2014

Predicting Insider's Malicious Security Behaviours: A General Strain Theory-Based Conceptual Model

Duy P.T. Dang
RMIT University, duy.dang@rmit.edu.au

20P. Predicting Insider’s Malicious Security Behaviours: A General Strain Theory-Based Conceptual Model

Duy P.T. Dang
RMIT University
duy.dang@rmit.edu.au

Abstract

Insider’s malicious information security behaviours have always been a persistent problem and requiring urgent mitigation solutions. More recently, seminal calls for future research suggested exploring the influences of employee-workplace interaction and pre-kinetic events such as organisational injustice since they are argued to hold potential impacts on the insider’s intention to perform abusive computer behaviours. This study responds to those calls by investigating the relationship between organisational injustice and insider’s intention to commit malicious security behaviours. In addition, it employed General Strain Theory–a highly influential theory in criminology yet receives little attention in information security behavioural research. The literature review suggested the employed theory to have close relationship with organisational injustice concepts, therefore adds more explanations to why insiders deliberately perform computer abuses. As a result, a testable conceptual model incorporating strains, disgruntlement and organisational injustice is proposed to describe the relationships between those factors and insider’s malicious information security behaviours. The research concludes with the model’s potential implications, limitations and provides future directions.

Keywords

information security behaviours, insider, general strain theory, organisational injustice, disgruntlement.

1. Introduction

Research on computer users’ behaviours has been playing vital role in maintaining organisational information security yet still falls short of contributions (Crossler et al. 2013). As a result, scholars in the field are calling for studies that incorporate multidisciplinary perspectives to enrich the current knowledge body, especially about exploring the insider’s malicious information security behaviours (Warkentin and Willison 2009; Willison and Warkentin 2013). Of most importance is the extended Security Action Cycle (Willison and Warkentin 2013) introducing the pre-kinetic events that would lead to the insider’s intention to perform computer abuses.

By definition, pre-kinetic events result from the interaction between the employees and their workplace environment (Willison and Warkentin 2013). More important, while these events are argued to influence the intention to perform malicious behaviours, their effects are determined by the harmony between the potential perpetrators and their workplace. For instance, the perpetrator’s abusive intention could be reinforced by disgruntlement that results from negative interaction between them and their organisation’s environment (Willison and Warkentin 2013). Understanding those events would help to prevent the abusive intention by improving the employees-workplace interaction, thus holds practical implications. Since the concept of pre-kinetic events in information security behavioural research has just been introduced, it is empirical to establish a solid foundation for future knowledge to be built upon.

This paper proposes an empirical conceptual model with testable hypotheses that incorporate theoretical constructs from organisational injustice literature and General Strain Theory (Agnew 2009) to predict the employee's intention to commit malicious security behaviours. The structure of the paper is as follow. First, a literature review is performed to justify the research motivations and establish a framework of theoretical constructs. Next, the paper provides a set of testable hypotheses that frame the conceptual model. Potential implications of the proposed conceptual model are then presented. Finally, the conclusion discusses the limitations and future directions to continue from this paper.

2. Research motivations

It is common to find studies that investigate information security issues by adopting multidisciplinary perspectives (Anderson and Moore 2009). For example, Protection Motivation Theory (Rogers 1975) is a theory in medical research that has been widely employed to investigate the cognitive process contributing to the intention to perform adaptive computer behaviours. Specifically, the theory explores the cognitive factors associating with the user's appraisal processes on the threats and the measures that counter such threats. These factors (i.e. perceived severity and vulnerability, response cost and efficacy, self-efficacy and rewards) were found to impact the user's intention to perform various desirable information security behaviours such as compliance with policy (Herath and Rao 2009; Siponen et al. 2007; Vance et al. 2012), adopt online privacy measures (Mohamed and Ahmad 2012), avoid malware in BYOD environment (Dang et al. 2013) and install anti-virus software (Lee et al. 2008). Likewise, Health Belief Model (Janz and Becker 1984) was also employed by a number of research to study information security behaviours (e.g. Liang and Xue 2009, 2010; Ng et al. 2009; Workman 2007). However, these two theories from the medical field were originally applied to investigate the contributing factors of healthy lifestyle (Boer et al. 1996; Janz and Becker 1984). In consequence, the inevitable limitation of both theories is that they were not suitable for explaining abusive intentions.

Criminology theories were also considered in information security behavioural research. Of most significance is the applications of General Deterrence Theory (GDT) which examines the controlling effects of sanction in information security context (e.g. Herath and Rao 2009; Hu et al. 2011; Seppo et al. 2007). Sanctions, which focus on the punishment's severity, certainty and celerity or swiftness (Hu et al. 2011), enable investigations on both compliance and noncompliance intentions. For example, Lee et al. (2004) studied the impacts of GDT's factors on the intention to commit computer abuses. The implementation of security systems was found to have statistically significant influence on self-defence intention which subsequently motivates abuses by insiders and invaders (Lee et al. 2004). In contrast, Hu et al. (2011) did not find any impacts of deterrence on intention to abuse, therefore concluded that deterrence alone failed to reduce such intention. On the other hand, the effects of GDT's factors on different compliance intentions were tested by a number of studies. Notably, Son (2011) found consistent findings about the non-statistically significant impacts of deterrence's factors on the employee's intention to comply with information security policy. Indeed, these studies displayed that the impacts of GDT on compliance/non-compliance intentions remain inconsistent and require further empirical research. In addition, GDT limits to only extrinsic impacts thus leaves the intrinsic factors less explored, albeit they are argued to possess stronger effects on compliance intentions (Son 2011). More recently, Karyda et al. (2005) suggested the potential applications of other criminology theories such as Social Bond

Theory, Social Learning Theory, Theory of Planned Behaviour and Situational Crime Prevention. Nonetheless, the literature review of this paper returned very few results of those theories in information security research.

The previous discussions have provided the motivations to conduct this study. First, incorporating multidisciplinary theories is a common practice to investigate the contributing factors of intention to perform information security behaviours. Second, while the commonly adopted Protection Motivation Theory has been producing consistent and significant findings regarding the motivations of desirable behaviours, there is little theoretical base that explains the abusive ones. As there is a lack of criminology theories applied to investigate abusive intention, it is argued that empirical contributions incorporating crimes-related theories for this purpose could produce novel results. Similarly, this paper's use of General Strain Theory as a criminology theory was justified.

3. Theoretical framework

Our theoretical framework incorporates multidisciplinary concepts and theories that altogether explain how the negative interaction between the employees and their workplace environment could potentially lead to their intention to commit abusive security behaviours. Specifically, these constructs are drawn upon General Strain Theory (including strains and negative emotions) and literature about organisational injustice.

3.1. General Strain Theory

General Strain Theory (GST) was revised and developed by Agnew (2009) upon the classic strain theories that date back to the 1960s. The central idea of GST is about three types of stressful events that encourage an individual to commit crimes through the production of *strains*. Specifically, these strains arise when a person is (1) prevented from achieving positive goals, (2) removed positive stimuli that they possess, or (3) presented with noxious or negative stimuli (Agnew and White 1992 p. 476). In brief, GST focuses on the negative relationships with the others that pressure a person to commit crimes (Agnew 2009).

The theory was originally introduced to predict delinquency and drug use by adolescents (Agnew and White 1992) and later on became highly influential in criminology and criminal justice journals (as cited in DeLisi 2011). More recently, Langton and Piquero (2007) asserted that GST could predict white-collar crimes (which include cybercrime), thus supports its potential applications in predicting malicious information security behaviours. In addition, information systems occupations have been suggested to be highly stressful (Thong and Yap 2000). Consequently, information systems professionals may be extremely prone to strains that encourage them to commit white-collar crimes as the *insiders*. Nonetheless, very few information security behavioural studies were found to apply Agnew's GST (2009) or incorporate strains into empirical models that explain computer abusive behaviours.

3.2. Organisational injustice

In GST, Agnew (2001) argued that strains resulting from various stressful situations could have different capabilities in motivating the intention to commit crimes. More specifically, strains that are perceived as unjust would more likely motivate intention to commit crimes through invocation of negative emotions (Agnew 2009). As a result, this paper incorporates the concepts of organisational injustice from management and organisational studies to explain in details how the employees perceive unjustness from strains. Organisational injustice depicts the perceived unfairness in (1) the outcomes (distributive injustice), (2) the procedures determining the outcomes (procedural injustice) and (3) the treatments received from the others (interactional injustice) (Cohen-Charash and Spector 2001). It is also worth noticing that the first two forms of injustice are regarded as *structural* as they are most likely produced by poor interaction with the organisation. On the other hand, interactional injustice involves more the social part as it concerns the interaction between the employees and their peers or supervisors, thus called *social form*.

Unlike organisational injustice, the counterpart *organisational justice* and its influences on information security behaviours have been investigated by a number of prior studies. For instance, Posey et al. (2011) investigated the reinforcement role of organisational justice towards internal computer abuses. Specifically, they found monitoring at workplace actually defeated its purpose and encouraged abusive information security behaviours as retaliation to the workplace. Moreover, Lim (2002) found significant relationships between organisational justice in reducing cyber-loafing by the employees. Nevertheless, it was rare to find studies investigating *organisational injustice* and their impacts on malicious computer behaviours.

Most recently, the concept of organisational injustice was recommended for future information security behavioural research by Willison and Warkentin (2013) to understand the causes and targets of malicious security behaviours, especially the intentional ones by the insiders. Similarly, literature outside information security behavioural area confirmed the links between the three forms of injustice and counterproductive or deviant work behaviours (e.g. Bechtoldt et al. 2007; Cohen-Charash and Spector 2001; Cropanzana et al. 2007; Francis and Barling 2005; Scheuerman 2013). As a result, organisational injustices were hinted to potentially reinforce the employee's intention to perform abusive information security behaviours. Similar to the lack of GST applications in information security behavioural research, very few studies were found to link organisational injustice with workplace's strains. This paper's theoretical framework consisting of GST and organisational injustice is illustrated in Figure 1 below.

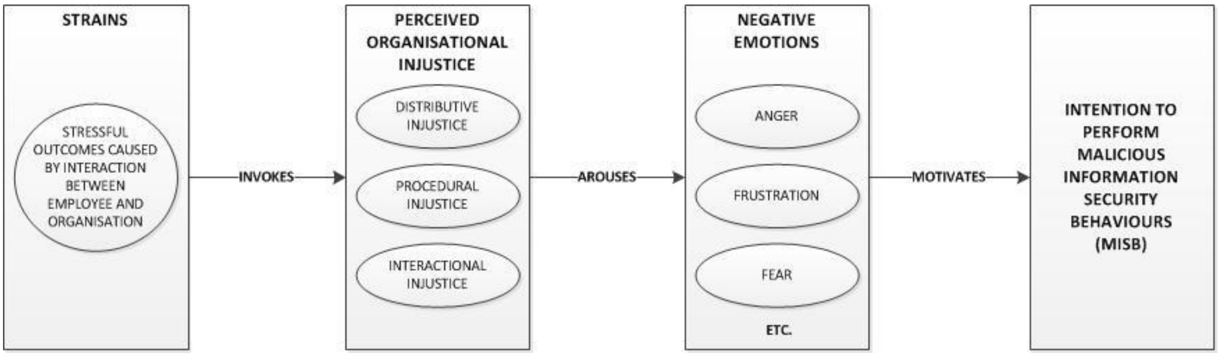
STRAINS
STRESSFUL OUTCOMES CAUSED BY INTERACTION BETWEEN EMPLOYEE AND ORGANISATION
INVOKES
PERCEIVED ORGANISATIONAL INJUSTICE
DISTRIBUTIVE INJUSTICE
PROCEDURAL INJUSTICE
INTERACTIONAL INJUSTICE
AROUSES
NEGATIVE EMOTIONS
ANGER
FRUSTRATION
FEAR
ETC.
MOTIVATES
INTENTION TO PERFORM MALICIOUS INFORMATION SECURITY BEHAVIOURS (MISB)

Figure 1: Proposed theoretical framework (adapted from General Strain Theory and organisational injustice literature)

4. Hypotheses development and conceptual model

The reviewed literature above has justified the relevant theories and concepts that could help to achieve this paper's research goal. The goal includes developing a conceptual model that predicts the insider's intention to commit malicious security behaviours. Having General Strain Theory and organisational injustice as the underpinning theoretical framework, the model argues that the strains resulting from the poor interaction between the employees and their workplace would reinforce their intention to perform malicious security behaviours as the insider. This reinforcing relationship is further explained by the invocation of perceived organisational injustice and disgruntlement. Testing the model's hypotheses would answer the following questions and their sub-questions:

- **RQ1.** What are the contributing factors of insider's intention to perform malicious information security behaviours (including organisation- and individual-targeted behaviours)?
- **RQ2.** To what extent would these contributing factors motivate insider's intention to perform malicious information security behaviours?

4.1. Strains and organisational injustices

It is necessary to identify what constitute strains and how to measure the strains construct so to assist future testing of the model. Accordingly, GST defined strains to be experienced by the employees from a variety of undesirable events. Therefore, it could be argued that the strains construct is measured in formative model comprising of different stressful situations. Agnew (2001) provided a list of strains that are considered as weakly or strongly related to crimes. Based on this list and own observations, this paper suggests four strains that are relevant to information systems professions and their workplace, namely (1) mismatching expectations, (2) sanction pressure, (3) job dissatisfaction and (4) abusive peers.

First, Agnew (2001 p. 345) proposed "work in a secondary labour market" as a strain reflecting negative perceptions of "unpleasant task, little autonomy, coercive control, low pay, few benefits, little prestigious, and very limited opportunities for advancement" and thus perceived as unjust by the employees. This strain is separated into *mismatching expectations* (covering the perceived lacks of monetary rewards, benefits, prestige and opportunities for advancement) and *job dissatisfaction* (including coercive control/insecurity while adding excessive workload and complex procedures). By doing so, it helps to increase the validity of each construct. For instance, a set of observable variables that measure the facets of job dissatisfaction alone would produce more accurate result than measuring both constructs together as originally suggested. In addition, it aligns the strains to match better the types of injustice that each of them would invoke. For example, it is anticipated that *mismatching expectations* construct would be more likely to invoke distributive injustice which concerns the perceived unfairness when evaluating contributions versus rewards (Cropanzana et al. 2007). As a result, the following hypotheses are proposed:

- H1. Mismatching expectations positively contribute to strains.
- H2. Job dissatisfaction positively contributes to strains.

Second, *sanction pressure* was added into the model according to one of Agnew's (2001) suggested strains. Specifically, the author asserted that the employees would feel stressful under supervision or discipline that are "very strict, erratic, excessive given the infraction, and/or harsh" (Agnew 2001 p. 344). This construct is related to the sanction construct of General Deterrence Theory (GDT). Nevertheless, while GDT depicts the potential threatening effects of sanction such as punishment's severity, certainty and celerity, the construct in this context measures the manners with which it is delivered. Indeed, as sanction has been studied for its controlling effects on compliance (e.g. Herath and Rao 2009; Seppo et al. 2007), investigating the impacts of this construct's interactive nature on noncompliance may produce interesting results. It is expected that *sanction pressure* would most likely contribute to perception of interactional injustice if insults, threats and excessively strict discipline were perceived as unfair. The hypothesis is proposed as below:

- H3. Sanction pressure positively contributes to strains.

Third, abusive peers construct focuses on the strain resulting from the poor interaction between the employees and their colleagues. This strain was adopted from Agnew's work (2001 p. 346) which includes “insults/ridicule, gossip, threats, attempts to coercive, and physical assaults”. Nevertheless, this study suggested removing the measure of physical assaults due to its rare occurrence in workplace. Given the interactive nature of this strain, it is expected that this strain would likely to result in perception of interactional injustice. The following hypothesis is presented.

- H4. Abusive peers positively contribute to strains.

As previously discussed that perception of unjustness (i.e. organisational injustice) plays important role in determining how likely a strain could motivate intention to commit the malicious information security behaviours, the following hypotheses are presented.

- H5. Strains positively contribute to the employee’s perception of distributive injustice.
- H6. Strains positively contribute to the employee’s perception of procedural injustice.
- H7. Strains positively contribute to the employee’s perception of interactional injustice.

3.3. Organisational injustices and insider’s malicious security behaviours

To explain in-depth how organisational injustices could reinforce intention to perform malicious security behaviours, negative emotions are added as a mediator. In fact, perceived unfairness was asserted to provoke negative emotions that subsequently foster crimes (Agnew 2001). Such idea was tested in Yang and Diefendorff's work (2009) which found significant relationships between interpersonal injustice and counterproductive workplace behaviours mediated by negative emotions. Consistently, the links between these three factors have been mentioned in many organisational and management studies (Spector et al. 2006). Agnew (2009) also recommended a variety of negative emotions that impact various types of crimes such as anger, depression and fear. Most recently, Willison and Warkentin (2013) suggested future investigations of disgruntlement as a motive of computer abuses. Likewise, disgruntlement was argued to be a psychological indicator of insider’s threat (Greitzer et al. 2010). In fact, anger could energise the perpetrator while making them disregard positive information and reduce the costs of crime, thus motivates the crimes (Agnew 2001). While there are numerous negative emotions that could reinforce crimes (Agnew 2009), anger or disgruntlement receives the most consensus so far in predicting crimes but not computer-related ones, therefore appears worth exploring for its mediator role. As a result, the below hypotheses are added.

- H8. Perception of distributive injustice positively contributes to disgruntlement.
- H9. Perception of procedural injustice positively contributes to disgruntlement.
- H10. Perception of interactional injustice positively contributes to disgruntlement.

3.4. Determining insider’s abusive security behaviours

Last but not least, this section determines the insider’s malicious security behaviours that could be suitably predicted by the proposed model. While malicious computer behaviours are commonly bound to the concept of counterproductive work behaviours, a number of information security studies have identified and categorised further such behaviours based on their intention and consequences. For instance, Loch et al. (1992) introduced the categorisation of information systems' threats in which "internal human's threats" were classified according to their intentions, namely "non-volitional noncompliance", "volitional (but not malicious) noncompliance" and "intentional malicious abuse". Likewise, the recent study of Crossler et al. (2013) also separates maladaptive behaviours of insiders into intentionally (i.e. deviant behaviours) and unintentionally conducted (i.e. misbehaviours). In addition, the taxonomy by Stanton et al. (2005) also detailed two types of intentional malicious behaviours apart from the rest based on their national-wide survey's results. As this study focuses on disgruntlement as a motivator of insider's malicious behaviours, it is reasonably expected that a disgruntled employee would perform abusive computer behaviours deliberately. Therefore, the proposed conceptual model could be most relevant to predict malicious behaviours that are performed intentionally rather than careless misuses.

The category of intentional malicious behaviours is further organised based on different criteria. For example, Stanton et al. (2005) classified malicious computer behaviours with deliberate intention according to the perpetrator's technical expertise. Moreover, Willison and Warkentin (2013) suggested that malicious security behaviours by the insiders could be identified separately depending on their targets. Specifically, retaliations aiming at the organisation such as deliberate noncompliance with security policy or selling confidential information would occur if the disgruntled employee perceived unfair rewards or harsh policy. On the other hand, poor interaction between employees would result in personal malicious behaviours that target individuals such as harassing or sabotaging each one's work.

Since the conceptual model includes the forms of injustice that are caused by structural (i.e. distributive and procedural injustice) and social (i.e. interactional injustice) factors, it would be most justified to consider Willison and Warkentin's suggestion (2013). Specifically, it is anticipated that structural forms of organisational injustice would lead to organisation-targeted retaliations. On the other hand, the social form would result in personal, individual-targeted malicious behaviours that aim at the perpetrator's colleagues. As a result, the following hypotheses are proposed.

- H11. Disgruntlement positively contributes to intention to perform organisation-targeted malicious information security behaviours.
- H12. Disgruntlement positively contributes to intention to perform individual-targeted malicious information security behaviours.

The conceptual model with all of its hypotheses is illustrated in Figure 2.

4. Conclusions

4.1. Potential implications for practice and research

Insider's malicious information security behaviours have always been widely regarded as a persistent and devastating problem due to its damages and unpredictable nature. As a result, emerging and seminal calls for future research (e.g. Crossler et al. 2013; Warkentin and Willison 2009; Willison and Warkentin 2013) have focused on this critical problem. This study responds to those calls and proposes a conceptual model that could potentially bring practical and theoretical implications.

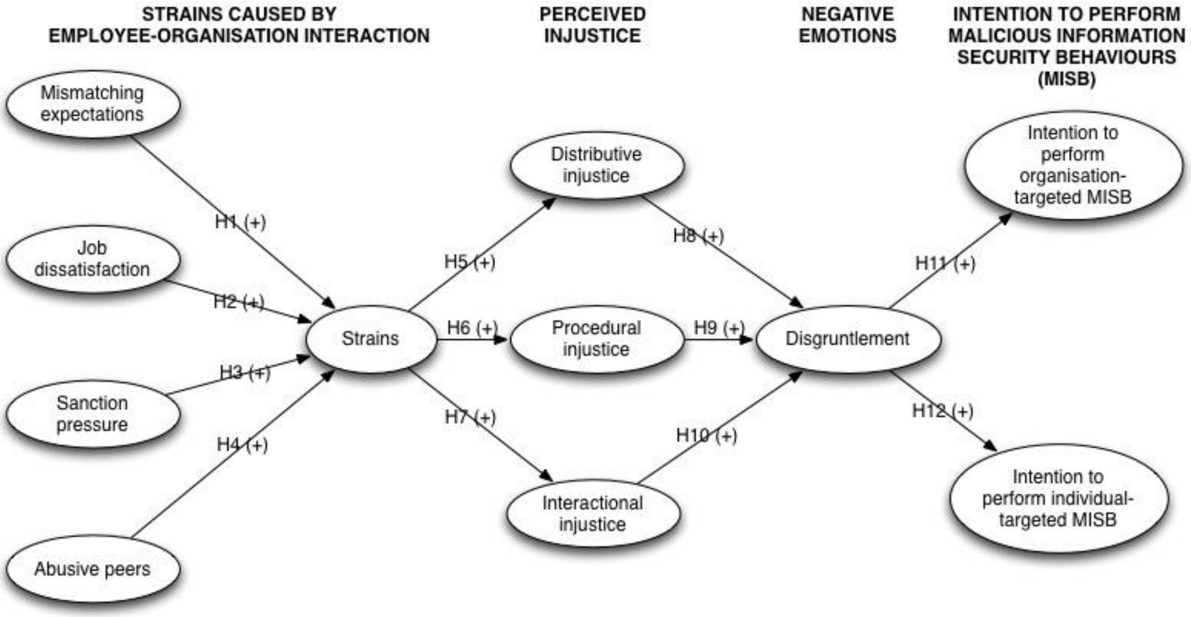

Figure 2: Proposed conceptual model

By determining the impacts of "pre-kinetic events" (i.e. strains and organisational injustice) on the insider's intention to commit malicious security behaviours, practical implications may include mitigating the insider problem through adjustments of policy and workplace's conditions. In addition, employees' perception of strains and injustice could be exploited to improve compliance and reduce potential intention to commit computer abuses. Moreover, the findings may help to clarify whether traditional security controls would reduce abusive computer behaviours or increase the likelihood of those behaviours through strains.

On the other hand, testing the model would shed light on a number of theoretical implications. First, the proposed model employs General Strain Theory (Agnew 2009) which is highly influential in criminology but has not yet received attention in information security behavioural research. Given that the theory is applicable for white-collar crimes (Langton and Piquero 2007) and information systems professionals are highly prone to occupational strains (Thong and Yap 2000), it could be reasonable to argue that testing the GST in information security context may bring interesting and novel results. More important, it contributes knowledge to extend the Security Action Cycle (Straub and Welke 1998) which has been widely used in information security research.

4.2. Future directions

The future work continuing this paper intends to consult more the extant literature (especially in criminology and justice) and experts in the field so that the theoretical framework could be refined. In particular, a qualitative approach would be very much useful to gather and explore insights of information systems professionals about topics such as occupational strains, organisational injustice and insider's malicious security behaviours. After refining the conceptual components and the conceptual model, a pilot study is recommended to assess validity and reliability of the constructs before conducting the main study.

4.3. Limitations

Despite the paper has developed the conceptual model according to suggestions and confirmed findings from seminal studies, the literature review was not exhaustive. In fact, the model is designed to test only the effects of four strains (i.e. mismatching expectations, job dissatisfaction, sanction pressure and abusive peers) on the two specific types of malicious security behaviours (i.e. organisation- and individual-targeted), which are mediated by disgruntlement. As a result, other relevant constructs could be considered and added to the current theoretical framework.

References

Agnew, R. (2001), “Building on the Foundation of General Strain Theory: Specifying the Types of Strain Most Likely to Lead to Crime and Delinquency,” *Journal of Research in Crime and Delinquency*, vol. 38 no. 4, pp. 319–361.

Agnew, R. (2009), “General Strain Theory,” inKrohn,M.D.,Lizotte,A.J. and Hall,G.P. (Eds.),*Handbook on Crime and Deviance*, Springer, pp. 169–185.

Agnew, R. and White, H.R. (1992), “An Empirical Test of General Strain Theory,” *Criminology*, vol. 30 no. 4, pp. 475–500.

Anderson, R. and Moore, T. (2009), “Information security: where computer science, economics and psychology meet.,” *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, Vol. 367, pp. 2717–2727.

Bechtoldt, M.N., Welk, C., Zapf, D. and Hartig, J. (2007), “Main and moderating effects of self-control, organizational justice, and emotional labour on counterproductive behaviour at work,” *European Journal of Work and Organizational Psychology*, vol. 16 no. 4, pp. 479–500.

Boer, H., Seydel, E.R. and Norman, P. (1996), “Protection motivation theory,” (Conner,M. and Norman,P.,Eds.)*Predicting Health Behaviour: Research and Practice with Social Cognition Models*, Maidenhead, Open University Press, pp. 95–120.

Cohen-Charash, Y. and Spector, P.E. (2001), “The Role of Justice in Organizations: A Meta-Analysis,” *Organizational Behavior and Human Decision Processes*, vol. 86 no. 2, pp. 278–321.

Cropanzana, R., Bowen, D.E., Gilliland, S.W. and Bowen, E. (2007), “The Management of Organizational Justice,” *Academy of Management Perspectives*, vol. 21 no. 4, pp. 34–48.

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*, Elsevier Ltd, vol. 32, pp. 90–101.

Dang, D.P.T., Pittayachawan, S. and Nkhoma, M.Z. (2013), “Contextual Difference and Intention to Perform Information Security Behaviours: a Protection Motivation Approach,” *Australasian Conference on Information Systems (ACIS)*, Melbourne, Australia.

DeLisi, M. (2011), “How general is general strain theory?,” *Journal of Criminal Justice*, Elsevier Ltd, vol. 39 no. 1, pp. 1–2.

Francis, L. and Barling, J. (2005), “Organizational injustice and psychological strain.,” *Canadian Journal of Behavioural Science*, vol. 37 no. 4, pp. 250–261.

Greitzer, F., Kangas, L., Nooman, C. and Dalton, A. (2010), *Identifying at-Risk Employees: A Behavioral Model for Predicting Potential Insider Threats*, US.

Herath, T. and Rao, H.R. (2009), “Protection motivation and deterrence: a framework for security policy compliance in organisations,” *European Journal of Information Systems*, vol. 18 no. 2, pp. 106–125.

Herath, T. and Rao, H.R. (2009), “Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness,” *Decision Support Systems,* Elsevier B.V., vol. 47 no. 2, pp. 154–165.

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,* vol. 54 no. 6, p. 54.

Janz, N.K. and Becker, M.H. (1984), “The health belief model: a decade later,” *Health Education Quarterly,* vol. 11 no. 1, pp. 1–45.

Karyda, M., Kiountouzis, E., Kokolakis, S. and Theoharidou, M. (2005), “The insider threat to information systems and the effectiveness of ISO17799,” *Computers & Security,* vol. 24 no. 3, pp. 472–484.

Langton, L. and Piquero, N.L. (2007), “Can general strain theory explain white-collar crime? A preliminary investigation of the relationship between strain and select white-collar offenses,” *Journal of Criminal Justice,* vol. 35 no. 1, pp. 1–15.

Lee, D., Larose, R. and Rifon, N. (2008), “Keeping our network safe: a model of online protection behaviour,” *Behaviour & Information Technology,* vol. 27 no. 5, pp. 445–454.

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,* vol. 41 no. 6, pp. 707–718.

Liang, H. and Xue, Y. (2009), “Avoidance of information technology threats: a theoretical perspective,” *MIS Quarterly,* vol. 33 no. 1, pp. 71–90.

Liang, H. and Xue, Y. (2010), “Understanding security behaviors in personal computer usage: a threat avoidance perspective,” *Journal of the Association for Information Systems,* vol. 11 no. 7, pp. 394–413.

Lim, V.K.G. (2002), “The IT way of loafing on the job: cyberloafing, neutralizing and organizational justice,” *Journal of Organizational Behavior,* vol. 23, pp. 675–694.

Loch, K.D., Carr, H.H. and Warkentin, M.E. (1992), “Threats to information systems: today’s reality, yesterday's understanding,” *MIS Quarterly,* pp. 173–186.

Mohamed, N. and Ahmad, I.H. (2012), “Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia,” *Computers in Human Behavior,* Elsevier Ltd, vol. 28 no. 6, pp. 2366–2375.

Ng, B.-Y., Kankanhalli, A. and Xu, Y. (Calvin). (2009), “Studying users’ computer security behavior: A health belief perspective,” *Decision Support Systems,* Elsevier B.V., vol. 46 no. 4, pp. 815–825.

Posey, C., Bennett, R.J., Roberts, T.L. and Lowry, P.B. (2011), “When computer monitoring backfires: Invasion of privacy and organizational injustice as precursors to computer abuse,” *Journal of Information System Security,* vol. 7 no. 1, pp. 24–47.

Rogers, R.W. (1975), “A protection motivation theory of fear appeals and attitude change,” *Journal of Psychology,* no. 91, pp. 93–114.

Scheuerman, H.L. (2013), “The relationship between injustice and crime: A general strain theory approach,” *Journal of Criminal Justice,* Elsevier Ltd, vol. 41 no. 6, pp. 375–385.

Seppo, P., Siponen, M. and Mahmood, A. (2007), “Employees’ behavior towards IS security policy compliance,” *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on. IEEE,* p. 156b–156b.

Siponen, M., Pahnila, S. and Mahmood, A. (2007), “Employees’ adherence to information security policies: an empirical study,” *New Approaches for Security, Privacy and Trust in Complex Environments,* vol. 232, pp. 133–144.

Son, J.-Y. (2011), “Out of fear or desire? Toward a better understanding of employees’ motivation to follow IS security policies,” *Information & Management,* Elsevier B.V., vol. 48 no. 7, pp. 296–302.

Spector, P., Fox, S. and Domagalski, T. (2006), “Emotions, Violence, and Counterproductive Work Behavior,” *Handbook of workplace violence*, pp. 29–46. Retrieved from http://www.corwin.com/upm-data/8744_KellowayCh3.pdf

Stanton, J.M., Stam, K.R., Mastrangelo, P. and Jolton, J. (2005), “Analysis of end user security behaviors,” *Computers & Security*, vol. 24 no. 2, pp. 124–133.

Straub, D. and Welke, R. (1998), “Coping with systems risk: security planning models for management decision making,” *MIS Quarterly*, vol. 22 no. 4, pp. 441–469.

Thong, J.Y.. and Yap, C.-S. (2000), “Information systems and occupational stress: a theoretical framework,” *Omega*, vol. 28 no. 6, pp. 681–692.

Vance, A., Siponen, M. and Pahnila, S. (2012), “Motivating IS security compliance: Insights from Habit and Protection Motivation Theory,” *Information & Management*, vol. 49 no. 3–4, pp. 190–198.

Warkentin, M. and Willison, R. (2009), “Behavioral and policy issues in information systems security: the insider threat,” *European Journal of Information Systems*, vol. 18 no. 2, pp. 101–105.

Willison, R. (2009), “Motivations for Employee Computer Crime : Understanding and Addressing Workplace Disgruntlement through the Application of Organisational Justice,” no. 1, pp. 1–28.

Willison, R. and Warkentin, M. (2013), “Beyond Deterrence: An Expanded View of Employee Computer Abuse,” *MIS Quarterly*, vol. 37 no. 1, pp. 1–20.

Workman, M. (2007), “Gaining Access with Social Engineering: An Empirical Study of the Threat,” *Information Systems Security*, vol. 16 no. 6, pp. 315–331.

Yang, J. and Diefendorff, J.M. (2009), “The Relations of Daily Counterproductive Workplace Behavior With Emotions, Situational Antecedents, and Personality Moderators: A Diary Study in Hong Kong,” *Personnel Psychology*, vol. 62 no. 2, pp. 259–295.