p. 1190). This underscores the need to refine studies on the topic by examining common behavioural traits at their higher-order structure, and differences at their subset level.

Accordingly, the current study took the behavioural taxonomy approach developed by Stanton, et al. (2005) to examine how predictors of behavioural intention are different at their aggregate level, termed *dysfunctional behaviour*, and at the subset level, where they were grouped into four categories: intentional destruction, detrimental misuse, dangerous tinkering and naïve mistake. In this way the study addressed the methodological issues raised by scholars (e.g. Crossler, et al., 2013; Guo, 2013; Posey, et al., 2013; Warkentin & Willison, 2009) in the AIS discipline, and enabled examination of changes in the predictors of behavioural

intention across different types of dysfunctional behaviours. Moreover, as urged by scholars (e.g. Sutton, 2004a, 2006; Sutton & Arnold, 2011; Worrell, et al., 2013), this research also contributes a theory to the body of AIS literature to explain insider dysfunctional behaviour when dealing with AIS.

Insider dysfunctional behaviour is not an entirely people-centric problem. It consists of a myriad of complex interactions between individuals, organisations and information systems (Cheng, et al., 2013). Using the theory of planned behaviour (TPB) as a base theory, and a reference to actor-network theory (ANT) to account for socio-technological interactions, this thesis explored these intricate connections, to advance our understanding of insider dysfunctional behaviour and answer *how* and *why* individuals choose to engage in such acts.

At the aggregate behavioural level, this study found attitude, subjective norm, perceived control over behavioural outcome, and perceived control over resources demonstrated significant effects on intention to engage in dysfunctional behaviour. The findings re-affirm what has been understood from studies on software piracy by Peace, Galletta, and Thong (2003), on unethical IT use by Chatterjee (2008), and on IS security compliance policy by Ifinedo (2012). Other studies (e.g. Banerjee, et al., 1998; Kraemer, et al., 2009; Lowry, et al., 2014; Posey, et al., 2011) suggest other contextual factors, such as the behaviour of co-workers (Cheng, et al., 2013), social ties (Worrell, et al., 2013), and technology (Chatterjee, 2008) interact with predictors. To account for this contextual relevance, organisational culture and AIS complexity were introduced into the equation.

The findings showed that the influence of organisational culture is significant, although the effect is limited to cultural interactions with attitude and

subjective norm, suggesting that organisational culture plays a critical role in shaping employees' attitudes and their reliance on others' perceptions and action. Similarly, AIS complexity exerts an interaction effect only on attitude. The fact that attitude presents the largest magnitude in terms of statistical quality demonstrates a large effect size for practical consideration; and its salience across all four categories of dysfunctional behaviour indicates the importance of this cognitive assessment. Similar findings have also been shown in studies by Blanke (2008), and Leonard, et al. (2004). Blanke investigated predictive ability of attitude, computer self-efficacy, and security policy awareness on computer abuse intention, and found that attitude was a salient predictor in her model. On the other hand, Leonard et al. looked into information technology ethical issues and found that attitude remained a significant predictor of behavioural intention, regardless of whether respondents saw ethics as important or otherwise.

The stability of attitude as a predictor of dysfunctional behaviour intention therefore demands appropriate managerial attention and should prompt organisations to revise their approach to reducing insider threats with programs that include elements that can affect the attitudes of their employees. For example, AIS security awareness programs can be designed to emphasise accountability (Boss, et al., 2009; Kraemer, et al., 2009; Posey, et al., 2013; Vance, et al., 2013), punishment severity for malicious conduct (Bandura, 1978b; Barlow, et al., 2013; Chatterjee, 2008; Cheng, et al., 2013; Greene & D'Arcy, 2010; Peace, et al., 2003; Siponen, et al., 2014), and create a strong security culture (Boss, et al., 2009; Cheng, et al., 2013; Greene & D'Arcy, 2010; Kraemer, et al., 2009; Martinez-Moyano, et al., 2011; Pfleeger & Caputo, 2012; Van Niekerk & Von Solms, 2010). Such a focus can affect

attitude towards dysfunctional behaviour because it presents individuals with a degree of social intolerance towards committing such behaviour, when "a simple display of acceptable computer use policy may not provide the required momentum to adequately exert changes to attitude", as suggested in a survey by Cronan, Foltz, and Jones (2006).

Unlike attitude which remains significant, when dysfunctional behaviour is analysed according to its taxonomic dimensions (i.e. subset level), other predictors of intention, moderating effects of organisational culture, and AIS system complexity vary at the four sublevels of dysfunctional behaviour. For example, employee reliance on the importance of others (i.e. subjective norm) is not a critical evaluation when it comes to a simple, non-malicious action like sharing a password in order to get work done. This explains why password-sharing practices is seen as acceptable and thrives in certain organisations, such as the National Health Service in the United Kingdom (see Collins, 2008; Lieberman, 2011). However, the impact of employee reliance on others' intention to engage in dysfunctional behaviour is reduced when organisational culture disavows such practice, regardless of how harmless or non-malicious the action is. Cultivating appropriate organisational culture is therefore helpful to alleviate the threat of insider dysfunctional behaviour.

When AIS complexity is viewed as a control mechanism, these assertions are debatable. Technologies of control can have diverse organisational effects (Ahrens & Mollona, 2007; Sun, et al., 2011) depending on the way in which the control becomes an integral part of organisational practices (Schatzki, 2005). How much complexity should be incorporated into AIS is a question that remains unanswered. Kolkowska and Dhillon (2013), Post and Kagan (2007), and Renaud

and Goucher (2012) found that too much complexity can hinder progression of work, causing employees to by-pass the security measures designed to protect their work. There is therefore a need to balance the level of system complexity with the need to accomplish job tasks in a way that does not compromise either.

6.1 Limitations and Future Work

This study introduced the concept of dysfunctional behaviour aligned with a methodological approach to investigate negative insider behaviours in an AIS environment. It used a two-dimensional behaviour taxonomy, derived from Stanton, et al. (2005), where different behaviours are grouped into continuums of computer skill and intention. This concept differentiates itself from general IS deviant behaviour, computer abuse and misuse, because dysfunctional behaviour enables a systematic typological categorisation of behaviours. While the findings provide general behavioural disposition at aggregate level, the investigation was limited to one type of behaviour in each typology at the subset level. In order to account for general dispositions within groups, it is recommended that future studies further examine behaviour types in each category at different levels of computer skill and maliciousness.

The results of the current study also show how predictors of intention change in both magnitude and direction at dysfunctional behaviour subset level. While these changes can be explained by behavioural dimensions, cross-category similarities between vignettes 2 (high skill, highly malicious) and 3 (low skill, neutral intention) indicate influences other than those investigated here. Potential influencing factors, such as individuals' risk aversion and AIS data structure should therefore be accounted for. Furthermore, cognitive dissonance can cause

psychological discomfort, leading to an individual actively avoiding situations and information, thereby causing dissonance. On the other hand, data with low level importance can potentially diffuse the effects of computer skill, which can in turn lead to high-risk appetites, causing a risk homeostasis phenomenon. It is therefore important that future studies include an investigation into individual risk appetites to account for risk homeostasis (Nikolaidis, 2009; Wilde, 1998) and cognitive dissonance (Festinger, 1962), and to preserve the integrity of the data (Sun, et al., 2011) as control variables.

The sample in this study comprised medium-size enterprises (SMEs) because this category of business entity has limited financial capacity to invest in AIS security. Middle managers were selected as respondents because these individuals are equipped with relatively higher levels of systems access compared to other employees in the operational group. Owing to the nature of the sample the findings should be interpreted within the context of medium-sized companies. While Malaysian SMEs were chosen in this study, national culture could also be factor influencing the final result. Future work on dysfunctional behaviour could place the spotlight on employees in large-sized companies with cross-border samples to increase the generalisability of the findings.

Despites these limitations, the findings of the current study contribute a theory to the body of literature in AIS, explaining how dysfunctional behaviour is formed and can be predicted, using explanatory variables drawn from the theory of planned behaviour combined with organisational culture and technological factor. Coupled with the dysfunctional behaviour concept, the theory helps to explain variations in the findings of other behavioural studies in AIS and IS. In practical

terms this study juxtaposes four subsets of dysfunctional behaviours to irradiate similarities and differences, and illuminates general behavioural disposition, allowing for effective action to reduce insider threats to an acceptable and manageable level.

References

Abernethy, M. A., & Bouwens, J. (2005). Determinants of accounting innovation implementation. *Abacus*, *41*(3), 217-240. doi: 10.1111/j.1467-6281.2005.00180.x

Abernethy, M. A., & Brownell, P. (1997). Management control systems in research and development organizations: The role of accounting, behavior and personnel controls. *Accounting, Organizations and Society*, *22*(3–4), 233-248. doi: 10.1016/s0361-3682(96)00038-4

Abernethy, M. A., & Guthrie, C. H. (1994). An empirical assessment of the "fit" between strategy and management information system design. *Accounting & Finance*, *34*(2), 49-66. doi: 10.1111/j.1467-629X.1994.tb00269.x

Abu-Musa, A. A. (2006). Perceived security threats of computerized accounting information systems in the Egyptian banking industry. [Scholarly Journal]. *Journal of Information Systems*, *20*(1), 187-203.

Ahrens, T., & Mollona, M. (2007). Organisational control as cultural practice - A shop floor ethnography of a Sheffield steel mill. *Accounting, Organizations and Society*, *32*(4–5), 305-331. doi: 10.1016/j.aos.2006.08.001

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179-211. doi: 10.1016/0749-5978(91)90020-t

Ajzen, I. (2002a). Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior. *Journal of Applied Social Psychology*, *32*(4), 665-683. doi: 10.1111/j.1559-1816.2002.tb00236.x

Ajzen, I. (2002b). Residual effects of past on later behavior: Habituation and reasoned action perspectives. *Personality and Social Psychology Review*, *6*(2), 107-122. doi: 10.1207/s15327957pspr0602_02

Ajzen, I. (n.d.-a). Constructing a theory of planned behaviour questionnaire Retrieved 20 Feb 2012, 2012, from http://people.umass.edu/aizen/pdf/tpb.measurement.pdf

Ajzen, I. (n.d.-b). Sample TPB questionnaire Retrieved 30 Mar 2012, 2012, from http://people.umass.edu/aizen/pdf/tpb.questionnaire.pdf

Ajzen, I., & Madden, T. J. (1986). Prediction of goal-directed behavior: Attitudes, intentions, and perceived behavioral control. *Journal of Experimental Social Psychology*, *22*(5), 453-474. doi: 10.1016/0022-1031(86)90045-4

Albrechtsen, E., & Hovden, J. (2009). The information security digital divide between information security managers and users. *Computers & Security*, *28*(6), 476-490. doi: http://dx.doi.org/10.1016/j.cose.2009.01.003

Allen, P., & Bennett, K. (2010). *PASW statistics by SPSS: A practical guide, version 18.0* (1 ed.). Sydney: Cengage Learning Australia Pty Limited.

Allison, P. D. (2003). Missing data techniques for structural equation modeling. *Journal of Abnormal Psychology*, *112*(4), 545-557. doi: 10.1037/0021-843x.112.4.545

Almalawi, A., Yu, X., Tari, Z., Fahad, A., & Khalil, I. (2014). An unsupervised anomaly-based detection approach for integrity attacks on SCADA systems. *Computers & Security*, *46*(0), 94-110. doi: http://dx.doi.org/10.1016/j.cose.2014.07.005

Alvarado-Valencia, J. A., & Barrero, L. H. (2014). Reliance, trust and heuristics in judgmental forecasting. *Computers in Human Behavior, 36*(0), 102-113. doi: http://dx.doi.org/10.1016/j.chb.2014.03.047

Anderson, J. C., & Gerbing, D. W. (1988). Structural equation modeling in practice: A review and recommended two-step approach. *Psychological Bulletin, 103*(3), 411-423. doi: 10.1037/0033-2909.103.3.411

Anderson, J. P. (1980). Computer security threat monitoring and surveillance. Fort Washington: James P. Anderson Company.

Armitage, C. J., & Conner, M. (2001). Efficacy of the theory of planned behaviour: A meta-analytic review. *The British Journal of Social Psychology, 40*, 471-499.

Bagozzi, R. P. (2007). On the meaning of formative measurement and how it differs from reflective measurement: Comment on Howell, Breivik, and Wilcox (2007). *Psychological Methods, 12*(2), 229-237. doi: 10.1037/1082-989x.12.2.229

Bagozzi, R. P., & Yi, Y. (1990). Assessing method variance in multitrait-multimethod matrices: The case of self-reported affect and perceptions at work. *Journal of Applied Psychology, 75*(5), 547-560. doi: 10.1037/0021-9010.75.5.547

Baker, W., Hutton, A., Hylender, C. D., Pamula, J., Porter, C., & Spitler, M. (2011). 2011 data breach investigations report: Verizon.

Bandura, A. (1978a). Reflections on self-efficacy. *Advances in Behaviour Research and Therapy, 1*(4), 237-269. doi: http://dx.doi.org/10.1016/0146-6402(78)90012-7

Bandura, A. (1978b). Self-efficacy: Toward a unifying theory of behavioral change. *Advances in Behaviour Research and Therapy, 1*(4), 139-161. doi: http://dx.doi.org/10.1016/0146-6402(78)90002-4

Banerjee, D., Cronan, T. P., & Jones, T. W. (1998). Modeling IT ethics: A study in situational ethics. *MIS Quarterly, 22*(1), 31-60.

Baniela, S. I., & Ríos, J. V. C. (2010). The risk homeostasis theory. *The Journal of Navigation, 63*(4), 607-626. doi: http://dx.doi.org/10.1017/S0373463310000196

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2013). Don't make excuses! Discouraging neutralization to reduce IT policy violation. *Computers & Security, 39, Part B*(0), 145-159. doi: http://dx.doi.org/10.1016/j.cose.2013.05.006

Baruch, Y. (2005). Bullying on the net: Adverse behavior on e-mail and its impact. *Information & Management, 42*(2), 361-371. doi: http://dx.doi.org/10.1016/j.im.2004.02.001

Baruch, Y., & Holtom, B. C. (2008). Survey response rate levels and trends in organizational research. *Human Relations, 61*(8), 1139-1160. doi: 10.1177/0018726708094863

Baskerville, R., Park, E. H., & Kim, J. (2014). An emote opportunity model of computer abuse. *Information Technology & People, 27*(2), 155-181. doi: 10.1108/ITP-11-2011-0068

Beautement, A., & Sasse, A. (2009). The economics of user effort in information security. *Computer Fraud & Security, 2009*(10), 8-12. doi: 10.1016/s1361-3723(09)70127-7

Belanger, F. (2011). When users resist: How to change management and user resistance to password security. *Pamplin College of Business Magazine*.

Bellot, J. (2011). Defining and assessing organizational culture. *Nursing Forum, 46*(1), 29-37. doi: 10.1111/j.1744-6198.2010.00207.x

Benaroch, M., Chernobai, A., & Goldstein, J. (2012). An internal control perspective on the market value consequences of IT operational risk events. *International Journal of Accounting Information Systems*(2012). doi: 10.1016/j.accinf.2012.03.001

Benford, T. L., & Hunton, J. E. (2000). Incorporating information technology considerations into an expanded model of judgment and decision making in accounting. *International Journal of Accounting Information Systems, 1*(1), 54-65. doi: 10.1016/s1467-0895(99)00004-4

Benita, C. (2003). Accountability lost: The rise and fall of double entry. *The International Journal of Management Science, 31*, 303-310. doi: 10.1016/S0305-0483(03)00048-3

Bennett, D. A. (2001). How can I deal with missing data in my study? *Australian and New Zealand Journal of Public Health, 25*(5), 464-469. doi: 10.1111/j.1467-842X.2001.tb00294.x

Birnberg, J. G., & Snodgrass, C. (1988). Culture and control: A field study. *Accounting, Organizations and Society, 13*(5), 447-464. doi: 10.1016/0361-3682(88)90016-5

Blanke, S. J. (2008). *A study of the contributions of attitude, computer security policy awareness, and computer self-efficacy to the employees' computer abuse intention in business environments.* 3336919 Ph.D., Nova Southeastern University, Ann Arbor. ProQuest Dissertations & Theses Global database.

Bloor, G., & Dawson, P. (1994). Understanding professional culture in organizational context. *Organization Studies, 15*(2), 275-295. doi: 10.1177/017084069401500205

Borchert, D. (2011). *A meta-model of ethical behavior: An empirical examination of ethical leadership, ethical identity, ethical climate and emotions on unethical work behavior.* Saint Louis University Ph.D., Saint Louis University, United States -- Missouri. ProQuest database.

Boritz, J. E. (2005). IS practitioners' views on core concepts of information integrity. *International Journal of Accounting Information Systems, 6*(4), 260-279. doi: 10.1016/j.accinf.2005.07.001

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. *European Journal of Information Systems, 18*(2), 151-164.

Breiman, L., & Friedman, J. H. (1985). Estimating optimal transformations for multiple regression and correlation. *Journal of the American Statistical Association, 80*(391), 580-598. doi: 10.2307/2288473

Brick, J., & Kalton, G. (1996). Handling missing data in survey research. *Statistical Methods in Medical Research, 5*(3), 215-238. doi: 10.1177/096228029600500302

Burchell, S., Clubb, C., Hopwood, A., Hughes, J., & Nahapiet, J. (1980). The roles of accounting in organizations and society. *Accounting, Organizations and Society, 5*(1), 5-27. doi: 10.1016/0361-3682(80)90017-3

Burns, C. E. (2013). *The Relationship between Personality and Computer Deviance.* 3599478 D.B.A., Walden University, Ann Arbor. ProQuest Dissertations & Theses Global database.

Bye, H. H., Horverak, J. G., Sandal, G. M., Sam, D. L., & van de Vijver, F. J. (2014). Cultural fit and ethnic background in the job interview. *International Journal of Cross Cultural Management, 14*(1), 7-26. doi: 10.1177/1470595813491237

Calderon, T. G., Chandra, A., & Cheh, J. J. (2006). Modeling an intelligent continuous authentication system to protect financial information resources. *International Journal of Accounting Information Systems, 7*(2), 91-109. doi: 10.1016/j.accinf.2005.10.003

Cameron, K. S., & Quinn, R. E. (2011). Diagnosing and changing organizational culture : Based on the competing values framework Retrieved from http://ECU.eblib.com.au/patron/FullRecord.aspx?p=706769

Cattell, R. B. (1966). The scree test for the number of factors. *Multivariate Behavioral Research, 1*(2), 245-276. doi: 10.1207/s15327906mbr0102_10

Celuch, K., Goodwin, S., & Taylor, S. A. (2007). Understanding small scale industrial user internet purchase and information management intentions: A test of two attitude models. *Industrial Marketing Management, 36*(1), 109-120. doi: http://dx.doi.org/10.1016/j.indmarman.2005.08.004

Chang, M. K. (1998). Predicting unethical behavior: A comparison of the theory of reasoned action on the theory of planned behavior. *Journal of Business Ethics, 17*(16), 1825-1834.

Chatman, J. A., & Jehn, K. A. (1994). Assessing the relationship between industry characteristics and organizational culture: How different can you be? *The Academy of Management Journal, 37*(3), 522-553.

Chatterjee, S. (2008). *Unethical behavior using information technology.* Ph.D. 3370378, Washington State University, United States -- Washington. ABI/INFORM Complete; ProQuest Central; ProQuest Dissertations & Theses (PQDT) database.

Chatterjee, S., Lubatkin, M. H., Schweiger, D. M., & Weber, Y. (1992). Cultural differences and shareholder value in related mergers: Linking equity and human capital. *Strategic Management Journal, 13*(5), 319-334. doi: 10.1002/smj.4250130502

Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security, 39, Part B*(0), 447-459. doi: http://dx.doi.org/10.1016/j.cose.2013.09.009

Cheng, P.-y., & Chu, M.-c. (2014). Behavioral factors affecting students' intentions to enroll in business ethics courses: A comparison of the theory of planned behavior and social cognitive theory using self-identity as a moderator. *Journal of Business Ethics, 124*(1), 35-46. doi: http://dx.doi.org/10.1007/s10551-013-1858-0

Cheolho, Y., & Hyungon, K. (2013). Understanding computer security behavioral intention in the workplace. *Information Technology & People, 26*(4), 401-419. doi: 10.1108/ITP-12-2012-0147

Chin, W. W. (1998a). Issues and opinion on structural equation modeling. *MIS Quarterly, 22*(1), VII-XVI.

Chin, W. W. (1998b). The partial least squares approach to structural equation modelling. In G. A. Marcoulides (Ed.), *Modern methods for business research* (pp. 295-336). Mahwah, New Jersey: Lawrence Erlbaum Associates.

Choo, F., & Tan, K. (2007). An "American Dream" theory of corporate executive Fraud. *Accounting Forum, 31*(2), 203-215. doi: 10.1016/j.accfor.2006.12.004

Choung, R., Locke, G. R., III, Schleck, C., Ziegenfuss, J., Beebe, T., Zinsmeister, A., & Talley, N. (2013). A low response rate does not necessarily indicate non-response bias in gastroenterology survey research: a population-based study. *Journal of Public Health, 21*(1), 87-95. doi: 10.1007/s10389-012-0513-z

. Cognitive dissonance. (2008). In W. A. Darity, Jr. (Ed.), *International Encyclopedia of the Social Sciences* (2nd ed. ed., Vol. 1, pp. 599-601). Detroit: Macmillan Reference USA.

Cohen, J. (1988). *Statistical power analysis for the behavioural sciences* (2nd ed.). Hillsdale, New Jersey: Lawrence Erlbaum Associates.

Cohn, M., & Bellone, B. H. (1997). History of accounting software. *Accounting Technology, 13*(1), 18-36.

Collins, T. (2008). Password sharing leaves NHS audit trail in tatters Retrieved 15 February, 2012, from http://www.computerweekly.com/news/2240103960/Password-sharing-leaves-NHS-audit-trail-in-tatters#.T3Pl1Cv-o6Q.email

Coltman, T., Devinney, T. M., Midgley, D. F., & Veniak, S. (2008). Formative versus reflective measurement models: Two applications of formative measurement. *Journal of Business Research, 61*(12), 1250-1262.

Cooper, R. B. (1994). The inertial impact of culture on IT implementation. *Information & Management, 27*(1), 17-31. doi: 10.1016/0378-7206(94)90099-x

Cronan, T. P., Foltz, C. B., & Jones, T. W. (2006). Piracy, computer crime, and IS misuse at the university. *Commun. ACM, 49*(6), 84-90. doi: 10.1145/1132469.1132472

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security, 32*(0), 90-101. doi: http://dx.doi.org/10.1016/j.cose.2012.09.010

Curtis, M. B., & Payne, E. A. (2008). An examination of contextual factors and individual characteristics affecting technology implementation decisions in auditing. *International Journal of Accounting Information Systems, 9*(2), 104-121. doi: http://dx.doi.org/10.1016/j.accinf.2007.10.002

D'Arcy, J. P. (2007). *Misuse of information systems : The impact of security countermeasures*. New York, NY, USA: LFB Scholarly Publishing LLC.

D'Arcy, J. P., Galletta, D., & Hovav, A. (2009). User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. [Technical report]. *Information Systems Research, 20*, 79+.

D'Arcy, J. P., & Hovav, A. (2009). Does one size fit all? Examining the differential effects of is security countermeasures. *Journal of Business Ethics, 89*, 59-71.

d'Astous, A., François, C., & Montpetit, D. (2005). music piracy on the web - How effective are anti-piracy arguments? Evidence from the theory of planned

behaviour. *Journal of Consumer Policy, 28*(3), 289-310. doi: 10.1007/s10603-005-8489-5

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research, 20*(1), 79 - 98.

Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers & Security, 29*(2), 196-207. doi: 10.1016/j.cose.2009.09.002

da Veiga, A., & Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security, 49*(0), 162-176. doi: http://dx.doi.org/10.1016/j.cose.2014.12.006

Daily, C. M., Dalton, D. R., & Cannella Jr, A. A. (2003). Corporate governance: Decades of dialogue and data. *The Academy of Management Review, 28*(3), 371-382.

Dalton, D. R., & Todor, W. D. (1993). Turnover, transfer, absenteeism: An interdependent perspective. *Journal of Management, 19*(2), 193-219. doi: 10.1016/0149-2063(93)90052-o

Davern, M. J., & Wilkin, C. L. (2010). Towards an integrated view of IT value measurement. *International Journal of Accounting Information Systems, 11*(1), 42-60. doi: 10.1016/j.accinf.2009.12.005

Davis, G. A. (2004). Possible aggregation biases in road safety research and a mechanism approach to accident modeling. *Accid Anal Prev, 36*(6), 1119-1127. doi: 10.1016/j.aap.2004.04.002

Davis, R. A. (2001). A cognitive-behavioral model of pathological Internet use. *Computers in Human Behavior, 17*(2), 187-195. doi: http://dx.doi.org/10.1016/S0747-5632(00)00041-8

Deal, T. E., & Kennedy, A. A. (1988). *Corporate cultures : The rites and rituals of corporate life*. London Penguin Books.

Debreceny, R. S., & Gray, G. L. (2010). Data mining journal entries for fraud detection: An exploratory study. *International Journal of Accounting Information Systems, 11*(3), 157-181. doi: 10.1016/j.accinf.2010.08.001

Dent, J. F. (1991). Accounting and organizational cultures: A field study of the emergence of a new organizational reality. *Accounting, Organizations and Society, 16*(8), 705-732. doi: 10.1016/0361-3682(91)90021-6

DeSanctis, G., & Poole, M. S. (1994). Capturing the complexity in advanced technology use: Adaptive structuration theory. *Organization Science, 5*(2), 121-147. doi: 10.2307/2635011

Dickson, G. W., & Simmons, J. K. (1970). The behavioral side of MIS: Some aspects of the "people problem". *Business Horizons, 13*(4), 59-71. doi: 10.1016/0007-6813(70)90159-x

Dillard, J. F., & Yuthas, K. (2006). Enterprise resource planning systems and communicative action. *Critical Perspectives on Accounting, 17*(2–3), 202-223. doi: 10.1016/j.cpa.2005.08.003

Dinev, T., Goo, J., Hu, Q., & Nam, K. (2009). User behaviour towards protective information technologies: The role of national cultural differences. *Information Systems Journal, 19*(4), 391-412. doi: 10.1111/j.1365-2575.2007.00289.x

Doherty, N. F., Anastasakis, L., & Fulford, H. (2011). Reinforcing the security of corporate information resources: A critical review of the role of the acceptable use policy. *International Journal of Information Management, 31*(3), 201-209. doi: 10.1016/j.ijinfomgt.2010.06.001

Dolwick, J. (2009). 'The social' and beyond: Introducing actor-network theory. *Journal of Maritime Archaeology, 4*(1), 21-49. doi: 10.1007/s11457-009-9044-3

Dong-Han, H., Jinkyun, P., & Wondea, J. (2011). A framework-based approach to identifying and organizing the complexity factors of human-system interaction. *Systems Journal, IEEE, 5*(2), 213-222. doi: 10.1109/jsyst.2010.2102574

Doty, D. H., & Glick, W. H. (1998). Common methods bias: Does common methods variance really bias results? *Organizational Research Methods, 1*(4), 374-406. doi: 10.1177/109442819814002

Dunkerley, K. D. (2011). *Developing an information systems security success model for organizational context.* Doctor of Philosophy Doctorate Thesis, Nova Southeastern University, Fort Lauderdale, Florida. (UMI Number: 3456547)

Eggert, A., & Serdaroglu, M. (2011). Exploring the impact of sales technology on salesperson performance: a task-based approach. *Journal of Marketing Theory and Practice, 19*(2), 169-185.

Ernest Chang, S., & Lin, C. S. (2007). Exploring organizational culture for information security management. *Industrial Management & Data Systems, 107*(3), 438-458. doi: doi:10.1108/02635570710734316

Farrell, A. M. (2010). Insufficient discriminant validity: A comment on Bove, Pervan, Betty, and Shiu (2009). *Journal of Business Research, 63*(3), 324-327.

Fayard, D., Lee, L. S., Leitch, R. A., & Kettinger, W. J. (2012). Effect of internal cost management, information systems integration, and absorptive capacity on inter-organizational cost management in supply chains. *Accounting, Organizations and Society, 37*(3), 168-187. doi: 10.1016/j.aos.2012.02.001

Felps, W., Mitchell, T. R., & Byington, E. (2006). How, when, and why bad apples spoil the barrel: Negative group members and dysfunctional groups. *Research in Organizational Behavior, 27*(0), 175-222. doi: 10.1016/s0191-3085(06)27005-9

Festinger, L. (1962). *A theory of cognitive dissonance*. Standford, California: Stanford University Press.

Field, A. (2013). *Discovering statistics using IBM SPSS statistics*. London: Sage Publications Ltd.

Fioretti, G. (1999). A subjective measure of complexity. *Advance Complex System, 4*, 349-370.

Fioretti, G., & Visser, B. (2004). A cognitive approach to organizational complexity. Retrieved from Social Science Research Network website: http://ssrn.com/abstract=524702 doi:http://dx.doi.org/10.2139/ssrn.524702

Fleming, N. (2006, 11 Jul). Security risk to NHS patients' records, News, *The Telegraph*. Retrieved from http://www.telegraph.co.uk/news/uknews/1523572/Security-risk-to-NHS-patients-records.html

Fornell, C., & Bookstein, F. (1982). Two structural equation models: LISREL and PLS applied to consumer exit-voice theory. *Journal of Marketing Research, 19*, 440-452.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *JMR, Journal of Marketing Research, 18*(1), 39.

Fox, S., & Spector, P. E. (1999). A model of work frustration–aggression. *Journal of Organizational Behavior, 20*(6), 915-931. doi: 10.1002/(sici)1099-1379(199911)20:6<915::aid-job918>3.0.co;2-6

Frese, M. (1987). A theory of control and complexity: Implications for software design and integration of computer systems into the workplace. *Psychological Issues of Human Computer Interaction in the Work Place*, 313-337.

Fullerton, R. R., Kennedy, F. A., & Widener, S. K. (2013). Management accounting and control practices in a lean manufacturing environment. *Accounting, Organizations and Society, 38*(1), 50-71. doi: http://dx.doi.org/10.1016/j.aos.2012.10.001

Furchgott, R. (2008, 29 August 2008). With software, till tampering is hard to find, *The New York Times*. Retrieved from http://www.nytimes.com/2008/08/30/technology/30zapper.html

Furnell, S., & Phyo, A. H. (2003). Considering the problem of insider IT misuse. *Australasian Journal of Information Systems, 10*(2), 134 - 138.

Furnell, S., & Rajendran, A. (2012). Understanding the influences on information security behaviour. *Computer Fraud & Security, 2012*(3), 12-15. doi: http://dx.doi.org/10.1016/S1361-3723(12)70053-2

Gaston, J. (2006). Modeling an intelligent authentication system to protect financial information. *International Journal of Accounting Information Systems, 7*(2), 113-114. doi: 10.1016/j.accinf.2006.04.003

Gatzlaff, K. M., & McCullough, K. A. (2010). The effect of data breaches on shareholder wealth. *Risk Management and Insurance Review, 13*(1), 61-83.

Geerts, G. L., & McCarthy, W. E. (2002). An ontological analysis of the economic primitives of the extended-REA enterprise information architecture. *International Journal of Accounting Information Systems, 3*(1), 1-16. doi: 10.1016/s1467-0895(01)00020-3

Gefen, D., & Straub, D. (2005). A practical guide to factorial validity using PLS-graph: Tutorial and annotated example. *Communications of the Association for Information Systems, 16*, 91-109.

Gerard, H. B. (1994). A retrospective review of Festinger's: A theory of cognitive dissonance. *PsycCRITIQUES, 39*(11), 1013-1017. doi: 10.1037/034205

Glassman, J., Prosch, M., & Shao, B. B. M. (in press). To monitor or not to monitor: Effectiveness of a cyberloafing countermeasure. *Information & Management*(0). doi: http://dx.doi.org/10.1016/j.im.2014.08.001

Goffee, R., & Jones, G. (1996). What holds the modern company together? *Harvard Business Review, 74*(6), 133+.

Goltz, H. H., & Smith, M. L. (2010). Yule-Simpson's paradox in research. *Practical Assessment, Research & Evaluation, 15*(15), 1-9.

Gordon, G. G. (1991). Industry determinants of organizational culture. *The Academy of Management Review, 16*(2), 396-415.

Gorla, N., & Somers, T. M. (2014). The impact of IT outsourcing on information systems success. *Information & Management, 51*(3), 320-335. doi: http://dx.doi.org/10.1016/j.im.2013.12.002

Graham, J. W. (2012). Missing data : Analysis and design Retrieved from http://ECU.eblib.com.au/patron/FullRecord.aspx?p=1156148

Grande, E. U., Estébanez, R. P., & Colomina, C. M. (2011). The impact of accounting information systems (AIS) on performance measures: Empirical evidence in spanish SMEs. *International Journal of Digital Accounting Research, 11*(15778517), 25-43.

Granlund, M. (2011). Extending AIS research to management accounting and control issues: A research note. *International Journal of Accounting Information Systems, 12*(1), 3-19. doi: 10.1016/j.accinf.2010.11.001

Granlund, M., & Mouritsen, J. (2003). Special section on management control and new information technologies. *European Accounting Review*, *12*(1), 77-83. doi: 10.1080/0963818031000087925

Grant, G. J. (2010). *Ascertaining the relationship between security awareness and the security behavior of individuals.* Ph.D. 3423144, Nova Southeastern University, United States -- Florida. ProQuest Dissertations & Theses (PQDT) database.

Gray, G. L., Chiu, V., Liu, Q., & Li, P. (2014). The expert systems life cycle in AIS research: What does it mean for future AIS research? *International Journal of Accounting Information Systems, 15*(4), 423-451. doi: http://dx.doi.org/10.1016/j.accinf.2014.06.001

Greene, G., & D'Arcy, J. P. (2010, 16-17 June 2010). *Assessing the impact of security culture and the employee-organisation relationship on IS security compliance.* Paper presented at the 5th Annual Symposium on Information Assurance 2010, New York.

Greenemeier, L. (2006). Insider threats. *InformationWeek*(1118), 25-28.

Griffin, R. W., O'Leary-Kelly, A., & Collins, J. (1998). Dysfunctional work behaviors in organizations. *Journal of Organizational Behavior* (08943796), 65-65.

Guo, K. H. (2013). Security-related behavior in using information systems in the workplace: A review and synthesis. *Computers & Security, 32*, 242-251. doi: http://dx.doi.org/10.1016/j.cose.2012.10.003

Gupta, N., & Jenkins Jr, G. D. (1991). Rethinking dysfunctional employee behaviors. *Human Resource Management Review, 1*(1), 39-59. doi: 10.1016/1053-4822(91)90010-a

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). *Multivariate data analysis* (7 ed.). Upper Saddle River, NJ, USA: Prentice-Hall, Inc.

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2006). *Multivariate data analysis* (6 ed.). New Jersey: Pearson Prentice Hall.

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing Theory and Practice, 19*(2), 139-151. doi: 10.273/MTP1069-6679190202

Hair Jr, J. F., Sarstedt, M., Hopkins, L., & Kuppelwieser, V. G. (2014). Partial least squares structural equation modeling (PLS-SEM). *European Business Review, 26*(2), 106-121. doi: doi:10.1108/EBR-10-2013-0128

Hampton, C. (2005). Determinants of reliance: An empirical test of the theory of technology dominance. *International Journal of Accounting Information Systems, 6*(4), 217-240. doi: 10.1016/j.accinf.2005.10.001

Hansen, T., Møller Jensen, J., & Stubbe Solgaard, H. (2004). Predicting online grocery buying intention: a comparison of the theory of reasoned action and the theory of planned behavior. *International Journal of Information Management, 24*(6), 539-550. doi: http://dx.doi.org/10.1016/j.ijinfomgt.2004.08.004

Hanseth, O., Aanestad, M., & Berg, M. (2004). Actor-network theory and information systems. *Information Technology & People, 17*(2), 116 - 123.

Harris, M., & Furnell, S. (2012). Routes to security compliance: be good or be shamed? *Computer Fraud & Security, 2012*(12), 12-20. doi: http://dx.doi.org/10.1016/S1361-3723(12)70122-7

Harrison, M., & Datta, P. (2007). An empirical assessment of user perceptions of feature versus application level usage. *Communications of the Association for Information Systems, 20*(1). doi: citeulike-article-id:12261329

Heinze, N., & Hu, Q. (2009). Why college undergraduates choose IT: A multi-theoretical perspective. *European Journal of Information Systems, 18*(5), 462-475.

Henri, J.-F. (2006). Organizational culture and performance measurement systems. *Accounting, Organizations and Society, 31*(1), 77-103. doi: 10.1016/j.aos.2004.10.003

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154-165. doi: http://dx.doi.org/10.1016/j.dss.2009.02.005

Herbst, S. A., & Houmanfar, R. (2009). Psychological approaches to values in organizations and organizational behavior management. *Journal of Organizational Behavior Management, 29*(1), 47-68. doi: 10.1080/01608060802714210

Hill, M., Mann, L., & Wearing, A. J. (1996). The effects of attitude, subjective norm and self-efficacy on intention to benchmark: A comparison between managers with experience and no experience in benchmarking. *Journal of Organizational Behavior, 17*(4), 313-327.

Hodgson, G. (2010). Choice, habit and evolution. *Journal of Evolutionary Economics, 20*(1), 1-18. doi: 10.1007/s00191-009-0134-z

Hofstede, G. (1998a). Attitudes, values and organizational culture: disentangling the concepts. [Article]. *Organization Studies, 19*(3), 477+.

Hofstede, G. (1998b). Identifying organizational subcultures: An empirical approach. *Journal of Management Studies, 35*(1), 1-12. doi: 10.1111/1467-6486.00081

Hofstede, G., Neuijen, B., Ohayv, D. D., & Sanders, G. (1990). Measuring organizational cultures: A qualitative and quantitative study across twenty cases. *Administrative Science Quarterly, 35*(2), 286-286.

Hopwood, A. G. (1972). An empirical study of the role of accounting data in performance evaluation. *Journal of Accounting Research, 10*(ArticleType: research-article / Issue Title: Empirical Research in Accounting: Selected Studies 1972 / Full publication date: 1972 / Copyright © 1972 Accounting

Research Center, Booth School of Business, University of Chicago), 156-182.
Hovav, A., & D'Arcy, J. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea. *Information & Management, 49*(2), 99-110. doi: http://dx.doi.org/10.1016/j.im.2011.12.005
Howell, D. C. (2013). *Statistical methods for psychology* (8 ed.). Belmont: Wadsworth, Cengage Learning.
Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences, 43*(4), 615-660. doi: 10.1111/j.1540-5915.2012.00361.x
Hwang, Y., & Grant, D. (2011). Behavioral aspects of enterprise systems adoption: An empirical study on cultural factors. *Computers in Human Behavior, 27*(2), 988-996. doi: 10.1016/j.chb.2010.12.003
IC - Integrated Framework summary: COSO. (1992). *Committee of Sponsoring Organizations of the Treadway Commission*. Retrieved from http://coso.org/documents/Internal%20Control-Integrated%20Framework.pdf
Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security, 31*(1), 83-95. doi: 10.1016/j.cose.2011.10.007
Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management, 51*(1), 69-79. doi: http://dx.doi.org/10.1016/j.im.2013.10.001
IMD world competitiveness yearbook. (2008). Lausanne: Institute for Management Development.
IMD world competitiveness yearbook. (2013). Lausanne: Institute for Management Development.
Ismail, N. A. (2009). Accounting information system: Education and research agenda. *Malaysian Accounting Review, 8*(1), 63-80.
Ismail, N. A., & King, M. (2005). Firm performance and AIS alignment in Malaysian SMEs. *International Journal of Accounting Information Systems, 6*(4), 241-259. doi: 10.1016/j.accinf.2005.09.001
Jacobson, L., & Joanne, K. (2009). *Contextual and individual predictors of counterproductive work behaviors.* Ph.D. 3357268, Arizona State University, United States -- Arizona. Retrieved from http://search.proquest.com/docview/304832971 ProQuest Dissertations & Theses (PQDT) database.
Jans, M., Lybaert, N., & Vanhoof, K. (2010). Internal fraud risk reduction: Results of a data mining case study. *International Journal of Accounting Information Systems, 11*(1), 17-41. doi: 10.1016/j.accinf.2009.12.004
Jarvis, C. B., Mackenzie, S. B., Podsakoff, P. M., Giliatt, N., & Mee, J. F. (2003). A critical review of construct indicators and measurement model misspecification in marketing and consumer research. *Journal of Consumer Research, 30*(2), 199-218.
Jaworski, B. J., & Young, S. M. (1992). Dysfunctional behavior and management control: An empirical study of marketing managers. *Accounting,*

Organizations and Society, 17(1), 17-35. doi: 10.1016/0361-3682(92)90034-p

Jensen, J. M., & Patel, P. C. (2011). Predicting counterproductive work behavior from the interaction of personality traits. *Personality and Individual Differences, 51*(4), 466-471. doi: 10.1016/j.paid.2011.04.016

Jia, D., Bhatti, A., & Nahavandi, S. (2012). The impact of self-efficacy and perceived system efficacy on effectiveness of virtual training systems. *Behaviour & Information Technology, 33*(1), 16-35. doi: 10.1080/0144929X.2012.681067

Jiang, L., & Li, X. (2010). Discussions on the improvement of the internal control in SMEs. *International Journal of Business and Management, 5*(9), 214-216.

Jimmieson, N. L., Peach, M., & White, K. M. (2008). Utilizing the theory of planned behavior to inform change management: An investigation of employee intentions to support organizational change. *Journal of Applied Behavioral Science, 44*(2), 237 - 262.

Jon, J., Carter, P. E., & Zmud, R. W. (2005). A comprehensive conceptualization of post-adoptive behaviors associated with information technology enabled work systems. *MIS Quarterly, 29*(3), 525-557.

Jung, T., Scott, T., Davies, H. T. O., Bower, P., Whalley, D., McNally, R., & Mannion, R. (2009). Instruments for exploring organizational culture: A review of the literature. *Public Administration Review, 69*(6), 1087-1096. doi: 10.1016/s0925-7535(00)00013-8

Kaiser, H. F. (1974). An index of factorial simplicity. *Psychometrika, 39*(1), 31-36. doi: 10.1007/BF02291575

Karanja, E., Zaveri, J., & Ahmed, A. (2013). How do MIS researchers handle missing data in survey-based research: A content analysis approach. *International Journal of Information Management, 33*(5), 734-751. doi: http://dx.doi.org/10.1016/j.ijinfomgt.2013.05.002

Kenett, R., & Salini, S. (2011). *Statistics in practice: A modern analysis of customer surveys - with applications using R*. Hoboken, NJ, USA: Wiley.

Kerber, R. (2007). Latest TJX offer includes checks or vouchers, *Boston Globe*, pp. D.1-D.1. Retrieved from http://search.proquest.com/docview/405099917

. Key findings from the 2013 US state of cybercrime survey. (2013): PricewaterhouseCoopers.

Kidwell, B., & Jewell, R. D. (2003). An examination of perceived behavioral control: Internal and external influences on intention. *Psychology and Marketing, 20*(7), 625-642. doi: 10.1002/mar.10089

Kim, H.-J., Mannino, M., & Nieschwietz, R. J. (2009a). Information technology acceptance in the internal audit profession: Impact of technology features and complexity. *International Journal of Accounting Information Systems, 10*(4), 214-228. doi: http://dx.doi.org/10.1016/j.accinf.2009.09.001

Kim, H. J., Mannino, M., & Nieschwietz, R. J. (2009b). Information technology acceptance in the internal audit profession: Impact of technology features and complexity. *International Journal of Accounting Information Systems, 10*(4), 214-228. doi: 10.1016/j.accinf.2009.09.001

Kim, T. G., Hornung, S., & Rousseau, D. M. (2011). Change-supportive employee behavior: Antecedents and the moderating role of time. *Journal of Management, 37*(6), 1664-1693. doi: 10.1177/0149206310364243

Kline, R. B. (2010). *Principles and practice of structural equation modeling, third edition* (3 ed.). New York: Guilford Publications.

Kock, N. (2011). Using WarpPLS in e-collaboration studies: Mediating effects, control and second order variables, and algorithm choices. *International Journal of e-Collaboration, 7*(3), 1-13.

Kock, N. (2013). *WarpPLS 4.0 user manual*. Loredo, Texas: ScriptWarp Systems.

Kock, N. (2015). How likely is Simpson's paradox in path models? *International Journal of e-Collaboration, 11*(1), 1-7.

Kock, N., & Lynn, G. S. (2012). Lateral collinearity and misleading results in variance-based SEM: An illustration and recommendations. *Journal of the Association for Information Systems, 13*(7), 546-580.

Kolkowska, E., & Dhillon, G. (2013). Organizational power and information security rule compliance. *Computers & Security, 33*(0), 3-11. doi: http://dx.doi.org/10.1016/j.cose.2012.07.001

Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computers & Security, 28*(7), 509-520. doi: 10.1016/j.cose.2009.04.006

Kroll, C. N., & Song, P. (2013). Impact of multicollinearity on small sample hydrologic regression models. *Water Resources Research, 49*(6), 3756-3769. doi: 10.1002/wrcr.20315

Kwahk, K.-Y., & Ahn, H. (2010). Moderating effects of localization differences on ERP use: A socio-technical systems perspective. *Computers in Human Behavior, 26*(2), 186-198. doi: 10.1016/j.chb.2009.10.006

Lacey, D. (2010). Understanding and transforming organizational security culture. *Information Management & Computer Security, 18*(1), 4-13. doi: 10.1108/09685221011035223

Leach, J. (2003). Improving user security behaviour. *Computers & Security, 22*(8), 685-692. doi: 10.1016/s0167-4048(03)00007-5

Lee, A. S. (2001). Editor's comments. *MIS Quarterly, 25*(1), III-III.

Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: Determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems, 18*(2), 177-187. doi: http://dx.doi.org/10.1057/ejis.2009.11

Leonard, L. N. K., Cronan, T. P., & Kreie, J. (2004). What influences IT ethical behavior intentions—planned behavior, reasoned action, perceived importance, or individual characteristics? *Information & Management, 42*(1), 143-158. doi: http://dx.doi.org/10.1016/j.im.2003.12.008

Leslie, L. L. (1972). Are high response rates essential to valid surveys? *Social Science Research, 1*(3), 323-334. doi: http://dx.doi.org/10.1016/0049-089X(72)90080-4

Li, C., Peters, G. F., Richardson, V. J., & Watson, M. W. (2012). The Consequences of Information Technology Control Weaknesses on Management Information Systems: The Case of Sarbanes-Oxley Internal Control Reports. *MIS Quarterly, 36*(1), 179.

Li, H., Zhang, J., & Sarathy, R. (2010). Understanding compliance with internet use policy from the perspective of rational choice theory. *Decision Support Systems, 48*(4), 635-645. doi: http://dx.doi.org/10.1016/j.dss.2009.12.005

Liao, Q., Luo, X., Gurung, A., & Li, L. (2009). Workplace management and employee misuse: Does punishment matter? *The Journal of Computer Information Systems, 50*(2), 49-59.

Lieberman. (2011). 2011 Survey of IT Professionals: Password Practices and Outcomes. 1-6. Retrieved from Liberman Software website: http://www.liebsoft.com/uploadedFiles/wwwliebsoftcom/MARCOM/Press/Content/2011-Password-Survey.pdf

Lieberman, A. Z., & Whinston, A. B. (1975). A structuring of an events-accounting information system. *The Accounting Review, 50*(2), 246-258.

Lin, T.-C., & Huang, C.-C. (2010). Withholding effort in knowledge contribution: The role of social exchange and social cognitive on project teams. *Information & Management, 47*(3), 188-196. doi: http://dx.doi.org/10.1016/j.im.2010.02.001

Little, R. J. A. (1988). A test of missing completely at random for multivariate data with missing values. *Journal of the American Statistical Association, 83*(404), 1198-1202. doi: 10.2307/2290157

Lowry, P. B., & Gaskin, J. (2014). Partial least squares (PLS) structural equation modeling (SEM) for building and testing behavioral causal theory: When to choose it and how to use it. *Professional Communication, IEEE Transactions on, 57*(2), 123-146. doi: 10.1109/TPC.2014.2312452

Lowry, P. B., Posey, C., Roberts, T., & Bennett, R. (2014). Is your banker leaking your personal information? The roles of ethics and individual-level cultural characteristics in predicting organizational computer abuse. *Journal of Business Ethics, 121*(3), 385-401. doi: 10.1007/s10551-013-1705-3

Lynch, A., & Gomaa, M. (2003). Understanding the potential impact of information technology on the susceptibility of organizations to fraudulent employee behavior. *International Journal of Accounting Information Systems, 4*(4), 295-308. doi: 10.1016/j.accinf.2003.04.001

Lynch, D. M. (2006). Securing against insider attacks. *Information Security Journal, 15*(5), 39-47.

Magklaras, G. B., & Furnell, S. M. (2001). Insider Threat Prediction Tool: Evaluating the probability of IT misuse. *Computers & Security, 21*(1), 62-73. doi: 10.1016/s0167-4048(02)00109-8

Magklaras, G. B., & Furnell, S. M. (2002). Insider threat prediction tool: Evaluating the probability of IT misuse. *Computers & Security, 21*(1), 62-73. doi: 10.1016/s0167-4048(02)00109-8

Magklaras, G. B., & Furnell, S. M. (2005). A preliminary model of end user sophistication for insider threat prediction in IT systems. *Computers & Security, 24*(5), 371-380. doi: 10.1016/j.cose.2004.10.003

Magklaras, G. B., & Furnell, S. M. (n.d.). *The insider misuse threat survey: Investigating IT misuse from legitimate users*. University of Oslo. Retrieved from http://folk.uio.no/georgios/papers/IWAR04MagklarasFurnell.pdf

Mao, E., & Palvia, P. (2008). Exploring the effects of direct experience on IT use: An organizational field study. *Information & Management, 45*(4), 249-256. doi: http://dx.doi.org/10.1016/j.im.2008.02.007

Market Studies. (2007). *ARC Advisory Group*. Retrieved from http://www.arcweb.com/study-brochures/Study_erp.pdf

Markus, M. L., & Pfeffer, J. (1983). Power and the design and implementation of accounting and control systems. *Accounting, Organizations and Society, 8*(2–3), 205-218. doi: 10.1016/0361-3682(83)90028-4

Martinez-Moyano, I. J., Conrad, S. H., & Andersen, D. F. (2011). Modeling behavioral considerations related to information security. *Computers & Security, 30*(6–7), 397-409. doi: 10.1016/j.cose.2011.03.001

Mascha, M. F., & Smedley, G. (2007). Can computerized decision aids do "damage"? A case for tailoring feedback and task complexity based on task experience. *International Journal of Accounting Information Systems, 8*(2), 73-91. doi: 10.1016/j.accinf.2007.03.001

Mauldin, E. G., & Richtermeyer, S. B. (2004). An analysis of ERP annual report disclosures. *International Journal of Accounting Information Systems, 5*(4), 395-416. doi: 10.1016/j.accinf.2004.04.005

Mauldin, E. G., & Ruchala, L. V. (1999). Towards a meta-theory of accounting information systems. *Accounting, Organizations and Society, 24*(4), 317-331. doi: 10.1016/s0361-3682(99)00006-9

McCarthy, W. E. (1982). The REA accounting model: A generalized framework for accounting systems in a shared data environment. *The Accounting Review, 57*(3), 554-578.

Meehl, P. E. (1990). Why summaries of research on psychological theories are often uninterpretable. [Monograph supplement]. *Psychological Reports, 66*(1), 195-244.

Mehta, N., & Hall, D. (2014). Information technology and knowledge in software development teams: The role of project uncertainty. *Information & Management, 51*(4), 417-429. doi: http://dx.doi.org/10.1016/j.im.2014.02.007

Mehta, P. D. (2001). Control variable in research. In N. J. Smelser & P. B. Baltes (Eds.), *International Encyclopedia of the Social & Behavioral Sciences* (pp. 2727-2730). Oxford: Pergamon.

Merchant, K. A., Van der Stede, W. A., & Zheng, L. (2003). Disciplinary constraints on the advancement of knowledge: the case of organizational incentive systems. *Accounting, Organizations and Society, 28*(2–3), 251-286. doi: 10.1016/s0361-3682(01)00051-4

Meyer, M. H., & Curley, K. F. (1991). An applied framework for classifying the complexity of knowledge-based systems. *MIS Quarterly, 15*(4), 455-472. doi: 10.2307/249450

Meyer, M. H., & Curley, K. F. (1995). The impact of knowledge and technology complexity on information systems development. *Expert Systems with Applications, 8*(1), 111-134. doi: http://dx.doi.org/10.1016/0957-4174(94)E0003-D

Mohamadali, N. A. K. (2012). *Exploring new factors and the question of 'which' in user acceptance studies of healthcare software.* Doctor of Philosophy, University of Nottingham, Nottingham.

Möller, S., Ben-Asher, N., Engelbrecht, K.-P., Englert, R., & Meyer, J. (2011). Modeling the behavior of users who are confronted with security mechanisms. *Computers & Security, 30*(4), 242-256. doi: 10.1016/j.cose.2011.01.001

Moody, G. D., & Siponen, M. (2013). Using the theory of interpersonal behavior to explain non-work-related personal use of the Internet at work. *Information & Management*, *50*(6), 322-335. doi: http://dx.doi.org/10.1016/j.im.2013.04.005

Mook, B. (2012). U.S. District Court in Greenbelt: CoStar wins $3.6M in password-sharing case, *The Daily Record*.

Moore, A., Cappelli, D., & Trzeciak, R. (2008). The "big picture" of insider it sabotage across U.S. critical infrastructures (S. E. Institute, Trans.): Carnegie Mellon University.

Moqbel, M. (2012). *The effects of the use of social networking sites in the workplace on job performance.* PhD Doctorate Texas A&M International Univeristy, Texas.

Muijen, J. J. v., Koopman, P., Witte, K. D., Cock, G. D., Susanj, Z., Lemoine, C., . . . Turnipseed, D. (1999). Organizational culture: The focus questionnaire. *European Journal of Work and Organizational Psychology*, *8*(4), 551-568. doi: 10.1080/135943299398168

Musa, N. (2011). *Role of the boards and senior management within formal, technical and informal components: IS/IT security governance in the malaysian publicly listed companies.* Doctor of Philosophy Doctorate thesis, University of Tasmania, Tasmania.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., & Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems*, *18*(2), 126-139. doi: http://dx.doi.org/10.1057/ejis.2009.10

Neu, D., Everett, J., Rahaman, A. S., & Martinez, D. (2012). Accounting and networks of corruption. *Accounting, Organizations and Society*(2012). doi: 10.1016/j.aos.2012.01.003

Nicholson, A., Webber, S., Dyer, S., Patel, T., & Janicke, H. (2012). SCADA security in the light of cyber-warfare. *Computers & Security*(0). doi: 10.1016/j.cose.2012.02.009

Nicolaou, A. I. (2000). A contingency model of perceived effectiveness in accounting information systems: Organizational coordination and control effects. *International Journal of Accounting Information Systems*, *1*(2), 91-105. doi: 10.1016/s1467-0895(00)00006-3

Nikolaidis, I. (2009). Risk homeostasis and network security [Editor's Note]. *Network, IEEE*, *23*(1), 2-2. doi: 10.1109/MNET.2009.4804316

Nunnally, J. C., & Bernstein, I. H. (1994). *Psychometric theory*. New York: McGraw Hill.

O'Leary, D. E. (2010). Enterprise ontologies: Review and an activity theory approach. *International Journal of Accounting Information Systems*, *11*(4), 336-352. doi: 10.1016/j.accinf.2010.09.006

Otley, D., & Fakiolas, A. (2000). Reliance on accounting performance measures: dead end or new beginning? *Accounting, Organizations and Society*, *25*(4–5), 497-510. doi: 10.1016/s0361-3682(98)00007-5

Otley, D. T. (1978). Budget use and managerial performance. *Journal of Accounting Research*, *16*(1), 122-149.

Ouellette, J. A., & Wood, W. (1998). Habit and intention in everyday life: The multiple processes by which past behavior predicts future behavior. *Psychological Bulletin, 124*(1), 54-74. doi: 10.1037/0033-2909.124.1.54

Padayachee, K. (2012a). Taxonomy of compliant information security behavior. *Computers & Security, 31*(5). doi: 10.1016/j.cose.2012.04.004

Padayachee, K. (2012b). Taxonomy of compliant information security behavior. *Computers & Security, 31*(5), 673-680. doi: http://dx.doi.org/10.1016/j.cose.2012.04.004

Paino, H., Ismail, Z., & Smith, M. (2010). Dysfunctional audit behaviour: an exploratory study in Malaysia. *Asian Review of Accounting, 18*(2), 162-173. doi: 10.1108/13217341011059417

Pallant, J. (2010). *SPSS Survival Manual* (5 ed.): Open University Press.

Patrick, A. S. (2008). *Monitoring corporate password sharing using social network analysis*. Paper presented at the International Sunbelt Social Network Conference, Florida.

Pavlou, P. A., & Fygenson, M. (2006). Understanding and predicting electronic commerce adoption: An extension of the theory of planned behavior. *MIS Quarterly, 30*(1), 115-143. doi: 10.2307/25148720

Peace, A. G., Galletta, D. F., & Thong, J. Y. L. (2003). Software piracy in the workplace: A model and empirical test. *Journal of Management Information Systems, 20*(1), 153-177.

Peel, D. (2006). An analysis of the impact of SME organisational culture on coaching and mentoring. *International Journal of Evidence Based Coaching and Mentoring, 4*(1), 9-19.

Pelled, L. H., & Xin, K. R. (1999). Down and out: An investigation of the relationship between mood and employee withdrawal behavior. *Journal of Management, 25*(6), 875-895. doi: 10.1177/014920639902500605

Peltier-Rivest, D., & Lanoue, N. (2011). Thieves from within: Occupational fraud in Canada. *Journal of Financial Crime, 19*(1), 54 - 64.

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & Security*(0). doi: 10.1016/j.cose.2011.12.010

Phau, I., & Ng, J. (2010). Predictors of usage intentions of pirated software. *Journal of Business Ethics, 94*(1), 23-37. doi: DOI:10.1007/s10551-009-0247-1

Phyo, A. H., & Furnell, S. M. (n.d.). *A detection-oriented classification of insider IT misuse*. Article. Dept. of Computer Science University College London. Retrieved from http://hornbeam.cs.ucl.ac.uk/hcs/teaching/ga10/lec4extra/detection.pdf

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology, 88*(5), 879-903. doi: 10.1037/0021-9010.88.5.879

Podsakoff, P. M., MacKenzie, S. B., & Podsakoff, N. P. (2012). Sources of method bias in social science research and recommendations on how to control it. *Annual Review of Psychology, 63*(1), 539-569. doi: doi:10.1146/annurev-psych-120710-100452

Pole, J. D., & Bondy, S. J. (2010). *Control Variables. Encyclopedia of Research Design. SAGE Publications, Inc*. Thousand Oaks, CA: SAGE Publications, Inc.

Posey, C., Bennett, R. J., & Roberts, T. L. (2011). Understanding the mindset of the abusive insider: An examination of insiders' causal reasoning following internal security changes. *Computers & Security, 30*(6–7), 486-497. doi: 10.1016/j.cose.2011.05.002

Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., & Courtney, J. F. (2013). Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. *MIS Quarterly, 37*(4), 1189-1210.

Post, G. V., & Kagan, A. (2007). Evaluating information security tradeoffs: Restricting access can interfere with user tasks. *Computers & Security, 26*(3), 229-237. doi: 10.1016/j.cose.2006.10.004

Poston, R. S., & Grabski, S. V. (2000). Accounting information systems research: Is it another QWERTY? *International Journal of Accounting Information Systems, 1*(1), 9-53. doi: 10.1016/s1467-0895(99)00003-2

Pratt, J., & Beaulieu, P. (1992). Organizational culture in public accounting: Size, technology, rank, and functional area. *Accounting, Organizations and Society, 17*(7), 667-684. doi: 10.1016/0361-3682(92)90018-n

Probst, C., Hansen, R., & Nielson, F. (2007). Where can an insider attack? Formal aspects in security and trust. In T. Dimitrakos, F. Martinelli, P. Ryan & S. Schneider (Eds.), (Vol. 4691, pp. 127-142): Springer Berlin / Heidelberg.

Quinn, R. E. (1988). *Beyond rational management: mastering the paradoxes and competing demands of high performance* (1st ed.). San Francisco: Jossey-Bass.

Ramadhan, S., Joshi, P. L., & Hameed, S. A. (2003). Accountants' perceptions of internal control problems associated with the use of computerized accounting systems: Evidence from Bahrain. [Journal Article]. *The Review of Business Information Systems, 7*(1), 59-72.

Randall, D. M., & Gibson, A. M. (1991). Ethical decision making in the medical profession: An application of the theory of planned behavior. *Journal of Business Ethics, 10*(2), 111-111.

Reinartz, W., Haenlein, M., & Henseler, J. (2009). An empirical comparison of the efficacy of covariance-based and variance-based SEM. *International Journal of Research in Marketing, 26*(4), 332-344. doi: http://dx.doi.org/10.1016/j.ijresmar.2009.08.001

Renaud, K., & Goucher, W. (2012). Health service employees and information security policies: an uneasy partnership? *Information Management & Computer Security, 20*(4), 296-311.

Rhee, H.-S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security, 28*(8), 816-826. doi: http://dx.doi.org/10.1016/j.cose.2009.05.008

Rhodes, R. E., & Courneya, K. S. (2003). Modelling the theory of planned behaviour and past behaviour. *Psychology, Health & Medicine, 8*(1), 57-69. doi: 10.1080/1354850021000059269

Richardson, R. (2011). 2010/2011 CSI computer crime and security survey: Computer Security Institute.

Rigdon, E. E. (1998). Structural equation modeling. In G. A. Marcoulides (Ed.), *Modern methods for business research* (pp. 251-294). Mahwah, New Jersey: Lawrence Erlbaum Associates.

Ringle, C. M., Sarstedt, M., & Straub, D. W. (2012). Editor's comments: a critical look at the use of PLS-SEM in MIS quarterly. *MIS Quarterly, 36*(1), iii-xiv.

Rizzuto, T. E., Schwarz, A., & Schwarz, C. (2014). Toward a deeper understanding of, information technology (it) adoption: a multilevel analysis. *Information & Management, 51*(4), 479-487. doi: http://dx.doi.org/10.1016/j.im.2014.02.005

Robey, D., & Azevedo, A. (1994). Cultural analysis of the organizational consequences of information technology. *Accounting, Management and Information Technologies, 4*(1), 23-37. doi: http://dx.doi.org/10.1016/0959-8022(94)90011-6

Rodgers, W., & Guiral, A. (2011). Potential model misspecification bias: Formative indicators enhancing theory for accounting researchers. *The International Journal of Accounting, 46*(1), 25-50. doi: 10.1016/j.intacc.2010.12.002

Rotter, J. B. (1960). Some implications of a social learning theory for the prediction of goal directed behavior from testing procedures. *Psychological Review, 67*(5), 301-316. doi: 10.1037/h0039601

Rotter, J. B. (1966). Generalized expectancies for internal versus external control of reinforcement. *Psychological Monographs: General and Applied, 80*(1), 1-28. doi: 10.1037/h0092976

Roy Sarkar, K. (2010). Assessing insider threats to information security using technical, behavioural and organisational measures. *Information Security Technical Report, 15*(3), 112-133. doi: 10.1016/j.istr.2010.11.002

Rubin, D. B. (1976). Inference and missing data. *Biometrika, 63*(3), 581-592. doi: 10.2307/2335739

Sarstedt, M., Ringle, C. M., Henseler, J., & Hair, J. F. (2014). On the emancipation of PLS-SEM: A commentary on Rigdon (2012). *Long Range Planning, 47*(3), 154-160. doi: http://dx.doi.org/10.1016/j.lrp.2014.02.007

Schafer, J. L., & Graham, J. W. (2002). Missing data: Our view of the state of the art. *Psychological Methods, 7*(2), 147-177. doi: 10.1037/1082-989x.7.2.147

Schatzki, T. R. (2005). Peripheral vision: The sites of organizations. *Organization Studies, 26*(3), 465-484. doi: 10.1177/0170840605050876

Scheffer, J. (2002). Dealing with missing data. *Research letters in the information and mathematical sciences, 3*(1), 153-160.

Schein, E. H. (1990). Organizational culture. *American Psychologist, 45*(2), 109-119. doi: 10.1037/0003-066x.45.2.109

Schmitt, T. A. (2011). Current methodological considerations in exploratory and confirmatory factor analysis. *Journal of Psychoeducational Assessment, 29*(4), 304-321. doi: 10.1177/0734282911406653

Schoenberg, N. E., & Ravdal, H. (2000). Using vignettes in awareness and attitudinal research. *International Journal of Social Research Methodology, 3*(1), 63-74. doi: 10.1080/136455700294932

Schultz, E. E. (2002). A framework for understanding and predicting insider attacks. *Computers & Security, 21*(6), 526-531. doi: 10.1016/s0167-4048(02)01009-x

Schumacker, R. E., & Lomax, R. G. (2012). *A beginner's guide to structural equation modeling : Third edition* (3 ed.). Hoboken: Taylor and Francis.

Selamat, Z., & Jaffar, N. (2011). Information technology acceptance: From perspective of Malaysian bankers. *International Journal of Business and Management, 6*(1), 207-217.

Shabtai, A., Bercovitch, M., Rokach, L., & Elovici, Y. (2014). Optimizing data misuse detection. *ACM Trans. Knowl. Discov. Data, 8*(3), 1-23. doi: 10.1145/2611520

Shafer, W. E. (2008). Ethical climate in Chinese CPA firms. *Accounting, Organizations and Society, 33*(7–8), 825-835. doi: 10.1016/j.aos.2007.08.002

Shameli-Sendi, A., Cheriet, M., & Hamou-Lhadj, A. (2014). Taxonomy of intrusion risk assessment and response system. *Computers & Security, 45*(0), 1-16. doi: http://dx.doi.org/10.1016/j.cose.2014.04.009

Shang, S. S. C. (2011). Dual strategy for managing user resistance with business integration systems. *Behaviour & Information Technology, 31*(9), 909-925. doi: 10.1080/0144929x.2011.553744

Sharma, S., Durand, R. M., & Gur-Arie, O. (1981). identification and analysis of moderator variables. *Journal of Marketing Research, 18*(August 1981), 291-300.

Siew Imm, N., Lee, J. A., & Soutar, G. N. (2007). Are Hofstede's and Schwartz's value frameworks congruent? *International Marketing Review, 24*(2), 164-180. doi: 10.1108/02651330710741802

Singh, S., Cabraal, A., Demosthenous, C., Astbrink, G., & Furlong, M. (2007). Security design based on social and cultural practice: Sharing of passwords. In N. Aykin (Ed.), *Usability and Internationalization. Global and Local User Interfaces* (Vol. 4560, pp. 476-485): Springer Berlin Heidelberg.

Siponen, M., Adam Mahmood, M., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management, 51*(2), 217-224. doi: http://dx.doi.org/10.1016/j.im.2013.08.006

Siponen, M., Vance, A., & Willison, R. (2012). New insights into the problem of software piracy: The effects of neutralization, shame, and moral beliefs. *Information & Management, 49*(7), 334-341. doi: 10.1016/j.im.2012.06.004

Smith, J. R., Terry, D. J., Manstead, A. S. R., Louis, W. R., Kotterman, D., & Wolfs, J. (2008). The attitude-behavior relationship in consumer conduct: The role of norms, past behavior, and self-identity. *The Journal of Social Psychology, 148*(3), 311-333. doi: 10.1111/j.1559-1816.1998.tb01685.x. 10.1037/0033-2909.124.1.54. 10.1111/j.1559-1816.1998.tb01683.x

Smith, M. (2011). *Research methods in accounting* (2nd ed.). London: Sage.

Son, J.-Y. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management, 48*(7), 296-302. doi: http://dx.doi.org/10.1016/j.im.2011.07.002

Sorter, G. H. (1969). An "events" approach to basic accounting theory. *Accounting Review, 44*(1), 12-19.

Spears, J. L., & Barki, H. (2010). User Participation in Information Systems Security Risk Management. *MIS Quarterly, 34*(3), 503.

Speier, C. (2006). The influence of information presentation formats on complex task decision-making performance. *International Journal of Human-*

Computer Studies, 64(11), 1115-1131. doi: http://dx.doi.org/10.1016/j.ijhcs.2006.06.007

Stanton, J. M., & Stam, K. R. (2006). *The visible employee: Using workplace monitoring and surveillance to protect information assets without compromising employee privacy or trust*. Medford, NJ: Information Today, Inc.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security, 24*(2), 124-133. doi: 10.1016/j.cose.2004.07.001

Stoel, M. D., & Muhanna, W. A. (2011). IT internal control weaknesses and firm performance: An organizational liability lens. *International Journal of Accounting Information Systems, 12*(4), 280-304. doi: 10.1016/j.accinf.2011.06.001

Sun, J., Ahluwalia, P., & Koong, K. S. (2011). The more secure the better? A study of information security readiness. *Industrial Management and Data Systems, 111*(4), 570-588.

Sutton, S. G. (2000). The changing face of accounting in an information technology dominated world. *International Journal of Accounting Information Systems, 1*(1), 1-8. doi: 10.1016/s1467-0895(99)00002-0

Sutton, S. G. (2004a). Editor's comments. *International Journal of Accounting Information Systems, 5*(3), 281-284. doi: 10.1016/j.accinf.2004.09.002

Sutton, S. G. (2004b). Editors comments: Rediscovering our IS roots. *International Journal of Accounting Information Systems, 5*(1), 1-4. doi: 10.1016/j.accinf.2004.02.001

Sutton, S. G. (2006). Enterprise systems and the re-shaping of accounting systems: A call for research. *International Journal of Accounting Information Systems, 7*(1), 1-6. doi: 10.1016/j.accinf.2006.02.002

Sutton, S. G. (2010a). *The fundamental role of technology in accounting: Researching reality* (Vol. 13): Emerald Group Publishing Limited.

Sutton, S. G. (2010b). A research discipline with no boundaries: Reflections on 20 years of defining AIS research. *International Journal of Accounting Information Systems, 11*(4), 289-296. doi: 10.1016/j.accinf.2010.09.004

Sutton, S. G., & Arnold, V. (2011). Focus group methods: Using interactive and nominal groups to explore emerging technology-driven phenomena in accounting and information systems. *International Journal of Accounting Information Systems*(0). doi: 10.1016/j.accinf.2011.10.001

Sveen, F. O., Torres, J. M., & Sarriegi, J. M. (2009). Blind information security strategy. *International Journal of Critical Infrastructure Protection, 2*(3), 95-109. doi: 10.1016/j.ijcip.2009.07.003

Tabachnick, B. G., & Fidell, L. S. (2007). *Using multivariate statistics* (5 ed.). Boston: Allyn and Bacon.

Tams, S. (2013). Moving cultural information systems research toward maturity. *Information Technology & People, 26*(4), 383-400. doi: doi:10.1108/ITP-11-2012-0138

Tapiador, J. E., & Clark, J. A. (2011). Masquerade mimicry attack detection: A randomised approach. *Computers & Security, 30*(5), 297-310. doi: 10.1016/j.cose.2011.05.004

Taskin, N. (2011). *Flexibility and strategic alignment of enterprise resource planning systems with business strategies: An empirical study*. Doctor of Philosophy, University of British Coumbia, Okanagan.

Tavakol, M., & Dennick, R. (2011). Making sense of Cronbach's alpha. *International Journal of Medical Education, 2*, 53-55. doi: 10.5116/ijme.4dfb.8dfd

Terry, D. J., Hogg, M. A., & White, K. M. (1999). The theory of planned behaviour: Self-identity, social identity and group norms. *British Journal of Social Psychology, 38*(3), 225-244. doi: 10.1348/014466699164149

Terry, D. J., & O'Leary, J. E. (1995). The theory of planned behaviour: The effects of perceived behavioural control and self-efficacy. *British Journal of Social Psychology, 34*(2), 199-220. doi: 10.1111/j.2044-8309.1995.tb01058.x

Thompson, R. L., Higgins, C. A., & Howell, J. M. (1991). Personal computing: Toward a conceptual model of utilization. *MIS Quarterly, 15*(1), 125-143.

Trafimow, D., Sheeran, P., Conner, M., & Finlay, K. A. (2002). Evidence that perceived behavioural control is a multidimensional construct: Perceived control and perceived difficulty. *British Journal of Social Psychology, 41*(1), 101-121. doi: 10.1348/014466602165081

Treiblmaier, H., & Filzmoser, P. (2010). Exploratory factor analysis revisited: How robust methods support the detection of hidden multivariate data structures in IS research. *Information & Management, 47*(4), 197-207. doi: http://dx.doi.org/10.1016/j.im.2010.02.002

Vaassen, E. H. J., & Hunton, J. E. (2009). An eclectic approach to accounting information systems. *International Journal of Accounting Information Systems, 10*(4), 173-176. doi: 10.1016/j.accinf.2009.10.004

Van der Stede, W. A. (2000). The relationship between two consequences of budgetary controls: budgetary slack creation and managerial short-term orientation. *Accounting, Organizations and Society, 25*(6), 609-622. doi: 10.1016/s0361-3682(99)00058-6

Van der Stede, W. A., Young, S. M., & Chen, C. X. (2005). Assessing the quality of evidence in empirical management accounting research: The case of survey studies. *Accounting, Organizations and Society, 30*(7–8), 655-684. doi: http://dx.doi.org/10.1016/j.aos.2005.01.003

Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security, 29*(4), 476-486. doi: http://dx.doi.org/10.1016/j.cose.2009.10.005

Vance, A., Lowry, P., & Eggett, D. (2013). Using accountability to reduce access policy violations in information systems. *Journal of Management Information Systems, 29*(4), 263-290.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information & Management, 49*(3–4), 190-198. doi: http://dx.doi.org/10.1016/j.im.2012.04.002

Vasarhelyi, M. A., & Alles, M. G. (2008). The "now" economy and the traditional accounting reporting model: Opportunities and challenges for AIS research. *International Journal of Accounting Information Systems, 9*(4), 227-239. doi: 10.1016/j.accinf.2008.09.002

Velpula, V. B., & Gudipudi, D. (2009). Behavior-anomaly-based system for detecting insider attacks and data mining. *International Journal of Recent Trends in Engineering, 1*(2), 261-266.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quaterly, 27*(3), 425-478.

Venkatesh, V., Morris, M. G., Gordon, B. D., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly, 27*(3), 425-478.

Wagner, C. H. (1982). Simpson's paradox in real life. *The American Statistician, 36*(1), 46-48. doi: 10.2307/2684093

Wall, D. S. (2013). Enemies within: Redefining the insider threat in organizational security policy. *Security Journal, 26*(2), 107-124. doi: http://dx.doi.org/10.1057/sj.2012.1

Wallace, L. G., & Sheetz, S. D. (2014). The adoption of software measures: A technology acceptance model (TAM) perspective. *Information & Management, 51*(2), 249-259. doi: http://dx.doi.org/10.1016/j.im.2013.12.003

Walsh, G., Evanschitzky, H., & Wunderlich, M. (2008). Identification and analysis of moderator variables: Investigating the customer satisfaction-loyalty link. *European Journal of Marketing, 42*(9/10), 977-1004. doi: http://dx.doi.org/10.1108/03090560810891109

Wang, J. (2012). *Wiley series in probability and statistics : Structural equation modeling with Mplus : Methods and applications (3rd edition)*. Somerset, NJ, USA: John Wiley & Sons.

Wang, J., Gupta, M., & Rao, H. R. (2015). Insider threats in a financial institution: Analysis of attack-proneness of information systems applications. *MIS Quarterly, 39*(1), 91-112.

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems, 18*(2), 101-105. doi: http://dx.doi.org/10.1057/ejis.2009.12

Westlund, A. H., Källström, M., & Parmler, J. (2008). SEM-based customer satisfaction measurement: On multicollinearity and robust PLS estimation. *Total Quality Management & Business Excellence, 19*(7-8), 855-869. doi: 10.1080/14783360802159527

Wilde, G. J. S. (1998). Risk homeostasis theory: an overview. *Injury Prevention, 4*(2), 89-91. doi: 10.1136/ip.4.2.89

Wilkinson, L. (1999). Statistical methods in psychology journals: Guidelines and explanations. *American Psychologist, 54*(8), 594-604. doi: 10.1037/0003-066x.54.8.594

Williams, P. A. H. (2008). In a 'trusting' environment, everyone is responsible for information security. *Information Security Technical Report, 13*(4), 207-215. doi: 10.1016/j.istr.2008.10.009

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly, 37*(1), 1-20.

Witte, K. D., & Muijen, J. J. v. (1999). Organizational culture: Critical questions for researchers and practitioners. *European Journal of Work and Organizational Psychology, 8*(4), 583-595. doi: 10.1080/135943299398186

Wold, H. (1985). Partial least square. In S. Kotz & N. L. Johnson (Eds.), *Encyclopedia of statistical sciences* (Vol. 6, pp. 581-591). New York: Wiley.

Wolf, M., Haworth, D., & Pietron, L. (2011). Measuring an information security awareness program. *The Review of Business Information Systems, 15*(3), 9-21.

Workman, M. (2005). Expert decision support system use, disuse, and misuse: A study using the theory of planned behavior. *Computers in Human Behavior, 21*(2), 211-231. doi: 10.1016/j.chb.2004.03.011

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior, 24*(6), 2799-2816. doi: http://dx.doi.org/10.1016/j.chb.2008.04.005

Worrell, J., Wasko, M., & Johnston, A. (2011). Social network analysis in accounting information systems research. *International Journal of Accounting Information Systems, 2011*(0). doi: 10.1016/j.accinf.2011.06.002

Worrell, J., Wasko, M., & Johnston, A. (2013). Social network analysis in accounting information systems research. *International Journal of Accounting Information Systems, 14*(2), 127-137. doi: http://dx.doi.org/10.1016/j.accinf.2011.06.002

Yan, Z., & Sin, K.-f. (2013). Inclusive education: teachers' intentions and behaviour analysed from the viewpoint of the theory of planned behaviour. *International Journal of Inclusive Education, 18*(1), 72-85. doi: 10.1080/13603116.2012.757811

Yeow, A., & Faraj, S. (2011). Using narrative networks to study enterprise systems and organizational change. *International Journal of Accounting Information Systems, 12*(2), 116-125. doi: 10.1016/j.accinf.2010.12.005

Zolait, A. H. S. (2011). The nature and components of perceived behavioural control as an element of theory of planned behaviour. *Behaviour & Information Technology, 33*(1), 65-85. doi: 10.1080/0144929X.2011.630419

Appendices

Appendix 1

Item loadings for exploratory factor analysis

	Factors									
	1	2	3	4	5	6	7	8	9	10
support1					0.784					
support2					0.569					
support3					0.594					
support4					0.634					
support5					0.324					
support6					0.717					
innovation1						0.639				
innovation2						0.766				
innovation3						0.703				
innovation4						0.829				
innovation5						0.752				
innovation6						0.725				
practice1								0.876		
practice2								0.629		
practice3								0.639		
performance1		0.478								
performance2		0.739								
performance3		0.655								
performance4		0.620								
performance5		0.593								
performance6		0.507								
complex1							0.832			
complex2							0.884			
complex3							0.710			
complex4							0.935			
intent4									0.790	
intent5									0.716	
intent1									0.589	
intent2									0.608	

intent3				0.532	
attitude1		0.702			
attitude2		0.684			
Subjective Norm1	0.841				
Subjective Norm2	0.915				
Subjective Norm3	0.654				
control1			0.672		
control2					0.763
control3					0.753
control4			0.738		
control5			0.682		

Extraction Method: Principal Axis Factoring. Rotation Method: Oblimin with Kaiser Normalisation.
Rotation converged in 17 iterations. Values less than (absolute) .30 were suppressed.

Appendix 2

Item loadings and cross-loading

	support	innovation	practice	performance	COMPLEX	INTENT	ATT	SN	PBC-Out	PBC-Res	*p*-value
support1	**(.663)**	-.102	-.053	-.204	.092	-.081	-.012	-.202	.174	.063	<0.001
support2	**(.607)**	.011	-.222	.054	.009	-.230	.176	-.054	-.593	.507	<0.001
support3	**(.772)**	-.105	.172	.275	-.168	.237	.046	.034	-.34	-.004	<0.001
support4	**(.76)**	.053	.135	-.152	.081	-.067	-.152	.007	.624	-.257	<0.001
support6	**(.662)**	.154	-.099	.008	.003	.091	-.029	.204	.050	-.228	<0.001
innovation1	-.069	**(.76)**	.119	-.090	.05	-.225	-.069	.259	-.025	.032	<0.001
innovation2	-.030	**(.761)**	-.118	-.174	.071	.046	-.102	-.074	.007	.278	<0.001
innovation3	.114	**(.735)**	.027	.010	-.149	-.159	-.018	.258	.034	-.076	<0.001
innovation4	.062	**(.748)**	-.022	.067	.133	.233	-.050	-.18	-.062	.055	<0.001
innovation5	-.066	**(.699)**	.209	.115	-.113	.030	-.102	.159	.267	-.428	<0.001
innovation6	-.012	**(.773)**	-.195	.082	-.003	.076	.326	-.397	-.197	.101	<0.001
practice1	-.019	.014	**(.776)**	-.189	-.070	.248	-.311	.049	-.289	.29	<0.001
practice2	.008	-.151	**(.878)**	.191	.068	-.111	.254	-.146	.005	.005	<0.001
practice3	.009	.142	**(.858)**	-.025	-.006	-.111	.021	.105	.256	-.267	<0.001
performance2	.098	-.133	-.058	**(.832)**	.010	-.071	.047	-.007	-.050	.085	<0.001
performance3	-.031	-.014	.088	**(.791)**	.041	-.303	.000	.129	.047	.094	<0.001
performance4	-.008	.046	.076	**(.851)**	.030	-.012	.070	.039	.084	-.135	<0.001
performance5	-.026	.008	.038	**(.761)**	-.146	.26	-.242	.044	-.105	.032	<0.001
performance6	-.040	.101	-.152	**(.763)**	.059	.145	.111	-.213	.016	-.072	<0.001

complexity1	.053	-.089	.077	.243	**(.792)**	.010	.022	-.036	-.045	.025	<0.001
complexity2	.103	.061	.005	.188	**(.778)**	.162	.206	-.172	-.138	.016	<0.001
complexity3	-.148	.002	-.070	-.164	**(.735)**	-.197	.09	.058	.004	.008	<0.001
complexity4	-.020	.033	-.020	-.326	**(.668)**	.018	-.364	.178	.210	-.057	<0.001
intent1	.009	.032	-.005	-.042	.020	**(.947)**	.196	-.014	-.011	.050	<0.001
intent2	.012	-.016	-.005	-.050	.032	**(.953)**	.166	-.006	.033	.012	<0.001
intent3	.016	-.031	-.039	-.004	.005	**(.928)**	.106	.123	.135	-.102	<0.001
intent4	-.019	<.001	.024	.066	-.043	**(.888)**	-.333	-.034	-.113	.007	<0.001
intent5	-.020	.016	.028	.036	-.018	**(.901)**	-.162	-.072	-.052	.034	<0.001
attitude1	-.011	.017	-.066	.033	.004	-.014	**(.975)**	-.004	.009	-.060	<0.001
attitude2	.011	-.017	.066	-.033	-.004	.014	**(.975)**	.004	-.009	.060	<0.001
SubjectiveNorm1	-.035	-.024	.018	.037	-.002	.011	.028	**(.967)**	-.088	.061	<0.001
SubjectiveNorm2	.011	-.073	.032	.038	-.011	-.097	.059	**(.972)**	.011	-.055	<0.001
SubjectiveNorm3	.024	.102	-.052	-.079	.014	.091	-.092	**(.922)**	.081	-.006	<0.001
control2	-.004	.003	.008	-.039	.036	-.019	.050	-.011	**(.980)**	.004	<0.001
control3	.004	-.003	-.008	.039	-.036	.019	-.050	.011	**(.980)**	-.004	<0.001
control1	-.019	-.044	.159	-.036	.009	.094	-.011	-.135	.360	**(.800)**	<0.001
control4	-.03	.078	-.091	.000	.002	-.042	.058	.039	-.166	**(.917)**	<0.001
control5	.048	-.04	-.048	.033	-.010	-.040	-.050	.081	-.420	**(.895)**	<0.001

Loadings are shown in bold and in brackets ( ). *p*-value is for loadings on parent contracts

.

Appendix 3

Item loadings and cross-loadings for final model

	COMPLEX	INTENT	ATT	SN	PBC-Out	PBC-Res	CULTURE	*p*-value
complex1	**(.792)**	-.019	-.017	.029	-.105	.061	.228	< .001
complex2	**(.779)**	.178	.232	-.217	-.158	.048	.260	< .001
complex3	**(.735)**	-.254	.135	.007	.030	.068	-.293	< .001
complex4	**(.668)**	.094	-.399	.210	.274	-.203	-.251	< .001
intent1	.012	**(.947)**	.169	.016	.007	.019	-.014	< .001
intent2	.026	**(.953)**	.124	.074	.005	-.006	-.056	< .001
intent3	-.003	**(.928)**	.128	.151	.124	-.125	-.068	< .001
intent4	-.032	**(.888)**	-.262	-.155	-.067	.034	.070	< .001
intent5	-.005	**(.901)**	-.183	-.097	-.074	.080	.075	< .001
attitude1	-.005	-.013	**(.975)**	-.005	.011	-.043	-.014	< .001
attitude2	.005	.013	**(.975)**	.005	-.011	.043	.014	< .001
SubjectiveNorm1	.021	-.008	.098	**(.967)**	-.010	.036	.002	< .001
SubjectiveNorm2	.013	-.100	.064	**(.972)**	.046	-.098	.000	< .001
SubjectiveNorm3	-.035	.113	-.170	**(.922)**	-.038	.065	-.002	< .001
control2	.040	-.025	.052	.016	**(.980)**	-.001	-.025	< .001
control3	-.040	.025	-.052	-.016	**(.980)**	.001	.025	< .001
control1	.022	.078	.086	-.249	.390	**(.800)**	.041	< .001
control4	-.020	-.038	.063	.014	-.026	**(.917)**	-.017	< .001
control5	.002	-.031	-.141	.209	-.501	**(.895)**	-.019	< .001
support	-.041	.002	.040	.138	-.259	.224	**(.711)**	< .001
innovation	-.113	.075	.096	-.171	.091	-.054	**(.787)**	< .001
practice	.090	-.106	.051	-.153	.256	-.274	**(.785)**	< .001
performance	.057	.027	-.171	.186	-.105	.117	**(.840)**	< .001

Loadings are shown in bold and in brackets ( ). *p*-value is for loadings on parent contracts.

Appendix 4

A summary of the gaps in the literature, leading to formulation of research questions, objectives and how these are addressed in the study

Literature gap	Research questions	Objectives	Addressed in the thesis
Behavioural studies in AIS mostly look at malpractices in general with limited or no attempt to differentiate one type of behaviour from another.	Research question 1: How are different types of insider dysfunctional behaviour related to or different from each other?	1. To categorise insiders' dysfunctional behaviour into relevant taxonomy.	Introduction of dysfunctional behaviour concept based on Stanton et al.'s (2005) two-dimensional behaviour taxonomy. This results in four behavioural typologies. Different malpractices are related to or differ from each other in terms of intention dimension (malicious-neutral) and computer skill required (low-high).
Insider threats are addressed mostly from technical or technological approach. Disparate and sometimes conflicting findings suggest other contextual factors are present in the equation.	Research question 2: What are the contextual factors influencing the predictors of behavioural intention?	2. To investigate the influence of contextual factors on the predictors of intention to engage in dysfunctional behaviour in the AIS environment.	Identified organisational culture, and AIS complexity as contextual factors influencing the predictor-intention relationships. The research model explains 78% (substantial) variations in intention through 4 predictors with 2 moderating variables.

Literature gap	Research questions	Objectives	Addressed in the thesis
Despite heavy investment in training and security awareness programs, insider threats still pose a great risk to AIS assets.	Research question 3: From a socio-technical perspective, how should insider threats be managed?	3. To analyse the influence of dysfunctional behaviour dimensions across different types of dysfunctional behaviour.	Analysis at dysfunctional behavioural aggregate level gives general behavioural dispositions on how individual, organisational culture, and technology (AIS complexity) interact. The effects of taxonomic dimensions, i.e. degree of maliciousness and computer skill, cause predictors of intention to vary across four types of dysfunctional behaviour. This explains different findings in AIS behavioural studies. Analysis at subset level indicates the salience of attitude. Thus, efforts towards attitudinal change are important, apart from balancing system complexity and cultivating security culture to manage insider threats.

Appendix 5
Item descriptive statistics

	Mean	Standard deviation
Support	4.673	1.374
Innovation	5.278	1.348
Practice	5.592	1.208
Performance	5.369	1.277
COMPLEX	4.884	1.586
INTENT	3.501	1.901
ATT	3.515	1.907
SN	3.863	1.830
PBC-Out	4.083	1.896
PBC-Res	4.364	1.782

Appendix 6
Instruments

Dear Sir/Madam,

An Invitation to Participate in a Research Project

I, Mohd Saiyidi Mokhtar MAT RONI, a PhD candidate at Edith Cowan University, Australia am currently undertaking a research project as part of the requirements of a PhD at the university. The research project title is "**An Analysis of Insider Dysfunctional Behaviour in an Accounting Information System**" which has been reviewed and approved by the ECU Human Ethics Committee.

This research project is conducted to seek answers to factors affecting employee security policy non-compliance behaviour in AIS. The findings are expected to provide useful insights into the non-security compliance behaviour issue, thus helping business organisations to re-structure their AIS security approaches.

Being part of the business community, you are invited to participate in this research project that will also benefit your organisation. The participation in this project is entirely voluntary. You can participate in this project by completing the questionnaire and mail it using a paid, pre-printed reply-address enveloped attached with this letter. Alternatively, you can also use the online version of the questionnaire which is available at Qualtrics at ECU.

The usefulness and potential benefits of the study will depend upon the care and the truthfulness of the responses the survey is designed to capture. Please read the instructions for each section carefully. Choose a response that portrays the best indications of how you would typically think, feel and experience. You are expected to spend no longer than 20 minutes to complete the survey.

As a strict adherence to the ethical conduct of this study, your response is kept anonymous. No personally identifiable information will be collected from you. All data will be treated with a strict accord to the requirements and guidelines of the ethics set forth by the university.

Should you require further information on this research, you are very much welcome to contact the following:

Mohd Saiyidi Mokhtar MAT RONI
(PhD Candidate)
School of Accounting, Finance and Economics
Faculty of Business and Law
Edith Cowan University
270 Lakeside Drive
Joondalup
Australia
WA 6027
Email: m.matroni@ecu.edu.au or saiyidi@yahoo.com

Prof Malcolm Smith
(Project Supervisor)
School of Accounting, Finance and Economics
Faculty of Business and Law
Edith Cowan University
Email: malcolm.smith@ecu.edu.au

Assoc. Prof. Hadrian Djajadikerta
(Project Supervisor)
School of Accounting, Finance and Economics
Faculty of Business and Law
Edith Cowan University
Email: h.djajadikerta@ecu.edu.au

Should you have any concern or complaint about the study and wish to speak to an independent person, you are advised to communicate with:
Research Ethics Officer
Edith Cowan University
Phone: +61 8 6304 2170
Email: research.ethics@ecu.edu.au

The findings of this study will also benefit you and your organisation, a copy of the result will made available for you upon your request. At the end of the survey please indicate your interest in the findings and furnish me with your contact detail for the result to be sent. The contact detail is kept separately from the survey with no identifiable information that can link between the two.

Your participation in this study is much treasured. Thank you.

Yours Sincerely

Mohd Saiyidi Mokhtar MAT RONI
PhD Candidate
School of Accounting, Finance and Economics
Faculty of Business and Law
Edith Cowan University

Please indicate your gender

- ○ Male
- ○ Female

Which age group that you belong to?

- ○ 20 years old or less
- ○ between 21 to 25 years old
- ○ between 26 to 30 years old
- ○ between 31 to 35 years old
- ○ between 36 to 40 years old
- ○ between 41 to 45 years old
- ○ above 45 years old

Please indicate your academic/professional qualifications.
(Select all that apply)

- ☐ LCE / SRP / PMR
- ☐ SPM / SPMV
- ☐ Diploma
- ☐ Bachelor Degree
- ☐ Master
- ☐ PhD
- ☐ Professional qualifications (e.g. ACCA, CIMA, MIA)

How long have you been working with the current company?

- ○ less than 1 year
- ○ 1 – 5 years
- ○ 6 – 10 years
- ○ 11 – 15 years
- ○ more than 15 years

Please choose the sector and the industry that best describe your company.

The sector in which your company is operating.
(Select all that apply).

- ☐ Trading
- ☐ Manufacturing
- ☐ Service

The industry in which your company is operating.
(Select all that apply).

☐ Accounting	☐ Call Centers	☐ Energy	☐ Music
☐ Advertising	☐ Cargo Handling	☐ Entertainment & Leisure	☐ Online Auctions
☐ Aerospace	☐ Chemical	☐ Executive Search	☐ Pharmaceuticals
☐ Agriculture	☐ Computer	☐ Financial Services	☐ Publishing
☐ Aircraft	☐ Consulting	☐ Food, Beverage & Tobacco	☐ Real Estate
☐ Airline	☐ Consumer Products	☐ Grocery	☐ Retail & Wholesale
☐ Apparel & Accessories	☐ Cosmetics	☐ Health Care	☐ Software
☐ Automotive	☐ Defense	☐ Internet Publishing	☐ Sports
☐ Biotechnology	☐ Departmental Stores	☐ Legal	☐ Telecommunications
☐ Broadcasting	☐ Education	☐ Motion Picture & Video	☐ Transportation
☐ Brokerage	☐ Electrical & Electronics		

Please indicate your level of assessment on the following aspects of your organisation.

In regards to the support in your organisation, **how many people..**

	None	Very little	Little	Some	Many	A lot	All
with personal problems are helped?	○	○	○	○	○	○	○
who wish to advance in promotion are supported by their superiors?	○	○	○	○	○	○	○

In regards to the support in your organisation, **how often...**

	Never	Rarely	Very rarely	Not sure	Sometimes	Most of the Time	Always
Is constructive criticism accepted?	○	○	○	○	○	○	○
do managers express concern about employees' personal problems?	○	○	○	○	○	○	○
are new ideas about work organisation encouraged?	○	○	○	○	○	○	○
do management practices allow freedom in work?	○	○	○	○	○	○	○

In regards to the innovation in your organisation, **how often...**

	Never	Rarely	Very rarely	Not sure	Sometimes	Most of the Time	Always
does your organization search for new markets for existing products?	○	○	○	○	○	○	○
Is there a lot of investment in new products?	○	○	○	○	○	○	○
do unpredictable elements in the market environment present good opportunities?	○	○	○	○	○	○	○
does the organization search for new opportunities in the external environment?	○	○	○	○	○	○	○
does the company make the best use of the employee skills to develop better products /services?	○	○	○	○	○	○	○
does the organization search for new products/services?	○	○	○	○	○	○	○

In regards to the practices in your organisation, **how often...**

	Never	Rarely	Very rarely	Not sure	Sometimes	Most of the Time	Always
are instructions written down?	○	○	○	○	○	○	○
are jobs performed according to defined procedures?	○	○	○	○	○	○	○
does management follow the rules themselves?	○	○	○	○	○	○	○

In regards to the goal / performance of employees in your organisation, **how often...**

	Never	Rarely	Very rarely	Not sure	Sometimes	Most of the Time	Always
Is competitiveness in relation to other organizations measured?	○	○	○	○	○	○	○
Is individual appraisal directly related to the attainment of goals?	○	○	○	○	○	○	○
does management specify the targets to be attained?	○	○	○	○	○	○	○
Is it clear how performance will be evaluated?	○	○	○	○	○	○	○
are there hard criteria against which job performance is measured?	○	○	○	○	○	○	○
Is reward dependent on performance?	○	○	○	○	○	○	○

In order to complete your tasks at work, you always interact with the computer system provided by your organisation. These systems include the point-of-sale, inventory/stock management, financial and management accounting system, production planning and control system, payroll and human resource management system. These systems are normally coined as an accounting information system.

Please indicate your level of assessment on the following aspects of the computerised system you are using at your organisation.

	Strongly Disagree	Disagree	Slightly Disagree	Neither Agree nor Disagree	Slightly Agree	Agree	Strongly Agree
My interaction with the system is clear and understandable.	○	○	○	○	○	○	○
I find the system is easy to use.	○	○	○	○	○	○	○
Using the system takes too much time from my normal duties.	○	○	○	○	○	○	○
Using the system involves too much time doing mechanical operation (e.g. key in data)	○	○	○	○	○	○	○

<Include scenario 1, 2, 3 or 4 here.>

Based on the scenario above, please answer the following questions.

Please provide your assessment of the likelihood of your action in regards to the case above.
(from 1 being VERY UNLIKELY to 7 being VERY LIKELY).

	Very Unlikely	Unlikely	Somewhat Unlikely	Undecided	Somewhat Likely	Likely	Very Likely
If you are in Hashim's situation, how likely that you would perform a similar action?	○	○	○	○	○	○	○
All things considered, would you take the same action as Hashim did?	○	○	○	○	○	○	○

Please provide your assessment on your intention regarding the action in the case above.
(from 1 being STRONGLY DISAGREE to 7 being STRONGLY AGREE).

	Strongly Disagree	Disagree	Slightly Disagree	Neither Agree nor Disagree	Slightly Agree	Agree	Strongly Agree
I intend to carry out a similar action in future.	○	○	○	○	○	○	○
I predict I would carry out a similar action in future.	○	○	○	○	○	○	○
I plan to carry out a similar action in future.	○	○	○	○	○	○	○

Please provide your assessment on your attitude toward the action in the case above.
(from 1 being STRONGLY DISAGREE to 7 being STRONGLY AGREE).

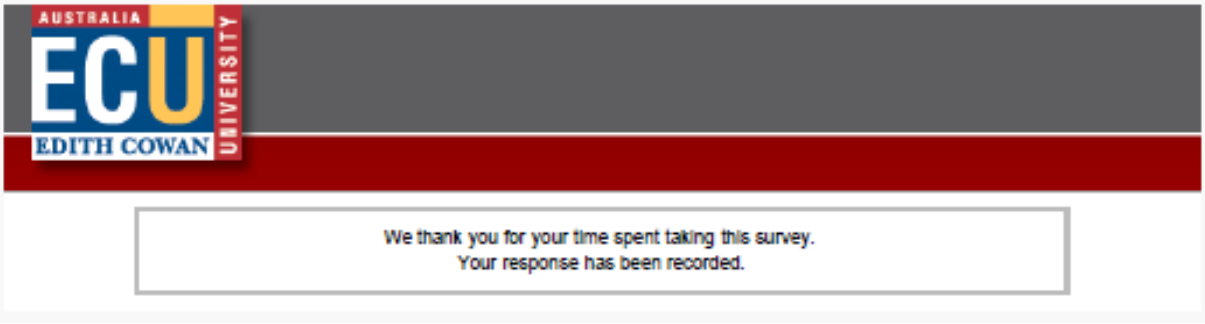
	Strongly Disagree	Disagree	Slightly Disagree	Neither Agree nor Disagree	Slightly Agree	Agree	Strongly Agree
Carrying out such action is good.	○	○	○	○	○	○	○
Carrying out such action is valuable.	○	○	○	○	○	○	○

Please provide your assessment on the following aspects of your work environment regarding the action in the case above.
(from 1 being STRONGLY DISAGREE to 7 being STRONGLY AGREE).

	Strongly Disagree	Disagree	Slightly Disagree	Neither Agree nor Disagree	Slightly Agree	Agree	Strongly Agree
People who influence my behaviour think that I should carry out such action.	○	○	○	○	○	○	○
People who are important to me think that I should carry out such action.	○	○	○	○	○	○	○
My fellow colleagues would themselves have carried out this action if they had been in my place.	○	○	○	○	○	○	○

If you were to carry out such action, please indicate your level of assessment of the followings.
(from 1 being STRONGLY DISAGREE to 7 being STRONGLY AGREE).

	Strongly Disagree	Disagree	Slightly Disagree	Neither Agree nor Disagree	Slightly Agree	Agree	Strongly Agree
Carrying out such action can decrease the time needed for my important job responsibilities.	○	○	○	○	○	○	○
Carrying out such action can significantly increase the quality of output of my job.	○	○	○	○	○	○	○
Carrying out such action can significantly increase the quantity of output of my job.	○	○	○	○	○	○	○
I have the resources necessary to carry out such action.	○	○	○	○	○	○	○
I have control over carrying out such action.	○	○	○	○	○	○	○


AUSTRALIA
ECU
EDITH COWAN
UNIVERSITY
We thank you for your time spent taking this survey.
Your response has been recorded.

Appendix 7

Mann-Whitney *U* test result on differences between two methods of data collection

	SOURCE	*N*	Mean Rank	Sig.
INTENT	mail	298	195.09	0.726
	online	89	190.36	
	Total	387		
ATT	mail	298	197.94	0.201
	online	89	180.82	
	Total	387		
SN	mail	298	200.27	0.143
	online	89	173.01	
	Total	387		
support	mail	298	192.45	0.616
	online	89	199.2	
	Total	387		
innovation	mail	298	185.59	0.107
	online	89	222.15	
	Total	387		
practice	mail	298	190.44	0.246
	online	89	205.92	
	Total	387		
performance	mail	298	193.05	0.759
	online	89	197.18	
	Total	387		
COMPLEX	mail	298	181.13	0.100
	online	89	237.09	
	Total	387		
PBC-Out	mail	298	197.93	0.201
	online	89	180.84	
	Total	387		
PBC-Res	mail	298	194.7	0.821
	online	89	191.66	
	Total	387		

Appendix 8

Mann-Whitney *U* test result on differences between late and early responses

	WAVE	*N*	Mean Rank	Sig.
INTENT	wave 1	193	194.420	0.940
	wave 2	194	193.580	
	Total	387		
ATT	wave 1	193	194.440	0.938
	wave 2	194	193.560	
	Total	387		
SN	wave 1	193	194.460	0.936
	wave 2	194	193.550	
	Total	387		
support	wave 1	193	193.470	0.925
	wave 2	194	194.530	
	Total	387		
innovation	wave 1	193	193.920	0.989
	wave 2	194	194.080	
	Total	387		
practice	wave 1	193	193.840	0.978
	wave 2	194	194.160	
	Total	387		
performance	wave 1	193	193.650	0.951
	wave 2	194	194.350	
	Total	387		
COMPLEX	wave 1	193	194.110	0.985
	wave 2	194	193.890	
	Total	387		
PBC-Out	wave 1	193	194.440	0.937
	wave 2	194	193.560	
	Total	387		
PBC-Res	wave 1	193	194.580	0.918
	wave 2	194	193.420	
	Total	387		