

# **Contextualising the Insider Threat: A Mixed Method Study**

**Sean Browne**

Whitaker Institute, NUI Galway, Ireland, s.browne2@nuigalway.ie

**Willie Golden**

Whitaker Institute, NUI Galway, Ireland, willie.golden@nuigalway.ie

**Michael Lang**

Whitaker Institute, NUI Galway, Ireland, michael.lang@nuigalway.ie

## **ABSTRACT**

The insider threat is potentially the most damaging and costly threat to organisations, and while there is a considerable body of literature aimed at understanding this phenomenon, we contend that the theories contained in such literature are most beneficial if they can be utilised in a way that is contextually relevant. Our research, and this paper, is specifically focussed on developing and improving this contextual validity.

We find that malicious acts arising from disgruntlement are perceived as very real problems in practice. We also present a current list of non-malicious aberrant behaviours and show how they rank in relative seriousness to one another.

Given that the primary motivation for conducting this study is the view that reliance on the traditional conceptualisation of a boundary or perimeter is no longer viable, our essential contribution lies in devising a series of vignettes that empirically reflect this current contextual validity.

**Keywords:** Insider Threat, Malicious Behaviour, Non-malicious Behaviour, Computer Abuse, Data Mobility, Shadow IT.

## **INTRODUCTION**

In the modern networked world, replete with massive amounts of data, one of the greatest economic threats facing organisations is information loss inflicted by actors either from within or external to the organisation. While much attention has been paid in the past to the

external threats, the internal threat is gaining ground in the minds of those concerned with information security. Recent industry reports have variously described it as a ‘huge problem’ (van Kessel and Allan 2014) or indeed a ‘relentless problem’ (Vorometric 2015) and a problem that is becoming ‘more serious’ (Trendmicro 2014). Both the FBI and Homeland Security have warned that “disgruntled and former employees pose a significant cyber threat” (FBI and DHS 2014) and one of the world’s most respected information security training organisation reports that 74% of companies are concerned about insider threats (SANS Institute 2015).

Notably, this concern about the insider threat is not confined to industry and consultant-led reports. Within the academic field the insider threat has been described as the greatest threat of all (Warkentin and Willison 2009), a significant threat to organisations (D’Arcy and Devaraj 2012; D’Arcy and Hovav 2009; D’Arcy et al. 2009), and a major concern (Siponen and Vance 2010). In fact Vance et al (2013) open their paper by stating that a persistent problem in information security is insiders who abuse the trust placed in them. Furthermore, when proposing a research agenda for the Behavioural Information Security field, Willison and Warkentin (2013) assert that insider computer abuse has the greatest potential for loss and damage to the employer and they call for research that considers the thought process of the offender. This current study is motivated by a desire to contribute towards answering this call.

## **THEORETICAL FRAMEWORK**

As part of the Behavioural Infosec research field, our overall aim is to contribute to a greater understanding of non-compliant information security behaviour in the organisational context. Regarded as being crucial for organisations that want to leverage their human capital (Bulgurcu et al. 2010), one of the theories used to examine non-compliant behaviour that has proven popular in prior studies is Deterrence theory. With its origins in the works of early classical philosophers and subsequent criminological works it was introduced to the

mainstream IS literature with Straub's seminal (1990) study, showing that security countermeasures had a deterrent effect on intentional system misuse. While subsequent studies extended the theory to show that awareness of these countermeasures was in itself a deterrent to such behaviour (D'Arcy et al. 2009) others have sought to combine the theory with other theories. For example in (Siponen and Vance 2010) where Neutralisation Theory was incorporated, the deterrent effects of all forms of sanctions were rendered insignificant, and in (Barlow et al. 2013) only one of the three neutralisations examined were found to have a significant effect on intention to violate policy. Similarly with the inclusion of Ethics theory, it has been shown that, with the exception of sabotage, codes of ethics have no effect on computer abuse judgements and intentions (Harrington 1996) while (Hu et al. 2011) point to the importance of the level of self control among potential offenders. Social Bond Theory has also been used to examine aberrant behaviour (Cheng et al. 2013) with varying results between an individual's bond to co-workers and to the organisation. In summary, when viewed as a whole, deterrence based studies have to date presented disparate findings. There are several methodological approaches suggested for addressing this, one of which is to measure perceived the benefits of the behaviour in question in conjunction with perceived sanctions (D'Arcy and Herath 2011).

With a view to examining the impact of both sanctions and expected benefits of aberrant behaviour we have therefore chosen Rational Choice Theory (RCT) as the basis for our theoretical model (Nagin and Paternoster 1993; Paternoster and Simpson 1996). Commonly applied in criminal behaviour studies, a succinct description of the theory is available in (McCarthy 2002) where it is described as:

*“The rational choice approach to crime assumes that crime can be understood as if people choose to offend by using the same principles of cost-benefit analysis they use when selecting legal behaviours.”*

In addition to the dual focus on both the negative and positive consequences of human choice-making, our selection of the theory follows the logic expressed in (Paternoster and Simpson 1996; Vance and Siponen 2012) that RCT is particularly appropriate for explaining crimes of a so-called “white-collar” nature involving a deliberate decision processes. Given that the focus of this study is insider deliberate actions, it therefore seems appropriate to use RCT as a fulcrum around which to base our theoretical model.

However, simply adopting a theory or introducing additional constructs to existing theories is not sufficient. We also need to consider how we operationalise these models, what artefacts the measurement instruments contain and how we can make them relevant using empirical means. Effectively we need ensure that they are contextually relevant.

### **CONTEXTUALISATION**

This paper considers contextualisation from two perspectives, namely the position of the research in the overall body of research and the real world setting that it concerns.

Firstly, at its most basic level contextualisation refers to where within the IS security threat landscape the research is situated. Loch et al (1992) identified four dimensions of Information Systems Security, which was subsequently expanded on by Willison and Warkentin (2013) when they described a continuum of internal violations, ranging from passive non-volitional non-compliance, to intentional malicious computer abuse. In excluding passive or accidental actions of employees, this study is firmly placed in the volitional / intentional sphere. Thus the word “intentional” takes on a critical importance and it is crucial to understand that this includes both non-malicious as well as malicious actions.

Secondly, contextualisation also concerns the real world setting in which we apply our research, recognising that the fundamental nature of that world changes over time. In terms of external threats prior studies have focussed on the technical aspects of information security

designed to prevent or detect what could be described as intruders (Cavusoglu et al. 2005; Cavusoglu et al. 2009; Lee and Larsen 2009; Yue and Cakanyildirim 2007). Much of the internal threat based literature has dealt with issues like inappropriate use of organisational systems (Liao et al. 2009) or inappropriate accessing of information by employees (Hovav and D'Arcy 2012). What these studies have as a common denominator is the way in which they conceptualise information security – as something that can be protected within an organisational boundary.

However this reliance on the traditional conceptualisation of a boundary or perimeter is no longer viable in the modern networked world (Edwards 2013; Rebollo et al. 2012; Zissis and Lekkas 2012). In today's world of tech-savvy employees, data mobility and flexible working arrangements, employees' technology demands are increasingly being met by a multitude of providers, ultimately giving rise to an information ecosystem that is far removed from the traditional organisational boundaries.

Such is the rate of the change in the modern world that even language cannot keep pace.

Terms like 'The Cloud', 'BYOD' and the ubiquitous use of the word 'apps' have entered our everyday lexicon, and connote an idea of data and information mobility. Further descriptions such as; 'Stealth IT', 'Workaround Systems' and 'Feral Systems' (Fürstenau and Rothe 2014; Silic and Back 2014), emphasise the lack of agreed definitions but also point to the relentlessly changing nature of the way we work.

For example, Nasuni (2014) relates the change of emphasis to the availability of technology and a corresponding "culture of convenient, 'always on' access to information" and Schalow et al. (2013) argue that the blurring of work and personal life boundaries is nothing new but is driven by the consumerisation of Information Technology. In fact Banham (2015) suggests that embracing this trend is imperative, primarily because of its inevitability.

This desire to embrace non-institutional based information solutions is not new however. More than thirty years ago, using an analogous term “end-user computing” (EUC), Alavi and Weiss (1985) warned of the organisational risk of what they describe as “a rapidly growing and irreversible phenomenon”, or as Doll and Torkzadeh (1988) put it “one of the most significant phenomena to occur in the information systems industry”.

Whatever the reasons for the change in the relationship between technology and work, the reality is that a common element of the technological behavioural practices that are now in vogue involves greatly increased dispersion of data and information outside the traditional perimeter of the organisation. The literature and the discussion above also indicate that attempting to put a label on this paradigm shift is problematic and so we defer to Silic and Back (2014) and adopt their language in describing the new IS context as including “all hardware, software or any other solutions used by employees which are not approved by the IT department.” The next logical step then is asking to what extent previously used instruments for testing our behavioural theories are still relevant in this new IS context, and it is the resulting measurement instruments that the remainder of this paper concerns itself with.

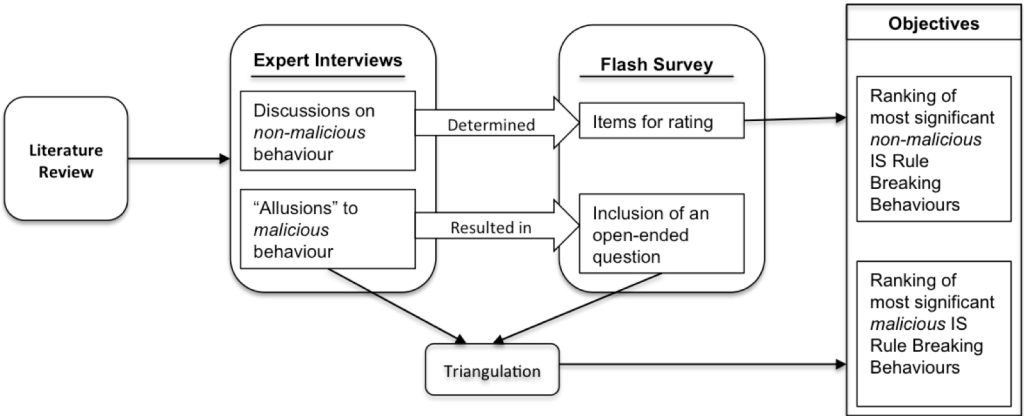
## **METHODOLOGY**

### **Approach**

In acknowledging the debate that exists in the information systems field about the relative importance of rigour and relevance in research, Siponen and Vance (2014) caution against the use of research instruments that are out of touch with practice. They suggest a number of guidelines for instrumentation design that are intended to improve practical relevance of research in information security without any loss in rigour, and point out that most existing studies meet less than half of their proposed recommendations – a deficiency that we are addressing in this and future research.

However what is of primary concern to this particular paper are their primary guidelines; that studies should measure specific violations rather than an abstract representation of violations, and that these should be violations that are deemed important by those practicing in the field

In order to adhere to these primary recommendations, three approaches are suggested (1) basing topics on a list obtained from literature and getting practitioners to rank them, (2) developing multiple scenarios and getting comments from practitioners or (3) using a belief elicitation technique (Limayem and Hirt 2003) to ask practitioners what their greatest concerns are (Siponen and Vance 2014).



**Figure 1:** Research Method and Objectives

Our approach has been a combination of all three. In the first instance, a review of the literature was undertaken to establish a baseline of offences with potential relevance. These formed the basis for developing an interview protocol used to conduct a series of expert ‘semi-structured’ interviews. However, being cognisant of the sensitive nature of the subject matter and the potential reticence of respondents to reply to direct questioning, on occasions the protocol was deviated from during the interview process. The interviews were then analysed and the principal findings were further examined, for ranking, via a survey instrument using a separate cohort of information security professionals.

## Interviews

The LinkedIn social networking site was used to “connect” with a number of information security professionals. Their selection was random but was governed by two criteria (a) that they were senior professionals currently working in information systems security and (b) that their roles spanned a number of different industries. In order to manage this process, the search for connections was conducted among the membership of the Irish chapter of ISACA. It was important to the validity of the study that a comprehensive cross-section of opinions was elicited and so two internationally active security consultants were also included in the expert pool to expand the breadth of organisational types in the sample.

Initially, invitations to participate were e-mailed to 19 individuals and interviews were commenced as soon as the first acceptance was received. The interview protocol was made up of a series of six primary questions designed to determine the interviewees opinion on (a) what type of actual actions of employees give them cause for concern; (b) if there are specific IS policies or standards in their organisation targeted at employees; (c) if the interviewees had to deal with many security incidents involving insiders and examples thereof; (d) why employees might break the rules even when they know they exist; (e) the arguments employees use to defend their actions and (f) if there are any screening measures used in the hiring of new employees.

Interviews were analysed immediately after completion and it was decided to cease interviewing new subjects when data saturation was reached. Defined as the point at which any additional data provides few, if any, new information or suggests new themes (Saunders et al. 2012) or incremental learning is minimal (Eisenhardt 1989), this occurred after 9 interviews. This was not considered surprising given the design and purpose of the interviews was to elicit opinions from experienced practitioners on their greatest concerns about employee behaviour.

Name	Organisation Description	Job Title
TechCo	Software application development	Global Head of Information Security
ScienCo	Multinational scientific manufacturing	Senior IS Infrastructure Manager
PackCorp	Packaging multinational	Group Information Security Officer
LeisCorp	Gaming multinational	Information Security Manager
Consult1	Information Security Consultant	Owner
FinInst	Banking	Chief Information Security Officer
MajorCo	Manufacturing & Distribution multinational	Head of Information Security
BankCo	Banking	VP Information Security, IT Risk & Controls
Consult2	Security Consultant	Owner

**Table 1.** Interviewee Demographic Details

In general, interviewees opined that the insider threat was a major issue but initially equivocated on whether malicious behaviour was of significance. On the subject of non-malicious behaviours, the majority opinion was that factors like convenience, the trend towards a data mobility culture and the fact that there are now more employees who believe they are ‘tech-savvy’ contributes to the problem. A flavour of some of the comments in this regard is shown in Table 2 below.

Type	Reason	Comment
Non-Malicious	Tech Savvy	<i>“We implemented a block of all cloud storage and then we found that people used the TOR network to bypass our web filter, so that they can still get to the web version of Dropbox”</i> (TechCo)
		<i>“I worked with one company and the HR manager was very proud that she was backing up all the HR and payroll files every night onto a USB stick. I said ‘very good and do you store that in your fire-proof safe or do you keep it securely off-site’ and she says ‘oh no it’s kept securely off-site’ and I went ‘very good and how do you do that?’ and she went ‘well I put it in my gym bag and I bring it home with me every day’”</i> (Consult 1)
	Convenience	<i>[On the dangers of free wifi – specifically in Boston Logan Airport] “It’s notorious. So you see something that says “Massport free Wi-Fi” and you go for it – next thing you’ve bought a lawnmower in Utah. It’s bananas, right? And it’s constant.”</i> (ScienCo)
		<i>“You might have guys in all parts of the organisation, not just in the IT department, but in a branch somewhere who’ll just say ... ‘Ah look, I don’t need to use that, sure I’ll just use wi-fi or whatever’ so that’s a huge thing”</i> (FinInst)
	Data Mobility	<i>“As email has proliferated, as people have gotten their own email addresses, people are still sending stuff to their personal email address when they shouldn’t be doing so”</i> (MajorCo)
<i>“You can break into three worlds: Personal email, social media and storage websites. They are your threats.”</i> (LeisureCo)		

**Table 2.** Examples of ‘non-malicious’ internal security violations

At this point it is worth noting that literature and research methodologies would have us believe that enquiries of this kind may be limited in what they can determine, due to the sensitive nature of the topic (Kotulic and Clark 2004) and the reluctance of interviewees to let

outsiders study their potential security issues (Posey et al. 2011). Therefore, it was anticipated that the findings of this section of the study would only relate to non-malicious behaviours. Crucially however, we also found that malicious behaviour was a major concern for those interviewed. Malicious harming of the organisation was alluded to several times during nearly every interview, with perimeter security being a major issue. Traditionally, perimeter security has been regarded as a concern relating to external actors but now it also forms part of the insider threat. Specifically, employees ‘stealing’ information, data, and intellectual property represent a real concern, particularly in the context of the disgruntled or displaced employee.

Malicious	Personal Gain	<i>“The insider threat has probably moved away from misuse to using the computers for personal gain or for fraud. I think that’s going to become even more likely over time”</i> (PackCorp)
		<i>“We have had security breaches with either staff leaving the company and they’ve taken confidential information with them like customer lists and stuff like that, or in one or two cases where staff have stolen source code and intellectual property ... and in one case went to set up their own company doing the same type of business, using the source code they had taken ... or taken source code from an internal system that the company was using ... and then the staff member gave it to his brother who set up a company providing this software as a business solution”</i> (Consult2)
		<i>“When people have decided to leave an organisation or the organisation has decided to let them go, that they send home a brain-dump of a lot of their stuff - so I’ve come across instances of source code, of strategic plans, of people’s CVs and it’s all around the topic that people are preparing themselves for in their next life”</i> (BankCo)
	Disgruntlement	<i>“there will always be disgruntled employees and it’s something we are aware of ... when we go with our quarterly updates to the board the disgruntled employee mightn’t be at the top of the list like it would have been 3-4 years ago, but it’s still a risk”</i> (FinInst)
		<i>“... you always have the disgruntled leaver factor and that is genuinely an issue ... now people who don’t have privileges on systems, it’s not so much a big deal, because there’s not so much damage they can do but ... y’know the other concern is people deliberately stealing information. So it’s one thing to send your information to your own Gmail account, but the fact that we now have things like oneDrive for Business and you can fire up all of these files to your oneDrive account - pull them down when you get home, have no traceability on them ... even if we had Data Loss Prevention (DLP) software ... if DLP was looking specifically at email it wouldn’t show up this ... and if you go off to a competitor and you are a sales or marketing person, you’re pulling that proprietary information or even planning information for the following financial year and bringing it to your competitors ... or to your new employers”</i> (MajorCo)

**Table 3.** Examples of ‘malicious’ internal security violations

The difficulty in obtaining complete and open responses in information security studies has long been problematic (Crossler et al. 2013; Guo et al. 2011). Bearing this in mind it was

therefore not surprising that when pressed on malicious threats, interviewees indicated that it was a real concern but in general showed a certain amount of reticence in divulging details or examples. This may be because asking people responsible for information security about what concerns them in relation to employee behaviours is effectively something that requires more than a modicum of self-reflection and self-criticism, if they are to answer honestly. Paradoxically this seems to be more pronounced in relation to non-malicious behaviours, presumably because practitioners feel that they should be able to prevent these from happening. Therefore, in an effort to get a better understanding of the relative importance of each of the behaviours, rather than simply confirming that they exist, a logical next step was to introduce a layer of anonymity. This formed the second part of our “contextual” investigation – using an anonymised survey instrument.

**Mini - Survey**

A very parsimonious questionnaire was prepared which contained, in addition to some demographic questions, a list and brief description of 11 insider threats (derived from the findings of the previously conducted interviews). These were exclusively of the type categorised as ‘non-malicious’ – a research strategy that was adopted because what was being sought from respondents was a ranking of the seriousness of offences and it was assumed that all malicious acts would be regarded as extremely serious. The 11 offences offered for rating are shown in Table 4 below.

	<b>Name</b>	<b>Organisation Description</b>
1	Email (1)	employees / contractors emailing the organisation's information to an unsecured email (such as their home address) in order to work on information off-site
2	Email (2)	contractors setting up auto-forwarding of emails to alternative email addresses when away from the office
3	USB Backup	employees / contractors using USB memory storage to 'backup' sensitive organisation data
4	Other Mobile Devices	employees / contractors using 'tablets' or 'phablets' to work on organisation data
5	Social Media (1)	employees / contractors using social media without approval and thus exposing the organisation to possible phishing attacks
6	Social Media (2)	employees / contractors publishing inappropriate or sensitive

		organisational information on social media platforms
7	Remote Login	employees / contractors installing software to enable their own unauthorised remote login
8	Wi-Fi (1)	employees / contractors using public unsecured or unapproved wi-fi networks to conduct organisation business
9	Wi-Fi (2)	employees / contractors creating their own unsecured wi-fi networks
10	Cloud Storage	employees / contractors using unauthorised online data storage services
11	Browsers	employees / contractors availing of services such as the TOR network to circumvent access control measures

**Table 4.** Rating Offences

The questionnaire also contained an open-ended, free form question, requesting respondents to offer their own opinions on the most significant sources of insider threat behaviour. The survey was posted on the ISACA Ireland LinkedIn webpage and over a two-week period received a total of 33 responses.

Approximately one third of the respondents were Information Security Consultants with a similar amount of Information Security Managers and the remainder were spread across General Management, Internal Audit, Risk Management and Security Analysis roles - over 70 per cent of respondents classified their positions as senior or middle management.

The interview instructions asked respondents to rate the “offences” on a 5-point seriousness scale. The instruction on seriousness was further defined as respondents’ own opinion of the threat, viewed from the twin perspectives of the likelihood of it occurring and the potential impact on the organisation if it did occur. The scale ranged from ‘Not Serious’ to ‘Extremely Serious’, with a midpoint of ‘Serious’.

Combining the product of 11 offences and 33 respondents yields a total of 363 responses to potential insider threat behaviours. Of these, only 72 (20%) fall into the categories of “Not Serious” or “A Little Serious” meaning that the remaining 80% represent concerns of significance in the eyes of the sample surveyed. Overall, the number of respondents that rated the offences as serious was relatively evenly spread across the offence categories. However, when we examined the number of responses that categorised offences as “Extremely

Serious”, a slightly different picture emerged. The most serious offence according to our sample is the idea of employees or contractors installing software to enable their own unauthorised remote login. This is followed by; employees / contractors creating their own Wi-Fi networks; and using services such as the TOR network to circumvent access control measures. Surprisingly, and contrary to popular opinion, two of the lower scores in this category relate to the use of tablets and “phablet” devices in the conduct of business and the use of unapproved social media or using social media in an inappropriate manner.

A summary of the responses is shown in Table 5 below.

“Offence” (see also Table 4)	Not Serious	A little Serious	Serious	Very Serious	Extremely Serious
Remote Login	1	2	2	8	20
Wi-Fi (2)	0	6	6	5	16
Browsers	1	6	4	6	16
USB Backup	0	3	4	11	15
Social Media (2)	0	4	4	12	13
Wi-Fi (1)	2	8	2	8	13
Cloud Storage	3	6	3	8	13
Email (2)	1	6	4	10	12
Email (1)	0	3	8	11	11
Social Media (1)	1	10	5	10	7
Other Mobile Devices	1	8	8	10	6
Totals	10	62	50	99	142
	72			291	
	20%			80%	

**Table 5.** Survey Results

While the dataset in this survey is reasonably small, it is noteworthy that it was conducted among a cohort of professionals in the field of information security who, by virtue of their membership of the LinkedIn group, are actually operating in the field. No inducements for participation were offered to respondents, save for an undertaking to revert with the results of the survey, and so the responses are assumed to be truthful.

The open-ended question in the questionnaire simply asked respondents to name and give a brief description of any other additional actions of insiders, which they believed could present a significant security threat. Of the 19 (55%) respondents who offered a view on this question

the majority related to non-malicious behaviours and mirrored some of those offered for ranking in the earlier section of the questionnaire. Additional non-malicious behaviours included the use of “Shadow IT”, “Abuse of access controls”, “not using encryption”, “carelessness” and “the use of screen-grab tools and unauthenticated printers”.

Several respondents only considered this question from a malicious perspective, despite not being prompted to. For example one respondent cited disgruntled employees and the notion of Intellectual Property Plagiarists. Others referred to employees walking out with confidential data or removal of data via unmonitored websites, and two of the survey respondents specified as concerns the downloading and sale of confidential data to competitors / black market and creating backdoors into the enterprise network for unapproved use.

To summarise the data overall, the ‘non-malicious’ actions of the “insider” that our survey respondents deemed most serious, revolve around the mobility of data, circumventing security controls for convenience purposes, and using third party or open source technologies in the workplace.

On the malicious side the theft of information or intellectual property was the most cited offence in both the interviews and mini-survey, occurring primarily with disgruntled and departing employees. What was surprising was that not only was it a concern, but that information security professionals readily admitted that it worried them. Thus while non-malicious behaviour of insiders has been the more popular focus for prior behavioural studies in this area, it is our contention that it is remiss to ignore malicious behaviours.

Our findings clearly show that the priorities of information security professionals have changed with regard to the insider threat, and the fact that malicious acts of employees are now openly viewed as a major concern rather than the tacit acknowledgement that they previously received, means that academic research should do likewise.

Methodologically, a significant amount of such academic research has previously employed the use of hypothetical vignettes (Weber 1992). What this research indicates is that a new set of vignettes, with specifics set firmly in the domain of current security concerns in practice, is needed. Therefore testing our theories requires that this be reflected in our measurement instruments. With this in mind, and drawing on the findings from our empirical work for context, we have developed a series of four vignettes to be used in future studies that are presented in Appendix A to this paper.

## **CONCLUSION**

Although research on malicious behaviour by disgruntled employees has previously been called for (Crossler et al. 2013; Willison and Warkentin 2013) our study is, to the best of our knowledge, one of the first to put it on the research agenda using empirical methods.

A second and equally compelling finding from this research is in relation to the types of rule breaking behaviour that are of greatest concern. This study clearly shows that behaviours examined in much of the prior literature (looking at passwords, sharing logins, sending inappropriate email etc) are no longer alone at the forefront in terms of importance. They have been replaced by behaviours concerning remote login, creation of personal wi-fi networks and circumventing browser controls.

Given the argument in (Siponen and Vance 2014) that studies in this area must measure specific behaviours then these two findings along with the creation of the resulting vignettes represent significant contributions to the field.

## APPENDIX A – SCENARIOS AND CONSISTENCY CHECK RESULTS

### 1. Non-Malicious Scenarios

- **Remote Login** (employees / contractors installing software to enable their own unauthorised remote login)

Mike<sup>1</sup> is a manager in a medium sized company and although not from an IT background, he considers himself to be reasonably up to date with modern technology and trends. Because of the demands of his job Mike<sup>1</sup> would like to have remote access to the company’s servers so that he could work from home in the evenings<sup>3</sup>. He has submitted an application to the IT department to be granted this access using the company’s virtual private network, but he hasn’t heard back from the IT department in six months<sup>2</sup>. While browsing the web Mike<sup>1</sup> discovers a website offering free remote control of any computer over the internet and decides to investigate. He knows that it is against the rules in his organisation to load any software on company computers without authorisation<sup>4</sup> but is re-assured by glowing testimonials on the website, so Mike<sup>1</sup> goes ahead and downloads the software to both his work and home computer giving himself remote access<sup>5</sup>.

- **Wi-Fi** (employees / contractors creating their own unsecured wi-fi networks)

Peter<sup>1</sup> is a branch manager in busy company with branches nationwide. Recently the branch has expanded and Peter<sup>1</sup> hired some new clerical staff, but has had difficulty arranging appropriate accommodation. Head-office supplied the branch with a ‘portable’ office unit but he is frustrated by the inaction of the Head-Office IT department in installing the necessary wiring and connections for the computers in the new office<sup>2</sup>. He knows that it is against company rules for anyone other than IT department personnel to install computer-networking equipment<sup>4</sup> but he is worried about the upcoming end-of-year reporting requirements<sup>3</sup>. Previously Peter<sup>1</sup> successfully set up his own home Wi-Fi network, so he buys the equipment necessary from the local computer store to extend the network wirelessly into the new office. Peter<sup>1</sup> then proceeds to install the Wi-Fi network extension during his lunchtime neglecting to change the default password<sup>5</sup>. He is pleased to inform the staff after lunch that they are now connected in their new office.

1	Number of times character’s name mentioned = 4
2	Manipulation in the story = Impatience
3	Motivation for the act non-malicious? * See definition of non-malicious below
4	Explicit that the act is against company rules
5	Phrase that says the act was performed by the character
160	Wordcount

#### **Definition of Non-Malicious**

According to Guo (2011), Non Malicious Security Violations are characterised as being: (a) *intentional* – differentiating them from accidental violations; (b) *self-benefitting without malicious intent* – or not intending to harm the company or indeed personally profit at the company’s expense; (c) *voluntary* – end users know they are breaking the rules; (d) *Have the potential to cause damage or present a security risk*

## 2. Malicious Scenarios

- **Disgruntlement / personal gain**

John<sup>1</sup> has worked for Buildco plc for the past 25 years preparing bids for major construction projects. Despite being central to the success of the company, John<sup>1</sup> is annoyed that he remains in middle management while several people he mentored are senior managers<sup>2</sup>. He has been approached by a rival company to join their senior management and has secretly accepted their offer. Buildco plc has strict rules around confidentiality whereby only senior management make the final adjustments to bids which are then not seen by anybody else. However, John<sup>1</sup>'s current boss regularly asks him to help her finalise her bids. During a recent meeting, when his boss was called from the office for a private call, John<sup>1</sup>, who is aware of the company's strict policy on confidentiality<sup>4</sup>, emailed the file that they were working on, from her computer to his contact in the rival construction company (and deleted the email)<sup>5</sup>, so his new prospective new employers could win the contract<sup>3</sup>.

- **Disgruntlement / personal gain II**

Tom<sup>1</sup> has worked in the accounts department of the same company since he left school. However, despite being excellent at his job Tom<sup>1</sup> hasn't progressed significantly, continually being passed over by others with professional qualifications<sup>2</sup>. Early on in his career Tom<sup>1</sup> developed a habit of bringing work home in his briefcase and recently he has taken to uploading the details of most of his daily work to a shared cloud storage drive. Although he knows that this is against the company rules<sup>4</sup>, his boss has a habit of ringing him outside of office hours and demanding answers to questions so he feels that this rule violation is necessary. Recently, a rival company has approached Tom<sup>1</sup> with a job offer, which he has accepted. However, before handing in his notice, he downloads all the information from the cloud storage drive to his personal laptop<sup>5</sup>, thinking that being armed with this information might help him to get ahead in his new job<sup>3</sup>.

1	Number of times character's name mentioned = 4
2	Manipulation in the story = Annoyance
3	Motivation for the act malicious ? * See definition of malicious below
4	Explicit that the act is against company rules ?
5	Phrase that says the act was performed by the character
160	Wordcount

### **Definition of Malicious**

Guo's (2011), characterisation of Non Malicious Security Violations can also be used to frame Malicious Violations by substituting "*with malicious intent*" for "*without malicious intent*" in part (b) of the definition and so are characterised here as: (a) *intentional*; (b) *self-benefitting with malicious intent*; (c) *voluntary*; (d) *Have the potential to cause damage or present a security risk* .

In defining "*with malicious intent*" we take note of the fact that Guo (2011) excluded from his definition of non-malicious acts, those acts that are unethical and benefit the end user at the organisation's expense, and so they are included in the definition of malicious security violations.

## REFERENCES

- Alavi, M., and Weiss, I.R. 1985. "Managing the Risks Associated with End-User Computing," *Journal of Management Information Systems*, pp. 5-20.
- Banham, R. 2015. "Why CIOs Should Be Happy About Shadow IT." *FORBES* Retrieved 30/06/2015, 2015, from <http://www.forbes.com/sites/centurylink/2015/05/04/why-cios-should-be-happy-about-shadow-it/>
- Barlow, J.B., Warkentin, M., Ormond, D., and Dennis, A.R. 2013. "Don't Make Excuses! Discouraging Neutralization to Reduce IT Policy Violation," *Computers & Security* (39:Part B), Nov, pp. 145-159.
- Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Quarterly* (34:3), Sep, pp. 523-548.
- Cavusoglu, H., Mishra, B., and Raghunathan, S. 2005. "The Value of Intrusion Detection Systems in Information Technology Security Architecture," *Information Systems Research* (16:1), Mar, pp. 28-46.
- Cavusoglu, H., Raghunathan, S., and Cavusoglu, H. 2009. "Configuration of and Interaction between Information Security Technologies: The Case of Firewalls and Intrusion Detection Systems," *Information Systems Research* (20:2), Jun, pp. 198-217.
- Cheng, L.J., Li, Y., Li, W.L., Holm, E., and Zhai, Q.G. 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), Nov, pp. 447-459.
- Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M., and Baskerville, R. 2013. "Future Directions for Behavioral Information Security Research," *Computers & Security* (32), Feb, pp. 90-101.
- D'Arcy, J., and Devaraj, S. 2012. "Employee Misuse of Information Technology Resources: Testing a Contemporary Deterrence Model," *Decision Sciences* (43:6), Dec, pp. 1091-1124.
- D'Arcy, J., and Herath, T. 2011. "A Review and Analysis of Deterrence Theory in the IS Security Literature: Making Sense of the Disparate Findings," *European Journal of Information Systems* (20:6), Nov, pp. 643-658.
- D'Arcy, J., and Hovav, A. 2009. "Does One Size Fit All? Examining the Differential Effects of IS Security Countermeasures," *Journal of Business Ethics* (89:1), May, pp. 59-71.
- D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (20:1), Mar, pp. 79-98.
- Doll, W.J., and Torkzadeh, G. 1988. "The Measurement of End-User Computing Satisfaction," *MIS Quarterly* (12:2), Jun, pp. 259-274.
- Edwards, C. 2013. "Identity - the New Security Perimeter," *Computer Fraud & Security*(9), Sep, pp. 18-19.
- Eisenhardt, K.M. 1989. "Building Theories from Case-Study Research," *Academy of Management Review* (14:4), Oct, pp. 532-550.
- FBI, and DHS. 2014. "Increase in Insider Threat Cases Highlight Significant Risks to Business Networks and Proprietary Information." Retrieved 22 Nov 2015, 2015, from <http://www.ic3.gov/media/2014/140923.aspx>
- Fürstenauf, D., and Rothe, H. 2014. "Shadow IT Systems: Discerning the Good and the Evil," in: *European Conference on Information Systems (ECIS)*. Tel Aviv, Israel.
- Guo, K.H., Yuan, Y.F., Archer, N.P., and Connelly, C.E. 2011. "Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model," *Journal of Management Information Systems* (28:2), Fal, pp. 203-236.
- Harrington, S.J. 1996. "The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions," *MIS Quarterly* (20:3), Sep, pp. 257-278.
- Hovav, A., and D'Arcy, J. 2012. "Applying an Extended Model of Deterrence across Cultures: An Investigation of Information Systems Misuse in the Us and South Korea," *Information & Management* (49:2), Mar, pp. 99-110.
- Hu, Q., Xu, Z., Dinev, T., and Ling, H. 2011. "Does Deterrence Work in Reducing Information Security Policy Abuse by Employees?," *Communications of the ACM* (54:6), pp. 54-60.
- Kotulic, A.G., and Clark, J.G. 2004. "Why There Aren't More Information Security Research Studies," *Information & Management* (41:5), May, pp. 597-607.
- Lee, Y., and 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), Apr, pp. 177-187.
- Liao, Q.Y., Luo, X., Gurung, A., and Li, L. 2009. "Workplace Management and Employee Misuse: Does Punishment Matter?," *Journal of Computer Information Systems* (50:2), Win, pp. 49-59.
- Limayem, M., and Hirt, S.G. 2003. "Force of Habit and Information Systems Usage: Theory and Initial Validation," *Journal of the Association for Information Systems* (4:1), pp. 65-97.
- Loch, K.D., Carr, H.H., and Warkentin, M.E. 1992. "Threats to Information-Systems - Today's Reality, Yesterday's Understanding," *MIS Quarterly* (16:2), Jun, pp. 173-186.
- McCarthy, B. 2002. "New Economics of Sociological Criminology," *Annual Review of Sociology* (28:1), pp. 417-442.
- Nagin, D.S., and Paternoster, R. 1993. "Enduring Individual-Differences and Rational Choice Theories of Crime," *Law & Society Review* (27:3), pp. 467-496.
- Nasuni. 2014. "Shadow IT in the Enterprise." Retrieved 30/06/2015, 2015, from <http://www.nasuni.com/resource/shadow-it-in-the-enterprise/>
- Paternoster, R., and Simpson, S. 1996. "Sanction Threats and Appeals to Morality: Testing a Rational Choice Model of Corporate Crime," *Law & Society Review* (30:3), pp. 549-583.
- Posey, C., Bennett, R.J., and 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), Sep-Oct, pp. 486-497.
- Rebollo, O., Mellado, D., and Fernandez-Medina, E. 2012. "A Systematic Review of Information Security Governance Frameworks in the Cloud Computing Environment," *Journal of Universal Computer Science* (18:6), 2012, pp. 798-815.

- SANS Institute. 2015. "Insider Threats and the Need for Fast and Directed Response." Retrieved 22 Nov 2015, 2015, from <https://http://www.sans.org/reading-room/whitepapers/analyst/insider-threats-fast-directed-response-35892>
- Saunders, M., Lewis, P., and Thornhill, A. 2012. *Research Methods for Business Students*. Essex, England: Pearson.
- Schalow, P.R., Winkler, T.J., Repschlaeger, J., and Zarekew, R. 2013. "The Blurring Boundaries of Work-Related and Personal Media Use: A Grounded Theory Study on the Employee's Perspective," *ECIS*, p. 212.
- Silic, M., and Back, A. 2014. "Shadow IT - a View from Behind the Curtain," *Computers & Security* (45), Sep, pp. 274-283.
- Siponen, M., and Vance, A. 2010. "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations," *MIS Quarterly* (34:3), Sep, pp. 487-502.
- Siponen, M., and Vance, A. 2014. "Guidelines for Improving the Contextual Relevance of Field Surveys: The Case of Information Security Policy Violations," *European Journal of Information Systems* (23:3), May, pp. 289-305.
- Straub Jr, D.W. 1990. "Effective IS Security: An Empirical Study," *Information Systems Research* (1:3), pp. 255-276.
- Trendmicro. 2014. "The Insider Threat: How Much Should Enterprises Worry About Its Impact on Cybersecurity?" Retrieved 22 Nov 2015, 2015, from <http://blog.trendmicro.com/insider-threat-much-enterprises-worry-impact-cybersecurity/>
- van Kessel, P., and Allan, K. 2014. "Get Ahead of Cybercrime - EY's Global Information Security Survey." Retrieved 22 Nov 2015, 2015, from <http://www.ey.com/GL/en/Services/Advisory/EY-global-information-security-survey-2014>
- Vance, A., Lowry, P.B., and Eggett, D. 2013. "Using Accountability to Reduce Access Policy Violations in Information Systems," *Journal of Management Information Systems* (29:4), Spr, pp. 263-289.
- Vance, A., and Siponen, M. 2012. "IS Security Policy Violations: A Rational Choice Perspective," *Journal of Organizational and End User Computing* (24:1), Jan-Mar, pp. 21-41.
- Vorometric. 2015. "Vorometric Insider Threat Report." Retrieved 22 Nov 2015, 2015, from [http://enterprise-encryption.vorometric.com/rs/vorometric/images/CW\\_GlobalReport\\_2015\\_Insider\\_threat\\_Vormetric\\_Single\\_Pages\\_010915.pdf](http://enterprise-encryption.vorometric.com/rs/vorometric/images/CW_GlobalReport_2015_Insider_threat_Vormetric_Single_Pages_010915.pdf)
- Warkentin, M., and Willison, R. 2009. "Behavioral and Policy Issues in Information Systems Security: The Insider Threat," *European Journal of Information Systems* (18:2), Apr, pp. 101-105.
- Weber, J. 1992. "Scenarios in Business Ethics Research: Review, Critical Assessment, and Recommendations," *Business Ethics Quarterly* (2:2), pp. 137-160.
- Willison, R., and Warkentin, M. 2013. "Beyond Deterrence: An Expanded View of Employee Computer Abuse," *MIS Quarterly* (37:1), Mar, pp. 1-20.
- Yue, W.T., and Cakanyildirim, M. 2007. "Intrusion Prevention in Information Systems: Reactive and Proactive Responses," *Journal of Management Information Systems* (24:1), Sum, pp. 329-353.
- Zissis, D., and Lekkas, D. 2012. "Addressing Cloud Computing Security Issues," *Future Generation Computer Systems-the International Journal of Grid Computing and Esience* (28:3), Mar, pp. 583-592.