THE INSIDER THREAT – UNDERSTANDING THE ABERRANT THINKING OF THE ROGUE "TRUSTED AGENT"

Research in Progress

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

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

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

Abstract

A deficiency exists in the Information Systems Security literature because of the paucity of research aimed at understanding the mind of the 'insider criminal'. Much of the academic and popular press focuses on external breaches but the greatest danger to an organisation lurks within. Whatever the motivation, the 'trusted agent' inside the organisation has the potential to do more damage than an anonymous outsider and it is by increasing our understanding of this threat that we will get greater value for our defence efforts. While acknowledging that a significant number of security incidents are attributable to employees, it is important to remember in an organisational context, that simply increasing security controls and sanctions has previously been shown to be counterproductive. Therefore this research-in-progress takes the approach of increasing our understanding of how such offenders think, through a synthesis of Rational Choice Theory, Deterrence Theory, Neutralisation Theory and elements from Criminological Theory. In deliberately prioritising problems that are important in practice and basing our measures on these priorities we will improve on the contextual relevance of previous studies in this area, thereby making a solid contribution to the field.

Keywords: Cybercrime, Computer Abuse, Insider Abuse.

1 Introduction

This research is motivated by a number of factors including the certainty that a substantial proportion of computer security incidents are due to the intentional actions of legitimate users (D'Arcy and Hovav 2007; Guo et al. 2011). Understanding these behaviours has several implications, not least the allocation of security budgets (D'Arcy and Hovav 2007) and developing and implementing security practices and policies (Siponen and Vance 2010), but our effectiveness in designing appropriate countermeasures will forever be hamstrung without a greater understanding of what prompts these individuals to attack or misuse computer systems (Mahmood et al. 2010). Furthermore, in the context of employee or insider abuse it is not just the volume of incidents that is important but also the potential for loss or damage to the employer. The insider threat represents the greatest threat of all (Warkentin and Willison 2009) and simply presuming to increase levels and stringency of computer security is not the panacea for all ills, as this can sometimes have the unintentional effect of fostering the behaviours that it is actually designed to deter (Posey et al. 2011). Therefore what is required is a holistic approach - grasping the notion of the employee as a criminal and getting to understand the mind of this ‘insider criminal’. Consequently our goal with this research is to ascertain what thoughts and cognitive elements are present, prior to an employee intentionally breaking information security rules. We will do this by extending existing theories, synthesising them in a new way and then applying them to current problems experienced in practice.

This study will also make additional contributions to the Behavioural Information Security Field in a number of ways. In expanding constructs like Intrinsic Benefit to include more than hedonistic feelings such as ‘thrill’ and ‘pleasure’, we will extend the construct away from its traditional conceptualisation. Additionally by drawing on criminological theory and incorporating variables such as ‘Emotional State’ and ‘Prior Punishment Experience’, we will expand the explanatory power of the model in a way that we have not seen in prior literature. Finally, by examining the notion of Moral Reasoning and applying it to the benefits to the offender of offending, we will extend the work previously begun by Myyry et al (2009). From a methodological point of view this study will incorporate the guidelines recently set out by Siponen and Vance (2014), designed to improve the contextual relevance of such work and in so doing will also take note of the suggestions expressed in (D'Arcy and Herath 2011) which sought to make sense of the disparate findings of previous studies.

The remaining sections of this paper are laid out as follows. In the next section is a brief review of the literature, and in particular empirical studies conducted in relation to the phenomenon of interest. Next we provide an explanation and justification of the elements contained in the research model with associated propositions, and finally we conclude with a brief description on the intended next steps.

2 Literature Review

The existing studies that relate to IS Rules or Policies have dependent variables that are expressed in negative and positive terms and we include both in our review because their constructs are not necessarily mutually exclusive. This is particularly exemplified in Myyry et al (2009) where the title refers to “adherence”, describing the dependent variable as “compliance” yet suggesting in the abstract that they are “proposing a theoretical model that explains *non-compliance”*.

A systematic review in line with Weber & Watson (2002) was carried out in order to plot the landscape in this regard. The period selected for review covered the years 2004 to 2014 inclusive and initially we performed a series of relevant security related keyword searches on the leading “Basket of 8” information systems journals for these years. This was subsequently expanded to include information security journals, which we selected on two bases. Initially we selected journals that included the word “security” in the their publication titles and subsequently, in order to manage the scope of this second search, we prepared a composite ranking of these journals based on a combination of academic ranking indices including ISI Web of Knowledge, SCOPUS and APHIS. We then selected journals based on whether they appeared in the top 10 positions in one or all of these rankings, and selected articles for detailed review based on an examination of their titles and abstracts. Finally, the resulting studies were triangulated with studies previously reviewed in two key publications in this area (D'Arcy and Herath 2011; Siponen and Vance 2014), as a final attempt at ensuring rigour in our review.

The range of topics included in the final review that contained a dependent variable which could be described as a positive behaviour included: *Behavioural Intention To Use Spyware* (Johnston and Warkentin 2010), *Information System Security Policy Compliance* (Chen et al. 2012; Myyry et al. 2009; Pahnila et al. 2007; Siponen et al. 2014; Siponen et al. 2010; Son 2011), *ISSP Compliance Intention* (Bulgurcu et al. 2010; Herath and Rao 2009a; Herath and Rao 2009b; Ifinedo 2012; Ifinedo 2014; Vance et al. 2012) and *Taking Precautions* (Boss et al. 2009). This would seem to suggest that the vast bulk of such studies relate to either Information Security Policy Compliance or Compliance Intention.

In terms of dependent variables that are expressed as negative behaviours, the extant literature is somewhat diverse, if a little limited. These studies and the theories used in their model development are summarised in Table 1 below and while none of them contain our exact description of the dependent variable i.e. “**Intentional IS Rule Violation**”, it is felt that most could be seen as proxies for the dependent variable described in this paper. The main reason for our use of the word ‘Rule’ rather than ‘Policy’ in our description is simply to deal with the reality that many firms may have rules that are not enshrined within formal information security policies.

Dependent Variable	**Reference**	**Theories Used**
Computer Abuse	(Straub Jr 1990)	General Deterrence Theory
	(Lee et al. 2004)	General Deterrence Theory, Social Control Theory, Theory of Planned Behaviour
	(Posey et al. 2011)	Causal Reasoning Theory, Attribution Theory
Computer Abuse (judgements and intentions)	(Harrington 1996)	General Deterrence Theory, Ethics Theory
Intention to Commit Corporate Crime	(Paternoster and Simpson 1996)	Deterrence Theory, Rational Choice Theory, Subjective Utility Theory
Internal Information Systems Misuse	(D'Arcy and Hovav 2007)	Deterrence Theory
IS Misuse Intention	(D'Arcy et al. 2009)	General Deterrence, Extended Deterrence Theory
	(Hovav and D'Arcy 2012)	Deterrence Theory, Legitimacy Theory
Intention To Violate ISSP	(Siponen and Vance 2010)	Deterrence Theory, Neutralisation Theory
	(Vance and Siponen 2012)	Deterrence Theory, Rational Choice Theory
	(Barlow et al. 2013)	Deterrence Theory, Neutralisation Theory, Framing Theory
	(Cheng et al. 2013)	Deterrence Theory, Social Bond Theory
Non-malicious Security Violation Intention	(Guo et al. 2011)	Deterrence Theory, Neutralisation Theory, Theory of Planned Behaviour, Theory of Reasoned action
Intention to commit computer misconduct	(Hu et al. 2011)	Deterrence Theory, Rational Choice Theory, Self-control Theory
Technology Misuse Intention	(D'Arcy and Devaraj 2012)	Deterrence Theory, Deindividuation Theory, Role Theory
Access Policy Violation Intention	(Vance et al. 2013)	Accountability Theory

Table 1. Prior literature examples of conceptualisations of “negative” behaviours and major theories used in model development

Most of the extant literature in this area has employed some form of deterrence theory approach as the primary theory of investigation, classically involving constructs like sanction severity and certainty or the more modern conceptualisation of formal and informal sanctions. It is our intention to remain consistent with this approach of the primacy of deterrence theory but to incorporate it into the basic structure of rational choice theory so that we can examine with equal rigour the benefits as well as the costs of offending. The next section outlines our rationale for combining these two theories in this research.

3 Framework Development

One of the leading theories in behaviour motivation is Protection Motivation Theory (Rippetoe and Rogers 1987; Rogers 1975) – a theory that has found considerable traction in the Behavioural Information Security field. In relation to the studies examined as part of the review for this research Protection Motivation Theory (PMT) features significantly. However, it is notable that all of these studies are based on compliance rather than non-compliance. This may occur because in general the theory is predicated on fear as a motivating factor, which makes sense in the context of dealing with an outsider threat, whereas, in our opinion, it is unlikely that an insider criminal's cognitions are "triggered" by fear of sanctions for non-compliance. Therefore, while PMT may indeed contain many relevant cognitive variables, it seems more logical to base the design of this study on a theory that starts from a different premise.

Rational Choice Theory (RCT) is a neo-classical economic approach that offers a theoretical explanation of individual choice making. A succinct description of the approach - to crime in particular - is available in (McCarthy 2002) where it is described thus:

> *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.*

The relevance of the RCT approach for our study begins with its emergence in the corporate crime literature including Paternoster and Simpson's (1996) suggestion that decisions to offend are based on balancing both the costs and benefits of offending. This intrinsic notion that the benefits of the act of offending are a vital part of the decision is what makes this theory so important to our study. Surprisingly, the application of the theory to IS security policy violation studies is rather sparse. Viewing RCT as a "modern extension of classical deterrence theory", Vance and Siponen (2012) contend that although relevant, the theory has "*not yet been applied to*" IS security research although it is central to an earlier article by Hu et al (2011). Thus we find it appropriate to base the framework for our research on Rational Choice Theory with the twin concepts of 'Costs of Offending to the Employee' and 'Benefits of Offending to the Employee' as the two primary dependent variables (see Figure 1).

3.1 Costs

The most commonly used variables relating to costs of violation are detection certainty and severity, although the research to date does not provide any significant degree of unanimity. For example (Straub Jr 1990) found both deterrent severity and deterrent certainty to be significant but with severity being a stronger predictor. In a later study (D'Arcy et al. 2009) found that while severity did have a significant effect on IS Misuse, certainty of sanctions did not. This latter result is mirrored in (Cheng et al. 2013) which can be in turn be contrasted with (Hu et al. 2011) which found all the deterrence constructs to be insignificant. This divergence of findings is made all the more interesting when looking at (Hovav and D'Arcy 2012) who found that the relative strengths of certainty and severity were actually inverted when tested in different cultures. This lack of consistency continues through the so-called "positive" behaviours relating to compliance and compliance intention. Detection certainty was found to have a significant relationship with ISSP compliance intention in (Herath and Rao 2009a; Herath and Rao 2009b) with severity of penalty actually having a negative impact. In (Son 2011) neither were significantly associated with compliance intention and in (Chen et al. 2012) punishment severity was found to relate significantly to compliance intention.

It is not just formal sanctions that form part of Deterrence studies. In more modern conceptualisations of deterrence theory we find classifications of sanctions into formal and informal sanctions. Informal sanctions have been operationalised in the extant research as; social censure, shame, loss of self-respect (Paternoster and Simpson 1996), loss of respect, shame and damage to promotion prospects (Siponen and Vance 2010), social desirability pressure, moral beliefs (D'Arcy and Devaraj 2012; Hovav and D'Arcy 2012) and loss of respect of co-workers, loss of respect from management and damage to promotion prospects (Vance and Siponen 2012). Again with regard to informal sanctions the results to date are somewhat mixed.

However, just because there are disparate findings does not mean that Deterrence Theory, which has been used to predict behaviours in such fields as criminology, politics, military strategy and sociology should be abandoned. For one thing, there is a suggestion that formal and informal sanctions may have an interactive effect and (D'Arcy and Devaraj 2012) argue that there is a lack of research that explores this relationship between formal and informal sanctions. A comparative analysis of the disparate findings is presented by (D'Arcy and Herath 2011), who identify several relevant factors such as Individual Factors (self-control, computer self-efficacy and moral beliefs), Contextual Factors (virtual status, employee position) and methodological issues that may account for some of the differences in previous findings. Because we intend to adopt their recommendations we believe that many of the concerns about disparate results from previous studies can be dispelled. Therefore its seems appropriate to include the following proposition in our model:

P1: The expected costs to the employee of breaking IS security rules, in the form of formal sanction severity and certainty along with informal / extralegal sanctions, will negatively impact the employee's intention to break those rules

3.2 Benefits

The concept of benefits to the employee of committing computer abuse / misuse seems to be particularly under-researched, based on our analysis of the extant literature. In general, benefits can be divided into extrinsic and intrinsic benefits with the former referring to benefits like material gains and the latter to benefits from the actual deviant act itself such as thrill or pleasure. For example (Hu et al. 2011) measure extrinsic benefits as 'having more material possessions or money' or 'being able to afford things previously not affordable', and they measure intrinsic benefits as feeling proud, thrilled, happy or satisfied. In a few studies, we see benefits from the aberrant actions measured as a simple time-saving benefit (Vance and Siponen 2012; Vance et al. 2012). While there is obviously a dearth of research in this particular area, it is noteworthy that perceived benefits had a positive significant effect in the aforementioned studies with intrinsic benefits being even more significant than extrinsic benefits in Hu et al (2011). What does not appear to have been addressed in the existing literature, however, is the notion of "vindication" as an intrinsic benefit. In other non-empirical literature we see several mentions of disgruntlement and organisational justice as motivations for internal abuse of computer systems (Warkentin and Willison 2009; Willison and Warkentin 2013), yet the satisfaction from 'taking revenge' does not appear to have been empirically examined in any of the literature reviewed to date.

It is our intention therefore to create novelty in this aspect by expanding the operationalisation of the intrinsic benefit construct, thereby making a unique contribution to the body of knowledge. Thus we suggest:

P2: The expected benefits to the employee of breaking IS security rules in the form of extrinsic and intrinsic Benefits will positively impact the employee's intention to break those rules.

3.3 Pre-Kinetic Aspects

The use of the term "pre-kinetic" is adapted from Willison and Warkentin (2013) and stems from military strategy with the focus on temporal antecedents of military aggression. In conceptualising a number of variables in our model that precede the rational choice evaluation, we have chosen to stress their temporal nature in triggering and informing subsequent processes, in a manner similar to the 'left-of-bang' (Allen 2003) meaning from military strategy.

3.3.1 Neutralisation

The concept of Neutralisation has proven popular in various streams of modern academic literature, having it's origins in a seminal paper by Sykes and Matza (1957). In their paper they describe justifications or excuses for delinquent behaviour as techniques of neutralisation and divide them into five major types: denial of responsibility, denial of injury, denial of the victim, condemnation of the condemners and appeal to higher loyalties.

Subsequent citations of the Sykes and Matza paper span several disciplines and given the suggestion in (Willison and Warkentin 2013) that neutralisation's relevance to the corporate context is because employees have a greater stake in conventional society and consequently may not be as singularly committed to their criminal tendencies as hardened criminals, it is surprising that the exploration of these techniques in relation to IS security behaviour is so sparse. Within the seven journal articles that we found in our review, only two involved empirical studies of neutralisation.

In the first of these two, Siponen and Vance (2010) advance an extension of Neutralisation Theory, which they describe as not having gained any traction in the context of IS. They include two additional types of neutralisation behaviour, - defence of necessity and metaphor of the ledger, - and then combine the theory with Deterrence Theory, finding that all techniques tested had a strong significant effect on the dependent variable and in fact that in the presence of the neutralisation construct, the various deterrent effects were negated. In a striking contrast with our proposed work, they only explored Neutralisation in the presence of the "costs" side of the Rational Choice calculus. In a later paper (Barlow et al. 2013) tested three types of Neutralisation with mixed findings. Thus we feel it appropriate to suggest:

P3(a): Neutralisation techniques may impact an employee's intention to break IS security rules by influencing how the expected costs and benefits of offending are evaluated.

3.3.2 Moral Reasoning

In a seminal paper (Haidt 2001) proposes that moral judgements are intuitive in nature, whereas Kohlberg found a six-level progression of increasing sophistication involving deliberate conscious thought. To test this theory Rest (1979) developed the Defining Issues Test (DIT) which has become the most widely utilised method in moral research and was used by Myyry et al (2009) in conjunction with the Theory of Motivational Types of Values (Schwartz 1992). Their findings suggested a link between compliance and types of moral reasoning.

Earlier, in a study of corporate crime, Paternoster and Simpson (1996) concluded that when moral inhibitions were high, considerations of costs and benefits of the crime were virtually superfluous, but when weak, deterrence factors came into play. Moral beliefs have also found their way into studies of IS misuse intention (D'Arcy and Devaraj 2012; Hovav and D'Arcy 2012; Hu et al. 2011; Vance and Siponen 2012).

The approach in this study will not be to simply elicit the moral belief from the respondent but rather to mirror the approach taken in Myyry et al (2009) in determining how the respondents reason in order to arrive at their moral beliefs. Given that we will be examining this in light not just of costs but also benefits we believe that we will have another point of distinctiveness in our research and therefore we put forward the following proposition:

P3(b): Moral reasoning will impact the evaluation of both costs and benefits of offending to an employee contemplating violating IS rules.

3.3.3 Emotional State

McCarthy (2002) posits that the rational choice perspective does not actually preclude the possibility of people acting irrationally (sometimes occurring because of a particular emotional state). Lowenstein (1996) makes a similar point and speaks of visceral factors "crowding out" all other goals which he then illustrates by referring to the behaviour of phobics who are "typically perfectly aware that the object of their fear is objectively nonthreatening, but are prevented by their own fear from acting on this judgment". Unfortunately empirical studies relating this construct to behaviour are somewhat scant although Lowenstein and colleagues did make an initial foray in this regard (Loewenstein et al. 1997). A similar study by (Bouffard 2002) found results consistent with the earlier Lowenstein experiment. In a further study examining anger, Exum (2002) found that alcohol and anger interacted to increase aggressiveness, although neither did so independently, but the perceived costs and benefits were unaffected. This notion of anger and its relationship with the crime of assault was examined by (Carmichael and Piquero 2004) who found that anger did not relate to sanctions but that it did have a significant intrinsic benefit effect.

Given the lack of empirical work in this area, in particular within the IS security field, we believe that it would make a worthwhile contribution to knowledge to include "emotional state" as a construct in our model and thus we submit the following proposition:

P3(c): High emotional states impact the evaluation of both costs and benefits of offending to an employee contemplating intention to violate IS rules and may extend to actually negating *considerations of costs and benefits entirely, resulting in a direct effect on intention to break rules.*

3.3.4 Impulsivity

The idea of impulsivity is not to be confused with, or to be considered part of, the previously discussed emotional state. The latter refers to states of mind whereas the former is effectively a personality trait. In their review of the deterrence literature, (D'Arcy and Herath 2011) suggest that empirical validation of a contingent effect of self-control on the sanctions to behaviour relationship does not exist, representing a gap in the literature. This gap has since been addressed somewhat by (Hu et al. 2011) although they do not seem to have explored its effect on sanctions or on the whole rational choice calculus.

A separate conceptualisation of the personality trait is provided in (Grasmick et al. 1993) who provide a 24-item scale for measuring the trait. The 4-item subscale relating to impulsivity is used in (Pogarsky and Piquero 2004) where impulsivity rendered the prospect of a delayed penalty less compelling. A similar finding emerged in (Nagin and Pogarsky 2001) although they described the trait as "present-orientation".

Because the literature in general seems to suggest that people sometimes act in an impulsive manner it is this latter notion of impulsivity that we believe is pertinent and worth measuring and thus we suggest the following proposition:

P3(d): Impulsivity levels in an individual will have the effect of diminishing the impact of both formal and informal sanctions while at the same time increasing the perceived benefits of offending.

3.4 Experiential Variables

There are two additional variables that we believe will add to the explanatory power of our model:
prior punishment experience and computer self-efficacy.

3.4.1 Prior Punishment Experience

Much of the deterrence literature contains, in addition to severity and certainty, the notion of punishment celerity. This refers to the swiftness of punishment and its reason for inclusion is in some respects attributed to, or grounded in, "Pavlovian Conditioning" where punishment is meted out with certainty and swiftness. In a somewhat dissenting view (Nagin and Pogarsky 2001) point out that humans possess far greater cognitive ability to connect acts with temporally remote consequences. Arguing that people remember punishment and associate it with its cause, they believe that it is through a person's awareness and knowledge of punishment, that deterrence is achieved. This effect was observed in (Pogarsky and Piquero 2004) and while the variable does not seem to have found its way into the Information Systems Security field we believe it appropriate to posit that:

P4: Prior punishment experience by self and known others will have a significant positive impact on the costs of offending in terms of formal and informal sanctions.

3.4.2 Computer Self-Efficacy (CSE)

While the concept of computer self-efficacy permeates the IS literature extensively, its applicability in the context of security policy violation may be a little bit less obvious. However, Son (2011) did find that the variable was positively related to *compliance,* with similar findings in (Ifinedo 2012; Ifinedo 2014). While these studies are compliance rather than non-compliance related, D'Arcy and Herath (2011) suggest that individuals high in self-efficacy often believe that they can circumvent security measures and get away with it, or to put it another way the deterrent effect is lesser for those with greater skills and expertise. An earlier criminological study by McCarthy (2002) agrees and D'Arcy and Hovav's (2009) suggestion that CSE attenuates the relationship between sanction and intention therefore prompts us to suggest that:

P5: Computer self-efficacy will have a significant negative impact on the relationship between costs of behaviour to the offender and intention to break IS Security rules

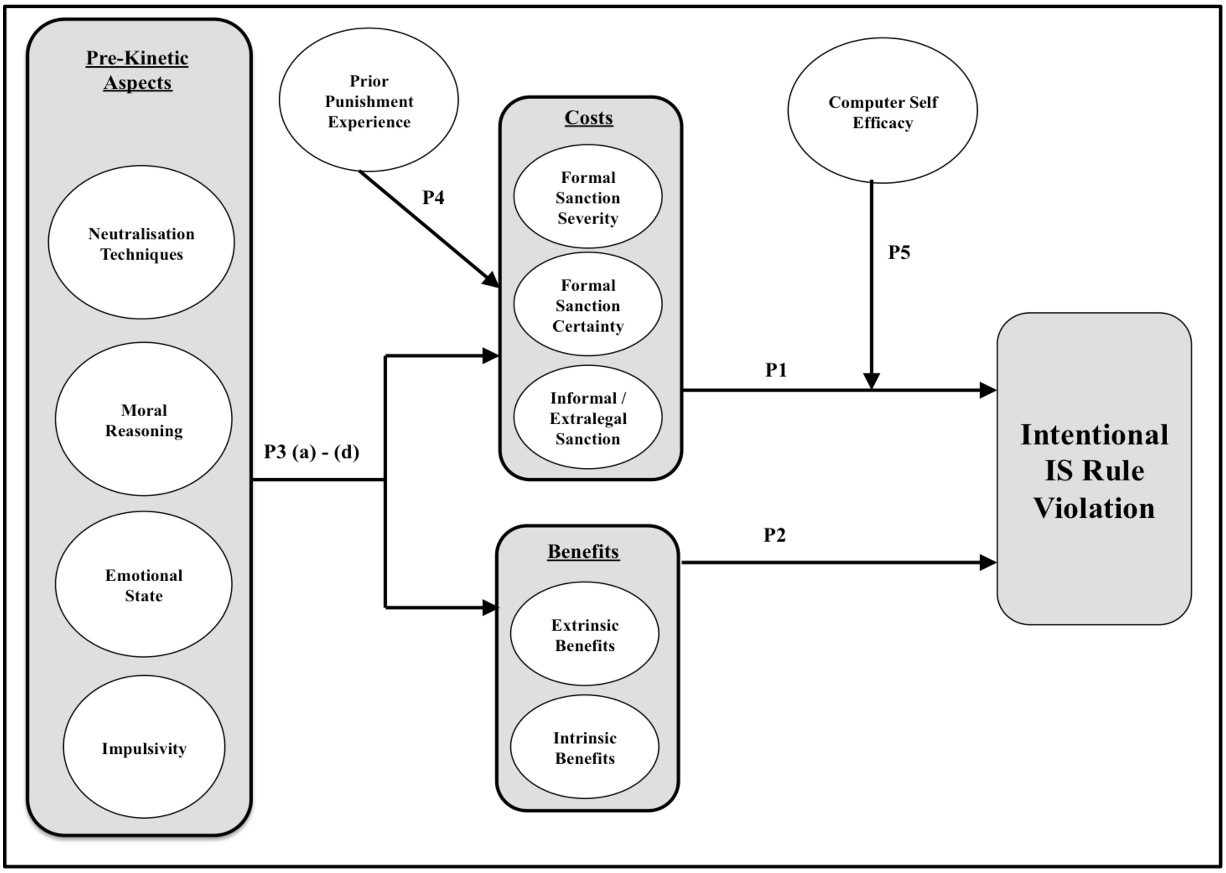

Figure 1: Proposed Research Model

4 Next Steps

The research will be conducted using a mixed-methods approach, a paradigm that continues to grow and gain legitimacy (Fry et al. 1981; Johnson et al. 2007; Morgan 2007). The research instrument will have as its foundation a series of relevant vignettes or scenarios. The use of vignettes has been successfully employed in previous studies to examine behaviours such as thinking style and entrepreneurial decision making (Bird et al. 2012; Epstein et al. 1996; Sadler-Smith and Shefy 2004; Vance et al. 2007), morality and computer related behaviours (Gattiker and Kelley 1999), moral reasoning (Myyry et al. 2009), police misconduct (Pogarsky and Piquero 2004), neutralisation techniques (Siponen and Vance 2010) and ISSP compliance / misuse (D'Arcy and Hovav 2009; D'Arcy et al. 2009; Hovav and D'Arcy 2012; Vance et al. 2012). According to Vance et al (2012) "such methods are a common way of assessing anti-social and ethical/unethical behaviour, and are increasingly used in studies of computer abuse".

In designing the instrumentation for this study a number of guidelines as laid down in (Siponen and Vance 2014) will be adhered in order that our results are more likely to "address important problems in practice". From a practical point of view Siponen and Vance (2014) suggest that when ISP violations or IS misuse is the phenomenon of interest then it makes sense to interview people responsible for designing and enforcing ISPs so that we can examine specific and relevant violations / misuses. It is our intention to adapt the approach taken in (Limayem and Hirt 2003) for belief elicitation, with the difference being that in our study this will take place using an 'expert interview' technique. The two item categories that need to be addressed are the (a) specific violations and (b) benefits from offending to the offender, which we will also ask respondents to rank in order of importance. Doing this for both violations and benefits, we believe, represents an approach not previously used in the literature, thereby creating a further contribution with this work, and one that will provide not only a firm foundation, but also a highly relevant one for the quantitative element of the research.

References

Allen, J. (2003). *Guest Blog: The Combat Operator*. URL: http://defensetech.org/2009/03/23/guest-blog-the-combat-operator/ (Visited on 26 Nov 2014).

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), 145-159.

Bird, B., Schjoedt, L., and Baum, J. R. (2012). "Entrepreneurs' Behavior: Elucidation and Measurement Introduction." *Entrepreneurship Theory and Practice* 36 (5), 889-913.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., and 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.

Bouffard, J. A. (2002). "The Influence of Emotion on Rational Decision Making in Sexual Aggression." *Journal of Criminal Justice* 30 (2), 121-134.

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), 523-548.

Carmichael, S., and Piquero, A. R. (2004). "Sanctions, Perceived Anger, and Criminal Offending." *Journal of Quantitative Criminology* 20 (4), 371-393.

Chen, Y., Ramamurthy, K., and Wen, K. W. (2012). "Organizations' Information Security Policy Compliance: Stick or Carrot Approach?" *Journal of Management Information Systems* 29 (3), 157-188.

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), 447-459.

D'Arcy, J., and Devaraj, S. (2012). "Employee Misuse of Information Technology Resources: Testing a Contemporary Deterrence Model." *Decision Sciences* 43 (6), 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), 643-658.

D'Arcy, J., and Hovav, A. (2007). "Deterring Internal Information Systems Misuse." *Communications of the ACM* 50 (10), 113-117.

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), 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), 79-98.

Epstein, S., Pacini, R., DenesRaj, V., and Heier, H. (1996). "Individual Differences in Intuitive-Experiential and Analytical-Rational Thinking Styles." *Journal of Personality and Social Psychology* 71 (2), 390-405.

Exum, M. L. (2002). "The Application and Robustness of the Rational Choice Perspective in the Study of Intoxicated and Angry Intentions to Aggress." *Criminology* 40 (4), 933-966.

Fry, G., Chantavanich, S., and Chantavanich, A. (1981). "Merging Quantitative and Qualitative Research Techniques - toward a New Research Paradigm." *Anthropology & Education Quarterly* 12 (2), 145-158.

Gattiker, U. E., and Kelley, H. (1999). "Morality and Computers: Attitudes and Differences in Moral Judgments." *Information Systems Research* 10 (3), 233-254.

Grasmick, H. G., Tittle, C. R., Bursik, R. J., and Arneklev, B. J. (1993). "Testing the Core Empirical Implications of Gottfredson and Hirschi General-Theory of Crime." *Journal of Research in Crime and Delinquency* 30 (1), 5-29.

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), 203-236.

Haidt, J. (2001). "The Emotional Dog and Its Rational Tail: A Social Intuitionist Approach to Moral Judgment." *Psychological Review* 108 (4), 814-834.

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), 257-278.

Herath, T., and Rao, H. R. (2009a). "Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness." *Decision Support Systems* 47 (2), 154-165.

Herath, T., and Rao, H. R. (2009b). "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations." *European Journal of Information Systems* 18 (2), 106-125.

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), 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), 54-60.

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.

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.

Johnson, R. B., Onwuegbuzie, A. J., and Turner, L. A. (2007). "Toward a Definition of Mixed Methods Research." *Journal of Mixed Methods Research* 1 (2), 112-133.

Johnston, A. C., and Warkentin, M. (2010). "Fear Appeals and Information Security Behaviors: An Empirical Study." *MIS Quarterly* 34 (3), 549-566.

Lee, S. M., Lee, S. G., and Yoo, S. (2004). "An Integrative Model of Computer Abuse Based on Social Control and General Deterrence Theories." *Information & Management* 41 (6), 707-718.

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), 65-97.

Loewenstein, G. (1996). "Out of Control: Visceral Influences on Behavior." *Organizational Behavior and Human Decision Processes* 65 (3), 272-292.

Loewenstein, G., Nagin, D., and Paternoster, R. (1997). "The Effect of Sexual Arousal on Expectations of Sexual Forcefulness." *Journal of Research in Crime and Delinquency* 34 (4), 443-473.

Mahmood, M. A., Siponen, M., Straub, D., Rao, H. R., and Raghu, T. S. (2010). "Moving toward Black Hat Research in Information Systems Security: An Editorial Introduction to the Special Issue." *MIS Quarterly* 34 (3), 431-433.

McCarthy, B. (2002). "New Economics of Sociological Criminology." *Annual Review of Sociology* 28 (1), 417-442.

Morgan, D. L. (2007). "Paradigms Lost and Pragmatism Regained Methodological Implications of Combining Qualitative and Quantitative Methods." *Journal of Mixed Methods Research* 1 (1), 48-76.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., and 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.

Nagin, D. S., and Pogarsky, G. (2001). "Integrating Celerity, Impulsivity, and Extra-Legal Sanction Threats into a Model of General Deterrence: Theory and Evidence." *Criminology* 39 (4), 865-891.

Pahnila, S., Siponen, M., and Mahmood, A. (2007). "Employees' Behavior Towards IS Security Policy Compliance". In: *Proceedings of the*: *40th Annual Hawaii International Conference on System Sciences.* Ed. by R.H. Sprague Jr. Waikoloa, Big Island, Hawaii, p. 156.

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), 549-583.

Pogarsky, G., and Piquero, A. R. (2004). "Studying the Reach of Deterrence: Can Deterrence Theory Help Explain Police Misconduct?" *Journal of Criminal Justice* 32 (4), 371-386.

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), 486-497.

Rest, J. 1979. *Development in Judging Moral Issues*. Minneapolis: University of Minnesota Press.

Rippetoe, P. A., and Rogers, R. W. (1987). "Effects of Components of Protection-Motivation Theory on Adaptive and Maladaptive Coping with a Health Threat." *Journal of Personality and Social Psychology* 52 (3), 596-604.

Rogers, R. W. (1975). "Protection Motivation Theory of Fear Appeals and Attitude-Change." *Journal of Psychology* 91 (1), 93-114.

Sadler-Smith, E., and Shefy, E. (2004). "The Intuitive Executive: Understanding and Applying 'Gut Feel' in Decision-Making." *Academy of Management Executive* 18 (4), 76-91.

Schwartz, S. H. (1992). "Universals in the Content and Structure of Values - Theoretical Advances and Empirical Tests in 20 Countries." *Advances in Experimental Social Psychology* 25 (1), 1-65.

Siponen, M., Mahmood, M. A., and Pahnila, S. (2014). "Employees' Adherence to Information Security Policies: An Exploratory Field Study." *Information & Management* 52 (2), 217-224.

Siponen, M., Pahnila, S., and Mahmood, M. A. (2010). "Compliance with Information Security Policies: An Empirical Investigation." *Computer* 43 (2), 64-71.

Siponen, M., and Vance, A. (2010). "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations." *MIS Quarterly* 34 (3), 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), 289-305.

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.

Straub Jr, D. W. (1990). "Effective IS Security: An Empirical Study." *Information Systems Research* 1 (3), 255-276.

Sykes, G. M., and Matza, D. (1957). "Techniques of Neutralization - a Theory of Delinquency." *American Sociological Review* 22 (6), 664-670.

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), 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), 21-41.

Vance, A., Siponen, M., and Pahnila, S. (2012). "Motivating IS Security Compliance: Insights from Habit and Protection Motivation Theory." *Information & Management* 49 (3-4), 190-198.

Vance, C. M., Groves, K. S., Paik, Y. S., and Kindler, H. (2007). "Understanding and Measuring Linear-Nonlinear Thinking Style for Enhanced Management Education and Professional Practice." *Academy of Management Learning & Education* 6 (2), 167-185.

Warkentin, M., and Willison, R. (2009). "Behavioral and Policy Issues in Information Systems Security: The Insider Threat." *European Journal of Information Systems* 18 (2), 101-105.

Webster, J., and Watson, R. T. (2002). "Analyzing the Past to Prepare for the Future: Writing A." *MIS Quarterly* 26 (2).

Willison, R., and Warkentin, M. (2013). "Beyond Deterrence: An Expanded View of Employee Computer Abuse." *MIS Quarterly* 37 (1), 1-20.