doi: 10.1111/isj.12129

Examining employee computer abuse intentions: insights from justice, deterrence and neutralization perspectives

Robert Willison,* Merrill Warkentin[†]* & Allen C. Johnston[‡]

*Newcastle University Business School, Newcastle, UK, [†]Mississippi State University, Mississippi State, MS USA, and [‡]University of Alabama at Birmingham, Birmingham, AL USA

Abstract. *Although employee computer abuse is a costly and significant problem for firms, the existing academic literature regarding this issue is limited. To address this gap, we apply a multi-theoretical model to explain employees' intentions to abuse computers. To understand the motives for such behaviour, we investigate the role of two forms of organizational justice – distributive and procedural – both of which provide explanations of how perceptions of unfairness are created in the organizational context. By applying deterrence theory, we also examine the extent to which formal sanctions influence and moderate the intentions to abuse computers. Finally, we examine how the potential motives for abuse may be moderated by techniques of neutralization, which allow offenders to justify their actions and absolve themselves of any associated feelings of guilt and shame. Utilizing the scenario-based factorial survey method for our experimental design, we empirically evaluated the association between these antecedents and the behavioural intention to violate Information systems (IS) security policies in an environment where the measurement of actual behaviour would be impossible. Our findings suggest that individual employees may form intentions to commit computer abuse if they perceive the presence of procedural injustice and that techniques of neutralization and certainty of sanctions moderate this influence. The implications of these findings for research and practice are presented. © 2016 Blackwell Publishing Ltd*

Keywords: organizational justice, techniques of neutralization, employee computer abuse, insider threat, security policy violation, factorial survey method, scenario

INTRODUCTION

Information systems (IS) security practitioners are responsible for addressing a wide range of threats, including employee computer abuse (Stahl *et al.,* 2012). However, attempts to gather official crime statistics on this problem are hindered by organizational under-reporting, a practice commonly attributed to the fear of reputational damage. To this extent, industry security surveys have provided insights into the magnitude of this threat. For instance, recent results reported in The Global State of Information Security Survey 2015 revealed that employees remain the most-often cited perpetrators of security incidents and that their crimes tend to be costlier to their firms than those perpetrated by external sources (Coopers, 2015). This survey, which included 9700 IT and security executives from firms in more than 154 countries, determined that current employees, service providers and consultants were responsible for over 50% of reported incidents. At 34.55%, current employees were the worst offenders (www.pwc.com/gsiss, 2015). These findings support earlier reports from Ernst and Young's Global Information Security Survey 2014 in which the respondents reported that employees were responsible for 57% of the attacks against organizational digital assets, and 38% of those attacks were because of carelessness or unawareness (Ernst and Young LLP, Global Information Security Survey 2014, www.ey.com/GISS). Other industry reports confirmed these findings (Ponemon Institute, 2013). More recently, an industry study (Kaspersky, 2015) found that three-fourths of the surveyed companies had experienced internal information security incidents and that employees were the largest single cause (42%) of confidential data losses.

We define employee computer abuse in terms of 'the unauthorized and deliberate misuse of … [computers and other forms of information technology] of the local organization information systems by individuals' with *inside access* (Straub, 1990: 257). Although individuals with inside access can include contractors, consultants and others (Sharma & Warkentin, 2014; Warkentin & Willison, 2009), our focus is primarily on *employees*, specifically those who have formed negative perceptions of their employer's managerial treatment.

The phenomenon of employee computer abuse deserves attention, and there have been a number of recent calls for a greater research focus on this area (Crossler *et al.,* 2013; Posey *et al.,* 2013; Willison & Warkentin, 2013). Although recent additional studies indicate some progress (Choi *et al.,* 2013; Chatterjee *et al.,* 2015), the issue of employee computer abuse still represents an under-researched area in the IS security field. To contribute to this body of work, we provide a holistic understanding of employee computer abuse by establishing a multi-theoretical model that is designed to examine this problem. We then test it in a scientifically rigorous study. Specifically, the model is based on three theories that were selected and integrated based on insights gleaned from the existing research, including organizational justice theory, deterrence theory and techniques of neutralization. This framework allows for consideration of not only the factors that may motivate employee computer abuse *directly* but also the factors that could either *enhance* or *mitigate* the direct causal relationships. We argue that no single theory can provide a thorough and complete understanding of the focal phenomenon. For example, even though deterrence theory, which was derived in the discipline of criminology, has been widely applied in the IS security discipline, it is unable to offer any insight into what may motivate employees to commit computer abuse. Therefore, when applied toward this goal, deterrence theory is typically accompanied by a host of theories that attempt to add further explanation for the reasons that individuals engage in computer abuse. For these reasons, we advance a model that draws on multiple theories in an attempt to address this limitation.

To examine employees' motives for computer abuse behaviour, we apply organizational justice theory (Adams, 1965; Leventhal, 1980; Leventhal *et al.,* 1980), which explains how perceptions of fairness or unfairness are created in the organizational context. We assert that individuals who feel that their employer has been unfair are more likely to engage in computer abuse behaviour. However, through the application of deterrence theory, we also examine how formal sanctions can act as a brake on these motivations for abuse (Straub, 1990; Straub & Welke, 1998; D'Arcy *et al.,* 2009). We assert that perceived sanction certainty and severity would negatively moderate the impact of perceived organizational injustice on the intention to engage in computer abuse behaviour. Finally, we examine how these potential motives for employee computer abuse may also be influenced by techniques of neutralization (Siponen & Vance, 2010; Willison & Warkentin, 2013; Willison, 2006), which rely on processes of justification and rationalization. These techniques allow potential offenders to absolve themselves of the influences of internalized norms and social censure, leaving them free to offend without feelings of guilt and shame. We assert that employees' adoption of these techniques of neutralization will positively moderate the impact of perceived organizational injustice on the intention to engage in computer abuse behaviour. The examination of this relationship is based on previous neutralization research. These extant works indicate that without the presence of a *situational stimulus* (i.e. a motivational factor), there is no reason for an offender to evoke a neutralization technique when contemplating deviant behaviour. Consequently, we apply perceptions of injustice as our situational stimulus. In other words, when an employee feels that the employer has been unfair, he or she may pursue computer abuse actions, but this outcome may be affected by neutralization processes. Our findings show the role of perceived injustice in facilitating the formation of intentions to commit computer abuse actions. They also show the impact of techniques of neutralization on these intentions. We also show that sanctions can mitigate these relationships.

The remainder of this paper is organized as follows. In the next section, we present our theoretical footing (Warkentin *et al*., 2011), describe our research model and present our hypotheses. This is followed by the description of our research design and the data analysis. We then report the results in the next section, followed by a discussion of the findings and their implications for research and practice. The conclusion forms our final section of the paper.

THEORETICAL BACKGROUND

To assess the motives of employee computer abuse, our research draws on the body of theoretical work on organizational justice, and further theoretical insights gained from deterrence theory and neutralization theory.

Organizational justice

The organizational justice research examines how various organizational phenomena may lead to employees' perceptions of justice or injustice and interchangeably fairness or unfairness. Scholars have identified four dimensions of perceived organizational justice – distributive, procedural, informational and interactional – as well as their relationship to other factors, including the consequences of perceived injustice, namely employees' reactions to perceptions of injustice (or unfairness). Distributive justice concerns equality in the allocation of resources or rewards, such as raises or bonuses, whereas procedural justice concerns fairness in the processes that are used to determine or resolve disputes with the allocation of those resources or rewards (Colquitt *et al.,* 2001). Informational justice concerns the 'explanations provided to people that convey information about why procedures were used in a certain way or why outcomes were distributed in a certain fashion' (Colquitt *et al.,* 2001, p. 427), while interactional justice is the degree to which the individuals impacted by decisions are afforded their due dignity and respect (Bies & Moag, 1986).

In their meta-analytic review of 183 studies, Colquitt *et al.* (2001) identified 11 broad categories of outcomes, which included withdrawal, evaluation of authority and organizational commitment. They also evaluated 'negative reactions,' which encompassed extreme behaviours in the form of theft (Greenberg, 1990), retaliation (Skarlicki & Folger, 1997; Skarlicki *et al.,* 1999), revenge (Bies & Tripp, 1998), workplace violence (Greenberg & Barling, 1999) and sabotage (Giacolone *et al.,* 1997; Skarlicki & Folger, 1997; Ambrose *et al.,* 2002). These investigations of negative reactions induced by perceptions of organizational injustice informed our theoretical foundations. Because our focal phenomenon is computer abuse, previous investigations of negative outcomes of perceived organizational injustice (Colquitt *et al.,* 2001) have informed our theoretical approach, which features *distributive* and *procedural* injustice perceptions as the causes of employee disgruntlement, and *informational* and *interactional* injustice perceptions as temporary subsequent phenomena. For example, when an employee perceives he or she was not given a fair raise, information about the procedure is explained by managers in a process by which informational and interactional justice perceptions are subsequently formed. However, if the process used to determine the raise and its outcome were fair, then the employee is unlikely to become concerned about the way in which both the process and outcome were conveyed or the way in which he or she was treated throughout the process. Further, Sweeney & McFarlin's (1993) empirical study supported a two-dimension organizational justice construct that comprised distributive and procedural justice. Although researchers are in general agreement regarding the distinction between *procedural* and *distributive* justice, controversy surrounds the distinction between *interactional* and *procedural* justice (Cohen-Charash & Spector, 2001). We choose to avoid such debate because it would detract from our fundamental investigation, in which we focus on the two original primary perceptions of justice – distribute and procedural justice – and their impact on our focal phenomenon of computer abuse.

Perceptions of distributive justice constitute one potential influence on employees' computer abuse intentions. In his theory of equity, Adams (1965) suggested that individual employees will compare the ratio of their work output (rewards, e.g. salary) and inputs (contribution, e.g. execution of employment role and responsibilities) to the ratio of a comparative 'other' (e.g. a departmental colleague). For example, employee A may compare his outcomes-to-inputs ratio with employee B's ratio; when A finds that B has the same ratio (e.g. the same pay for the same performance as in a pure meritocracy), then A may perceive equity. However, if A found that his or her ratio differed from B's because the latter earned significantly more for the same level of performance, then A may perceive inequity or distributive injustice. Subsequent research applied distributive justice to the study of several behaviours, including stealing (Greenberg, 1993), retaliation (Skarlicki & Folger, 1997) and sabotage (Ambrose *et al.,* 2002). Ambrose *et al.* (2002) found that when the source of injustice was distributive in nature, then the employees who perceived the unfairness were more likely to engage in *equity restoration*, such as theft.

Distributive justice has also been applied to study a range of behaviours in the IS field. These studies have examined cyber-loafing (Lim, 2002), information security policy compliance (Li *et al.,* 2014) and employee computer monitoring (Posey *et al.,* 2011). Posey *et al.* (2011) evaluated the possible adverse effects of computer monitoring in the workplace. Rather than studying the extent to which this monitoring could deter or prevent internal computer abuse, the research examined whether such monitoring could, in fact, create perceptions of privacy infringement and provoke destructive behaviours. Drawing on organizational justice and reactance theories utilized to understand perceptions of privacy infringement, the authors applied two forms of organizational justice, distributive and procedural, in their analysis. Of some significance for our study, the research found that greater levels of procedural and distributive justice were direct precursors to destructive behaviour in the form of internal computer abuse.

Based on the findings of these studies, we anticipate that the perceptions of distributed organizational injustice will lead to positive intentions to commit computer abuse. Thus, we hypothesize the following:

> H1: Distributive organizational injustice perceptions are positively associated with behavioural intention to commit computer abuse.

The development of the justice literature occurred through focusing on the actual procedures used to determine how distributions occur (Colquitt *et al.,* 2001). Emerging from this research was the concept of procedural justice, which is broadly defined as the perceived fairness of the procedures used to determine outcomes. Leventhal and his colleagues were the first to consider procedural justice in the organizational domain (Leventhal, 1980; Leventhal *et al.,* 1980). They specifically evaluated the nature of procedures, how they were enacted and their implications for perceptions of justice and injustice. Through this work, Leventhal (1980) advanced six rules, which, if followed, would engender perceptions of procedural justice. Similarly, if employees perceived that these rules were not followed, then perceptions of procedural injustice would ensue. As Cohen-Charash and Spector (2001: 280) noted, these rules include the following:

> ‘a) the consistency rule, stating that allocation procedures should be consistent across persons and over time; b) the bias-suppression rule, stating that personal self-interests of decision-makers should be prevented from operating during the allocation process; c) the accuracy rule, referring to the goodness of the information used in the allocation process; d) the correctability rule, dealing with the existence of opportunities to change an unfair decision; e) the representativeness rule, stating that the needs, values, and outlooks of all the parties affected by the allocation process should be represented in the process; and f) the ethicality rule, according to which the allocation process must be compatible with fundamental moral and ethical values of the perceiver.’

Other studies examined the role of procedural justice in acts such as retaliation (Skarlicki & Folger, 1997; Skarlicki *et al.,* 1999) and aggression (Greenberg & Barling, 1999). Greenberg & Barling (1999) studied employee aggression against co-workers, subordinates and supervisors. Specifically, they assessed two groups of possible causal factors. One group – personal behaviours – included employees' history of aggression and the amount of alcohol consumed by employees. The other group – workplace factors – included job insecurity, procedural justice, workplace surveillance and distributive justice. The study individually assessed each group of factors and then the possible interactions between the workplace and personal behaviour items. The findings showed that aggression by an employee against a supervisor was significantly predicted by procedural injustice and workplace surveillance. In addition, the procedural justice and the amount of alcohol consumed interacted to predict aggression by an employee against a subordinate and a co-worker. Similar to its distributive counterpart, procedural justice has been applied in the IS field (Lim, 2002; Posey *et al.,* 2011; Li *et al.,* 2014) to investigate how perceptions of procedural injustice motivate negative behaviours.

We anticipate that perceptions of procedural organizational injustice will lead to positive intentions to commit computer abuse. Thus, we hypothesize the following:

H2: Procedural organizational injustice perceptions are positively associated with behavioural intention to commit computer abuse.

Deterrence

The issue of deterring employee computer abuse has been addressed by several studies on IS security. The issue has received the most attention in the area of employee computer abuse (Campbell, 1988; Hoffer & Straub, 1989; Straub, 1990; Straub & Nance, 1990; Cardinali, 1995; Sherizen, 1995; Harrington, 1996; Straub & Welke, 1998). Perhaps not surprisingly, several writers have applied deterrence theory to study this phenomenon (Hoffer & Straub, 1989; Straub, 1990; Straub *et al.,* 1992; Harrington, 1996; Straub & Welke, 1998). Central to this theory is the role played by sanctions (Cook, 1982) in terms of their certainty and severity as perceived by the offender. The theory postulates that if an offender perceives that the certainty and severity of the sanctions associated with a crime are high, then he or she will be deterred from engaging in a criminal act (Straub, 1990). Sanction celerity is also sometimes included with certainty and severity as a deterrence factor, however, in their comprehensive review and assessment of the state of deterrence theory as it applies to IS security policy violation intentions and behaviours, D'Arcy and Herath (2011: 645) reported that IS security studies have largely omitted the sanction celerity construct because of measurement difficulties and because of its 'lack of theoretical importance,' citing studies by Nagin & Pogarsky (2001) and Paternoster (2010). Because none of the IS deterrence studies they reviewed included sanction celerity, we chose to be consistent with this consensus in our scholarly community.

Following the seminal research by Straub (1990), other academics considered the influence of deterrence on employees' computer abuse intentions (Harrington, 1996; D'Arcy *et al.,* 2009). In their study of the effects of the perceived certainty and severity of organizational sanctions on

IS misuse intentions, D'Arcy *et al.* (2009) extended the prior research by examining how these perceptions were influenced by the user's awareness of three forms of security countermeasures: (1) user awareness of security policies, (2) security education, training and awareness, and (3) computer monitoring. These countermeasures were positively associated with perceived sanction certainty and severity. More recently, Hu *et al.* (2011) tested a model utilized to examine security policy violations, which viewed the offender as making a rational choice (cost/benefit) analysis when presented with an opportunity that involved a violation of information security policies. However, Hu et al. argued that this calculation is influenced by an individual's self-control, his or her moral beliefs, and the perceived deterrence. Based on a sample of employees in five large organizations in China, their findings showed that deterrence had no significant impact on the individual's intention to commit actions, contrary to the established information security policy.

Although deterrence theory is widely applied in the IS security field, only a handful of studies have examined sanctions as moderators of the relationships between negative actions and the motives for them (McCusker & Carnevale, 1995; Liu, 2003; Henle & Blanchard, 2008). In these studies, perceptions of sanctions mitigated the formation of negative social or workplace behaviours stemming from some kind of motivational source, thus negatively moderating the relationship between the motivation and the negative behaviour. Henle & Blanchard (2008) found that organizational sanctions reduced the impact of workplace stress on cyber-loafing, whereas Liu (2003) determined that sanctions served as *moderators* in the formation of criminal acts caused by deviant associations among peers. Although the context of the moderating role of sanctions was unique in each study, the general implications of their findings are aligned with our assumptions about the relationship of the role of sanctions and perceptions of injustice.

In addition, in prior studies on the IS context, there has been little consideration of the relationship between organizational justice and deterrence. Although we recognize that the factors that motivate employee computer abuse may be common to the organizational domain, (i.e. not IS specific), we also recognize there is a need to consider whether these factors are affected by contextually relevant influences, such as the formal sanctions considered in our study (Willison & Warkentin, 2013). Given these arguments, we assert that the influence of perceptions of injustice on the intention to commit employee computer abuse will be moderated by perceived sanctions. Hence, we hypothesize the following:

H3a: Perceived sanction severity negatively moderates the relationship between distributive organizational injustice perceptions and behavioural intention to commit computer abuse.

H3b: Perceived sanction severity negatively moderates the relationship between procedural organizational injustice perceptions and behavioural intention to commit computer abuse.

H4a: Perceived sanction certainty negatively moderates the relationship between distributive organizational injustice perceptions and behavioural intention to commit computer abuse.

H4b: Perceived sanction certainty negatively moderates the relationship between procedural organizational injustice perceptions and behavioural intention to commit computer abuse.

Techniques of neutralization

Deviant behaviour, including the violation of organizational information security policies, is characterized as comprising actions that the members of a social group judge to be a violation of their shared rules, values or accepted conduct. In contemplating such behaviours, most individuals will be dissuaded by feelings of guilt and shame. However, Sykes & Matza (1957) showed that offenders who might otherwise feel guilt and shame were able to neutralize these feelings by justifying their behaviours before committing the deviant act. These 'techniques of neutralization' are processes that serve to attenuate or deflect the disapproval they would otherwise experience from others in the social environment, thereby protecting the violator from feelings of self-blame and enabling him or her to engage in the deviant act. Sykes and Matza suggested that these processes enable the offender to negate the influence of internal norms and social censure. They identified five techniques, which include denial of responsibility, denial of injury, denial of the victim, condemnation of the condemners and the appeal to higher loyalties.[1] For example, with regard to the denial of responsibility in the context of juvenile delinquents, Sykes and Matza claimed that deviant acts are because of forces outside of the individual and beyond his control such as unloving parents, bad companions or living in a slum neighbourhood. In effect, the delinquent approaches a 'billiard ball' conception of himself in which he sees himself as helplessly propelled into new situations (Sykes & Matza, 1957: 667).

Other research has followed the lead of Sykes and Matza by identifying additional techniques of neutralization (Klockars, 1974; Minor, 1981; Coleman, 1994). For example, Minor (1981) advanced the technique of the defence of necessity, in which an offender attempts to justify his or her actions based on the perceived necessity to commit the deviant act. Hence, a shoplifter may claim his actions are warranted given the need to feed his children.

Although initially advanced as a theory of delinquency, the techniques of neutralization have been used as a theoretical lens for researching diverse forms of criminal behaviour, including tax evasion (Thurman *et al.,* 1984), domestic violence (Dutton, 1986), car theft (Copes, 2003) and drug abuse (Priest & McGrath, 1970). Given the nature of its focus, neutralization theory has also been applied in the IS field to study deviant behaviour in the context of IT use, such as cyber-loafing (Lim, 2002; Lim & Teo, 2005), digital piracy (Hinduja, 2007; Ingram & Hinduja, 2008; Morris & Higgins, 2009; Siponen *et al.,* 2012) and IS security policy violations (Harrington, 1996; Willison, 2002, 2006; Siponen & Vance, 2010).

[1]Researchers in the field of criminology (Clarke, 1997) and IS (Willison & Warkentin, 2013) have noted the similarities between the techniques of neutralization and the theory of moral disengagement proposed by Albert Bandura (1986, 1999, 2002). Specifically, Bandura identified eight mechanisms of moral disengagement, which individuals can use to justify their deviant or criminal behaviour. The theory of moral disengagement was recently applied by D'Arcy *et al.* (2014), who examined how the burden of security requirements could lead to security-related stress (SRS) by which individuals justify policy non-compliance through moral disengagement.

We investigate the use of three neutralization techniques: denial of injury, denial of the victim (Sykes & Matza, 1957), and the metaphor of the ledger (Klockars, 1974). Denial of injury focuses on whether any injury or harm occurs as the result of a criminal act. Hence, an offender may claim that he or she was just 'borrowing' the car they stole, or an embezzler may argue that the company he works for can afford the loss given the profits they make. Denial of the victim involves a situation in which the offender may recognize the harm caused by his actions but is able to justify the act based on his situation. Hence, a production-line worker may view his or her act of theft as a rightful form of retaliation for being overlooked for a promotion. Klockars (1974) first identified the technique known as the metaphor of the ledger to represent the situation in which an individual views past law-abiding behaviour as a *credit* and criminal behaviour as a *debit* in his 'behaviour ledger.' Consequently, the individual might justify a debit in his or her ledger as insignificant compared with the numerous credits 'stored' because of past good behaviour.

The reason that we selected these three forms of neutralization to utilize in our analysis is based on an argument that was first advanced by Sykes & Matza (1957: 670), who stated that 'certain techniques of neutralization would appear to be better suited to particular deviant acts than others.' This argument was confirmed in other research, which similarly noted that the offender's choice of a neutralization technique was a reflection of the type of crime (Benson, 1985; Maruna & Copes, 2005). For example, in his study of white-collar offenders, Benson (1985) noted that the metaphor of the ledger was unlikely to be used and accepted by offenders who committed serious street crime. However, given the nature of the technique, it is far more likely to be applied in the workplace context. Therefore, we selected denial of injury, denial of the victim and the metaphor of the ledger because previous research has indicated their use by employees in organizations (Hollinger, 1991; Lim, 2002; Piquero *et al.,* 2005).

We examined these three techniques in terms of their moderating influence on the relationship between perceptions of organizational injustice and the formation of behavioural intention to commit employee computer abuse. Although numerous studies have examined the neutralization process as a direct predictor of deviant behaviour, only a small effect size has been found (Ball, 1966; Hirschi, 1969; Hollinger, 1991; Thurman *et al*., 1984). It has been suggested that one reason for this finding is the elicitation of the techniques. Some studies have argued that a preceding *situational stimulus* must be present in order for an individual to employ a neutralization technique (Agnew & Peters, 1986; Agnew, 1994; Hinduja, 2007; Willison & Warkentin, 2013). Without the presence of a situational stimulus, there is no reason for an individual to adopt and apply a neutralization technique. For example, with regard to delinquency, Agnew (1994: 561) noted the following:

> … at a minimum, neutralization will not lead to delinquency unless adolescents also believe they are in a situation in which neutralizations are applicable. For example, adolescents who believe that fighting is justified in response to insult will not turn to fighting unless they also believe they have been insulted.

This argument is also consistent with later research (Lim, 2002), which found that when employees perceived that they had been treated unfairly, they might have evoked the metaphor of the ledger in response. Finally, the above argument is also consistent with the findings of research that techniques of neutralization would offer the greatest explanatory power when they were applied with other theories (Maruna & Copes, 2005; Ingram & Hinduja, 2008). Thus, we hypothesize the following:

H5a: Neutralization (via denial of injury) positively moderates the relationship between distributive organizational injustice perceptions and behavioural intention to commit computer abuse.

H5b: Neutralization (via denial of injury) positively moderates the relationship between procedural organizational injustice perceptions and behavioural intention to commit computer abuse.

H6a: Neutralization (via denial of the victim) positively moderates the relationship between distributive organizational injustice perceptions and behavioural intention to commit computer abuse.

H6b: Neutralization (via denial of the victim) positively moderates the relationship between procedural organizational injustice perceptions and behavioural intention to commit computer abuse.

H7a: Neutralization (via metaphor of the ledger) positively moderates the relationship between distributive organizational injustice perceptions and behavioural intention to commit computer abuse.

H7b: Neutralization (via metaphor of the ledger) positively moderates the relationship between procedural organizational injustice perceptions and behavioural intention to commit computer abuse.

Figure 1 illustrates the relationships among the injustice, deterrence and neutralization perspectives that we have hypothesized. We anticipate that perceptions of distributive and procedural injustice will directly influence the formation of employee computer abuse behavioural intentions, whereas perceived sanctions and techniques of neutralization will mitigate and exacerbate the formation of those intentions, respectively. In the following section, we describe the experimental research design used in the empirical assessment of this model.

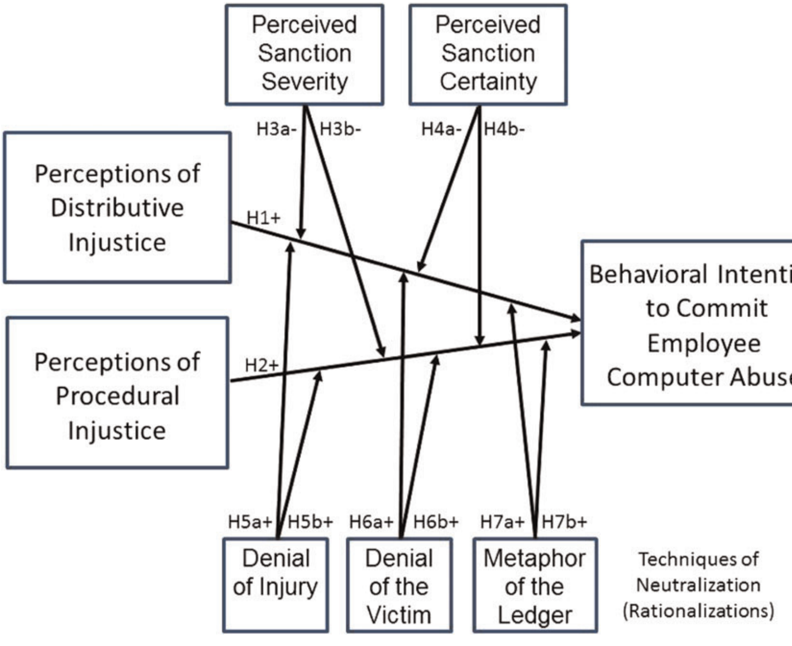

Figure 1. Research model.

RESEARCH DESIGN

To test our research model, we identified a valid and operationalizable experimental research design. A scenario-based factorial survey approach was chosen, in part because of its ability to elicit forthright responses from study participants who were under the duress of potential retribution from the disclosure of truth ('social desirability bias'), as well as because of its ability to reveal the structure of individual decision-making. A rich tradition of using scenario analysis in similar research was established in the criminology field, and it has been applied recently in IS research (c.f. Siponen & Vance, 2010 and Barlow *et al.,* 2013). By asking the respondents to read a scenario and imagine themselves in the context of the scenario's character, the researcher can establish a reliable and valid measure for behavioural intention as it relates to the various factors found in the scenario, even though the behaviour may be socially undesirable. This method was found to yield valid and truthful data because the respondents are not asked to admit to personal intentions but instead to place themselves in the position of the scenario's characters, whereby they are more likely to self-report their likelihood to commit a crime (Trevino & Victor, 1992).

The factorial survey method allows for variables of interest, in this case perceptions of injustice, deterrence and techniques of neutralization variables, to be manipulated within a scenario. These variables are referred to as dimensions, each of which has multiple levels. Each dimension and its corresponding levels are present in multiple scenario versions, producing a full representation of all possible combinations of the dimensions and their levels.

This full factorial design should guarantee that the levels are orthogonal and subsequently eliminate the possibility of the multi-collinearity that may exist between predictor variables (dimensions) in a model (Rossi & Anderson, 1982; Jasso, 2006; Vance *et al.,* 2015). However, because of the recommended practice among factorial survey experiments of removing unrealistic, contextually invalid or logically impossible scenarios from the full population of scenarios (Jasso, 2006), the chance of the multicollinearity among predictor variables (dimensions) in a model does not remain zero, but in all likelihood does remain quite small. This is the case for our study.

Sample

The data used in this study were collected from a sample of full-time working professionals in the U.S. An online surveying firm was solicited to aid in the collection of the data and provided access to the email addresses of over 3500 professionals screened to ensure that they were employees who were eligible for raises and used a computer in their line of work. To increase the generalizability of this study's results, the sample was selected to represent a large variety of interests and expertise, and all major industries and experience levels present in the reported sample. A total of 3532 persons were invited via email to participate in the study, and 968 persons ultimately provided complete and useful responses, a response rate of 27.4%. Of the respondents, 45% were male, approximately 30% were in the age range of 35 to 44 years and 44% reported 25 or more years of professional work experience.

Although there were 968 participants, the total number of observations was actually 3872 because each participant read and responded to four different scenarios. Although this approach was useful in generating a large number of observations from a small number of respondents, because there were repeated measurements from the same individual, we were required to account for within-respondent correlation errors in the subsequent regression modelling analyses.

Scenario design and instrumentation

Following the modified random design factorial survey approach advocated by Jasso & Rossi (1977) and Beck & Opp (2001), each participant was asked to read and respond to an online survey instrument that contained four randomly generated hypothetical scenarios. This approach was used to obtain multiple ratings per scenario, allowing for both respondent-specific and scenario-specific analyses. Each scenario described a situation in which an employee of a large financial institution contemplated the following: (1) a perceived act of distributive organizational injustice by the company, (2) a perceived act of procedural organizational injustice by the company, or (3) no act of organizational injustice and the reaction of stealing a supervisor's password in an effort to view all employee evaluations within the relevant department. Because they were embedded in the scenario versions, we also manipulated the employee's neutralization technique as follows: (1) no technique of neutralization, (2) denial of injury, (3) denial of victim, or (4) the metaphor of the ledger. As mentioned earlier, these neutralization techniques were selected because of their salience in the context of the organizational workplace (Benson, 1985; Maruna & Copes, 2005). Finally, each scenario included the manipulation of deterrence in the form of sanction certainty and sanction severity: sanction certainty was present in the form of either low or high certainty, and sanction severity was present in the form of either minimal or severe severity.

After reading each scenario, the respondents were asked to provide responses to a series of questions, including a three-item manipulation check, a realism check and a three-item measure of the dependent variable for a specific scenario. In our study, the dependent variable is the respondent's self-reported intention to perpetrate an act of employee computer abuse (password theft) as described in the scenario. After reading a scenario in which an employee steals a password and engages in information theft, the respondents were asked to estimate the likelihood that they would mirror the employee's actions under similar conditions. The response options ranged on a fully anchored scale from one to five, in which five served as 'strongly agree' with the statement that the respondent would engage in actions similar to those of the hypothetical employee in the scenario under circumstances that represented various levels of the antecedent variables. Following four such exercises (each with a different version of the scenario), each respondent also completed a set of demographic items. Example scenarios and the survey instrument are displayed in the Appendix.

Overall, the initial population of scenarios included 48 distinct cases. However, Piquero & Hickman (1999) and, recently, Siponen & Vance (2010, 2014), noted that scenarios must be designed to maintain realism and relevance for the potential respondents. To ensure a realistic scenario design, two controls were embedded in the study. First, as part of a pilot test prior to the survey, a seven-member panel of experts in research design and instrument development reviewed each scenario and validated the appropriate presence of each independent and control variable, as recommended by Straub *et al.* (2004). The panel also targeted unrealistic, contextually invalid or logically impossible scenarios for removal from the total universe of potential scenarios, ultimately reducing the final universe number of scenarios to 36.[2] Each scenario dimension, the levels under each dimension and its predicted effect on intentions to perpetrate computer abuse are shown in Table 1. Second, as mentioned previously, immediately following each scenario, the respondents were asked to gauge the realism of the scenario on a scale from 0 to 10, similar to Siponen & Vance (2010). This particular control is explored in detail in the following section.

Manipulation check and realism test

Following each scenario, the participants were presented with a three-item manipulation check and a single-item realism test. The items in the manipulation check were designed to ensure that the participants recognized the variability of the research factors embedded within each scenario, whereas the realism test was included to capture the degree, on a scale from 0 to 10, to which the participants believed the scenario to be realistic (Siponen & Vance, 2010). The results of this study were obtained from data collected only from the participants who were able to pass both manipulation checks and who scored five or higher on the realism check. If a

[2]An example of one unrealistic scenario that was removed from the total universe of scenarios was one that did not have either form of perceived injustice, but it still had Joe stealing his supervisor's password.

Table 1. Dimensions, levels and predicted effects

Dimension	Level	Predicted effect
Perceived Injustice	None	Reference Level
	Perceived Distributive Injustice	Positive Influence on Self-Reported Intentions to Commit Computer Abuse
	Perceived Procedural Injustice	Positive Influence on Self-Reported Intentions to Commit Computer Abuse
Perceived Sanction Severity	Low	Negative Moderating Influence on Relationship Between Perceived Injustice and Self-Reported Intentions to Commit Computer Abuse
	High	Negative Moderating Influence on Relationship Between Perceived Injustice and Self-Reported Intentions to Commit Computer Abuse
Perceived Sanction Certainty	Low	Negative Moderating Influence on Relationship Between Perceived Injustice and Self-Reported Intentions to Commit Computer Abuse
	High	Negative Moderating Influence on Relationship Between Perceived Injustice and Self-Reported Intentions to Commit Computer Abuse
Techniques of Neutralization	None	Reference Level
	Denial of Injury	Positive Moderating Influence on Relationship Between Perceived Injustice and Self-Reported Intentions to Commit Computer Abuse
	Denial of Victim	Positive Moderating Influence on Relationship Between Perceived Injustice and Self-Reported Intentions to Commit Computer Abuse
	Metaphor of the Ledger	Positive Moderating Influence on Relationship Between Perceived Injustice and Self-Reported Intentions to Commit Computer Abuse

participant missed a manipulation check answer or scored below five on the realism test, the subsequent responses of that participant for that particular scenario were omitted from the analysis, thereby increasing the overall rigor of our data collection procedures and improving our data quality. In fact, in the entire sample, the average score for realism was 6.76, which suggests that the scenarios were accepted by the participants as realistic in nature. Furthermore, the average reported intention to mirror the employee's actions and perpetrate computer abuse was 2 on a scale from 1 to 5; approximately 53% of the respondents reported the non-zero probability of perpetrating computer abuse.

DATA ANALYSIS AND RESULTS

For the model estimation, we used a generalized mixed linear model that accounted for both fixed and random effects (McLean *et al.,* 1991). This approach was appropriate because each participant was asked to assess multiple scenarios; thus, the observations were not independent, and unobserved differences in the participants could have introduced bias into the vignette assessments. However, by using a generalized mixed linear model, it is possible to control for this fixed individual effect (McLean *et al.,* 1991). Specifically, we used the general linear mixed model process in SPSS (version 19.0.0), which is analogous to the PROC MIXED procedure in SAS because it uses maximum likelihood estimates of variances, thereby accounting for correlations within the data caused by repeated measures. A typical least-squares analysis does not account for correlations within data that are caused by repeated measures, whereas this correlation is accounted for in the general linear mixed model that was utilized in the current study.

Control variables model tests

In addition to perceptions of procedural and distributive organizational injustice, we recognized that the behavioural intention to perpetrate computer abuse might also be influenced by the respondents' characteristics, such as age, gender and professional work experience. Consequently, we included these demographic controls in an initial control variables model that served as a baseline and established fit statistics that subsequent research models should improve in order to demonstrate the predictive power. We also included the three-item manipulation check and the single item realism test in this control variable model.

We also established a final control variable model by starting with the full set of control variables and removing those that were not significant determinants of intention to perpetrate an act of computer abuse. The removal of the non-significant control variables allowed us to arrive at a control variables model with optimal fit statistics. Among the full set of control variables, only age, experience and gender were significant and therefore included in the final model. Table 2 shows the final control variable model, which indicates an Akaike's Information Criterion (AIC) fit statistic of 9011.74 and a Schwarz's Bayesian Information Criterion (BIC) fit statistic of 9048.79. As shown in Table 2, in both AIC and BIC, a lower score indicates better model fit. Future research models should provide significantly lower AIC or BIC fit statistics, thereby indicating an improvement of the control variables model established in this study.

The examination of the control variables and their influence on computer abuse intentions revealed that the age, experience and gender of the participants influenced how they formulated their intentions of computer abuse. As the age and experience of the participants increased, their intentions to commit computer abuse decreased, which is consistent with the findings of previous studies in criminology. Gender is also an important factor in computer abuse intentions because male respondents are more likely than their female peers to form intentions to commit computer abuse.

Table 2. Control variable model

Effect	Estimate	Std. error	*T*-value
Intercept	2.534	0.081	31.462***
Age	−0.085	0.019	−4.596***
Experience	−0.067	0.030	−2.229***
Gender	−0.259	0.029	−8.803***
Fit statistics	AIC = 9011.74; BIC = 9048.79		

*$p < .05$;
**$p < 0.01$;
***$p < 0.001$.

Research model tests

Using the established control variable model, we then tested the direct effects of perceived organizational injustice on behavioural intentions to perpetrate computer abuse. As indicated in Table 3, the results of this test indicated that both perceived distributive injustice and perceived procedural injustice were sufficient to induce the intention to commit computer abuse among working professionals. None of the previously significant control variables was significant in this model. In this test, the AIC and BIC fit statistics were 8820.11 and 8869.53, respectively. Using a likelihood ratio test, we compared this model with the control variables model in terms of either AIC or BIC to determine if the difference in the fit statistics was significant. The likelihood ratio test yields a test statistic that is distributed as a chi-square distribution. For the AIC, we calculated a *p*-value as a measure of this statistic relative to its degrees of freedom (Littell *et al.,* 1996; Vance *et al.,* 2013) and determined that the fit scores were significantly improved ($p < 0.001$), thereby providing significantly better predictability than the control variable model did (Carte & Russell, 2003). These findings suggest that, in the absence of employer sanctions or techniques of neutralization, perceptions of procedural and distributive injustice are sufficient to form intentions to commit computer abuse.

To examine the moderating influence of perceived sanctions on the relationships between perceived injustice (distributive and procedural) and intention to commit computer abuse, we added the interaction effects to the direct influence model. The results, which are presented in Table 4, indicate the fit statistics of AIC = 8518.28 and BIC = 8585.57 in the moderating influence model. A likelihood ratio test of the relation of the moderating model's fit statistics to those of the direct influence model confirmed a significant improvement ($p < 0.001$) in the moderating effects model over the direct effects model. These results indicate that when the certainty of sanctions is high, employees are significantly less inclined to commit computer abuse when they perceive injustice. This finding suggests that high levels of sanction certainty moderate the impact of perceived injustice on intentions to commit computer abuse more effectively than low levels of sanction certainty do. The results also suggested that high levels of sanction severity are no more impactful on intentions to commit computer abuse formed from perceived injustice than low levels of sanction severity.

Table 3. Direct influence results: intention to commit computer abuse

	Direct influence model		
Dimension and level	Estimate	Std. error	*T*-value
Intercept	2.526	0.085	29.484**
Age	−0.057	0.038	−1.488
Experience	−0.063	0.062	−1.022
Gender	−0.301	0.167	−1.799
Perceived Distributive Injustice [1]	0.116	0.028	4.091**
Perceived Procedural Injustice [1]	0.144	0.044	3.309*
Observations	*N* = 3872		
Fit Statistics	AIC = 8820.11; BIC = 8869.53		

[1]Reference level: no injustice.
*$p \leq .05$;
**$p \leq .01$.

Table 4. Sanctioning moderating influence results: intention to commit computer abuse

	Direct influence model			Moderating influence model		
Dimension and level	Estimate	Std. error	*T*-value	Estimate	Std. error	*T*-value
Intercept	2.526	0.085	29.484**	2.350	0.123	19.073**
Age	−0.057	0.038	−1.488	−0.018	0.042	−0.437
Experience	−0.063	0.062	−1.022	−0.041	0.042	−0.988
Gender	−0.301	0.167	−1.799	−0.003	0.042	−0.078
Perceived Distributive Injustice [1]	0.116	0.028	4.091**	0.097	0.052	1.880
Perceived Procedural Injustice [1]	0.144	0.044	3.309*	0.086	0.042	2.039*
Sanction Severity [2] × Perceived Distributive Injustice				−0.305	0.179	−1.701
Sanction Severity [2] × Perceived Procedural Injustice				−0.057	0.039	−1.488
Sanction Certainty [3] × Perceived Distributive Injustice				−0.214	0.061	−3.517**
Sanction Certainty [3] × Perceived Procedural Injustice				−0.198	0.057	−3.482**
Observations	$N = 3872$			$N = 3872$		
Fit Statistics	AIC = 8820.11; BIC = 8869.53			AIC = 8518.28; BIC = 8585.57		

[1]Reference level: no injustice;
[2]Reference level: low sanction severity;
[3]Reference level: low sanction certainty;
*$p \le .05$;
**$p \le .01$.

Having introduced the moderating influence of techniques of neutralization on the relationships between perceived injustice (distributive and procedural) and intentions to commit computer abuse, we then added the interaction effects to the direct influence model. As shown in Table 5, the results indicated fit statistics of AIC = 8519.19 and BIC = 8574.18 in the second moderating influence model. A likelihood ratio test of the moderating model's fit statistics compared to those of the direct influence model confirmed a significant improvement ($p < 0.001$) in the moderating effects model over the direct effects model. These results indicate that techniques of neutralization might have a positive moderating effect on the influence of perceived procedural injustice on computer abuse intentions. In all three forms of neutralization investigated in this study – denial of injury, denial of victim and the metaphor of the ledger – each technique provided a significantly greater degree of positive moderating influence on the relationship between perceived procedural injustice and computer abuse intentions than when no neutralization technique was presented. The results also suggest that techniques of neutralization are unable to moderate the influence of perceived distributive injustice on computer abuse intentions.

The analysis of the moderating effects of both perceived sanctions and techniques of neutralization within the same model yielded fit statistics of AIC = 8622.50 and BIC = 8688.30 in the full moderating influence model. A likelihood ratio test of the moderating model's fit statistics compared to those of the direct influence model confirmed a significant improvement ($p < 0.001$) in the moderating effects model over the direct effects model. For presentation parsimony, only the significant moderating results of this test are provided in Table 6. As indicated, procedural injustice was a significant predictor of computer abuse intentions, and the interaction of sanction

Table 5. Techniques of neutralization moderating influence results: intention to commit computer abuse

	Direct influence model			Moderating influence model		
Dimension and level	Estimate	Std. error	*T*-value	Estimate	Std. error	*T*-value
Intercept	2.526	0.085	29.484**	2.503	0.097	25.597**
Age	−0.057	0.038	−1.488	−0.003	0.002	−1.274
Experience	−0.063	0.062	−1.022	−0.038	0.072	−0.523
Gender	−0.301	0.167	−1.799	−0.057	0.031	−1.844
Perceived Distributive Injustice [1]	0.116	0.028	4.091**	0.001	0.026	0.063
Perceived Procedural Injustice [1]	0.144	0.044	3.309*	0.009	0.189	0.493
Denial of Injury [2] × Perceived Distributive Injustice				0.005	0.005	1.189
Denial of Injury [2] × Perceived Procedural Injustice				0.111	0.041	2.727*
Denial of Victim [2] × Perceived Distributive Injustice				0.054	0.059	0.915
Denial of Victim [2] × Perceived Procedural Injustice				0.325	0.029	11.358*
Metaphor of the Ledger [2] × Perceived Distributive Injustice				0.012	0.011	1.131
Metaphor of the Ledger [2] × Perceived Procedural Injustice				0.101	0.006	15.876**
Observations	$N = 3872$			$N = 3872$		
Fit Statistics	AIC = 8820.11; BIC = 8869.53			AIC = 8519.19; BIC = 8574.18		

[1]Reference level: no injustice;
[2]Reference level: no neutralization technique;
*$p \leq .05$;
**$p \leq .05$.

Table 6. Combined sanctioning and techniques of neutralization moderating influence results: intention to commit computer abuse

	Direct influence model			Moderating influence model		
Dimension and level	Estimate	Std. error	*T*-value	Estimate	Std. error	*T*-value
Intercept	2.526	0.085	29.484**	2.538	0.088	28.820**
Age	−0.057	0.038	−1.488	−0.037	0.038	−0.988
Experience	−0.063	0.062	−1.022	−0.005	0.007	−0.734
Gender	−0.301	0.167	−1.799	−0.032	0.017	−1.875
Perceived Distributive Injustice [1]	0.116	0.028	4.091**	0.116	0.065	1.792
Perceived Procedural Injustice [1]	0.144	0.044	3.309*	0.150	0.065	2.312*
Sanction Certainty [2] x Perceived Procedural Injustice				−0.175	0.059	−2.938**
Denial of Victim [3] × Perceived Procedural Injustice				0.116	0.043	2.726**
Metaphor of the Ledger [3] × Perceived Procedural Injustice				0.162	0.051	3.157**
Observations	$N = 3872$			$N = 3872$		
Fit Statistics	AIC = 8820.11; BIC = 8869.53			AIC = 8622.50; BIC = 8688.30		

[1]Reference level: no injustice;
[2]Reference level: low sanction certainty;
[3]Reference level: no neutralization technique;
*$p \leq .05$;
**$p \leq .01$.

certainty with procedural injustice was significantly negative in its effects on computer abuse intentions. These findings support H2 and H4b, suggesting that as the individual perceives procedural injustice, the certainty of receiving sanctions for any computer abuse actions effectively deters those intentions. Of the interactions of perceived procedural injustice with techniques of neutralization, only the interactions of the denial of victim and the metaphor of the ledger and procedural injustice were significant. This finding supports H6b and H7b, suggesting that when employees perceive the procedures as unfair, then computer abuse actions are justified because they are 'payback' for previous good behaviour or because there is no real victim. Such perceptions strengthen the intentions of retaliatory computer abuse. Table 7 provides a summary of each hypothesis in this study and whether or not it was supported.

To understand the size of these effects, we assessed the coefficients for each of the embedded scenario variables following Vance *et al.* (2015). Because the embedded variables were measured as dummy variables (0 for not present; 1 for present), the coefficients of the variables (direct and moderating) shown in Table 6 represent the average increase in intentions to commit computer abuse. For instance, perceived distributive injustice increased the intention to commit computer abuse by .116, whereas the interaction of sanction certainty and perceived procedural injustice decreased intention to commit computer abuse by .175. Because the intention to

Table 7. Summary of hypothesis support

Hypothesis	Supported[1]
H1: Distributive organizational injustice perceptions are positively associated with behavioural intention to commit computer abuse.	No
H2: Procedural organizational injustice perceptions are positively associated with behavioural intention to commit computer abuse.	Yes
H3a: Perceived sanction severity negatively moderates the relationship between distributive organizational injustice perceptions and behavioural intention to commit computer abuse.	No
H3b: Perceived sanction severity negatively moderates the relationship between procedural organizational injustice perceptions and behavioural intention to commit computer abuse.	No
H4a: Perceived sanction certainty negatively moderates the relationship between distributive organizational injustice perceptions and behavioural intention to commit computer abuse.	No
H4b: Perceived sanction certainty negatively moderates the relationship between procedural organizational injustice perceptions and behavioural intention to commit computer abuse.	Yes
H5a: Neutralization (via denial of injury) positively moderates the relationship between distributive organizational injustice perceptions and behavioural intention to commit computer abuse.	No
H5b: Neutralization (via denial of injury) positively moderates the relationship between procedural organizational injustice perceptions and behavioural intention to commit computer abuse.	No
H6a: Neutralization (via denial of the victim) positively moderates the relationship between distributive organizational injustice perceptions and behavioural intention to commit computer abuse.	No
H6b: Neutralization (via denial of the victim) positively moderates the relationship between procedural organizational injustice perceptions and behavioural intention to commit computer abuse.	Yes
H7a: Neutralization (via metaphor of the ledger) positively moderates the relationship between distributive organizational injustice perceptions and behavioural intention to commit computer abuse.	No
H7b: Neutralization (via metaphor of the ledger) positively moderates the relationship between procedural organizational injustice perceptions and behavioural intention to commit computer abuse.	Yes

[1]Hypotheses H1 and H4a were initially supported in earlier tests of the direct effects of perceived organizational injustice on behavioural intentions to perpetrate computer abuse and of the moderating influence of perceived sanctions on the relationships between perceived injustice (distributive and procedural) and intention to commit computer abuse, respectively. The results of these tests are presented in Table 3 for H1 and Table 4 for H4a.

commit computer abuse variable had a range of 12 (3–15), the combined effect of all direct and moderating factors resulted in a 5.8% change in abuse intentions, which was small, yet significant effect.

DISCUSSION

Our study sought to understand how employees' perceptions of injustice motivate purposeful computer abuse violation intentions and how the formation of these abuse intentions is influenced by employer sanctions and by employee techniques of neutralization. The results of our study provided several important findings. First, in accounting for the moderating influence of sanctions and techniques of neutralization, only procedural injustice was significant in directly shaping computer abuse intentions. This new empirical finding is an important contribution to the literature. Our study is the first to detect this level of granularity and apply a research design that permitted the analysis of the effects of interaction among perceived organizational injustice, deterrence, and techniques of neutralization. This finding suggests that the motivation to commit an act of computer abuse is less influenced by the unfair distribution of workplace rewards than by the high-level unfair workplace evaluation procedures. In other words, when employees feel the process is not fair, they are more upset than when they are not compensated fairly. This interesting finding could be explained by the temporal relationship between the process and the subsequent outcome of the process. Perhaps employees perceive the root cause of distributive injustice to be unjust processes and, as a result, focus on procedural injustice as the reason for their computer abuse intentions. Future research is needed to attend to this possibility, isolating the organizational processes as antecedents of distributive injustice to determine if perceptions injustice in organizational processes undermine any fairness that might be attributed to the distribution of rewards and/or resources.

Second, our findings suggest that sanction certainty is effective in reducing the likelihood of employees forming computer abuse intentions in light of perceived procedural injustice. Interestingly, sanction severity was not significant in a similar moderating capacity, an outcome that is generally in tune with the once dominant, still lingering, perspective of deterrence researchers that sanction certainty is a far more effective deterrent than sanction severity is (Pogarsky, 2002). Perhaps employees are well aware of the severity of computer abuse sanctions, so the only variance in their responses to sanctions is determined by their belief in whether the sanctions will be administered or not. It is also possible that sanctions on employee computer abuse are more complex than they are conceptualized in this study and that a more detailed view of the formal or informal nature of sanctions is warranted. Nevertheless, our study is the first to examine the moderating influence of perceived sanctions on employee computer abuse intentions arising from injustice perceptions. The findings of this study contribute to the relatively sparse discussion of the moderating role of sanctions in the formation of deviant behavioural intentions in general. Future research is needed to continue to develop our understanding of how sanctions can influence employee computer abuse intentions and behaviours, perhaps differentiating between formal sanctions and informal sanctions within this context.

Third, as mentioned earlier, our findings indicate that distributive injustice is not a significant motivator in forming computer abuse intentions when faced with the possibility of sanctions in light of the potential to rationalize the abuse through techniques of neutralization. However, our findings indicate that techniques of neutralization increase the likelihood of employees forming computer abuse intentions only when they perceive procedural injustice not distributive injustice. Simply put, in considering the factors that exacerbate an employee's intentions to do harm, we must consider the motivating factors. Previous research has shown that if people believe procedures to be fair, they are more willing to accept negative outcomes (Maiese, 2003). Using this logic, if the procedures are perceived as unjust, individuals will not accept negative outcomes, and they will rationalize any negative actions, such as computer abuse, through techniques of neutralization. In our model, distributive injustice was found to be a non-significant determinant of computer abuse intentions, so it is possible that employees simply do not perceive this type of injustice to be influential enough to precipitate computer abuse intentions and the subsequent justification of such abuse. Because this study is the first of its kind to examine organizational injustice in concert with techniques of neutralization and sanctions, these findings should be tempered by the possibility that they are contextually specific. Future research is needed if we are to better understand the true nature of context in this regard.

Nevertheless, the findings of the present study promote the understanding of perceptions of injustice in the focal context. Rather than simply arguing that perceptions of injustice can lead to employee computer abuse, the findings of this study indicate that such perceptions are mitigated or reinforced through the influence of deterrents or neutralization, respectively. Previous research showed that a preceding situational stimulus must be present in order for an individual to employ a neutralization technique (Agnew & Peters, 1986; Agnew, 1994; Hinduja, 2007; Willison & Warkentin, 2013). Our study evaluated the role of the perceptions of procedural injustice as the situational stimulus, showing that neutralization techniques were influential moderators in this context.

Our findings have implications for practice. Managers should understand the relationships between employee review structures and how employees' perceptions of organizational injustice. Only by understanding how employees develop such perceptions and subsequently translate them into harmful actions can managers define strategies for mitigation. The factors that can increase or reduce this direct effect, namely neutralization and sanctions, should be leveraged by managers when perceptions of injustice are present. Barlow *et al.* (2013) showed that managerial messages that explicitly warn employees not to rationalize their security policy violations could be effective. Our findings further suggest that managers should pay particular attention to the transparency and communication associated with review structures that are designed to assist employees in understanding their accordance with the expectations of management and with their peers. Managerial communication, including security awareness training, should be designed to deter employees' use of neutralization techniques that serve to stimulate thoughts of employee retaliation against unjust actions. Of course, minimization of the distal antecedent (far 'left of bang'), namely organizational actions that lead to employee perceptions of injustice, are the most effective means of reducing insider abuse (Willison & Warkentin, 2010).

Support for our application and integration of three theoretical lenses confirms the complexity of the research phenomenon, which evidences that a single theory cannot explain the formation of employees' computer abuse intentions. As an initial basis for theoretical integration, our research model is parsimonious in nature because of the limitations of a single study. However, when considering theoretical integration, research in the IS security field should be informed by the relevant research in related disciplines. Our findings provide the foundation for further investigations that aim to integrate multiple theoretical perspectives on insider computer abuse.

Limitations

The present study has the following limitations, which it shares with other studies of computer abuse, deterrence, organizational injustice and neutralization, and with studies that utilize factorial survey analysis. Many behavioural security research studies are limited by their use of intention instead of actual behaviour as the dependent variable. How intention translates to actual behaviour is not completely clear, but the limited focus on intention is consistent with the majority of information security and criminology studies, in which intention is viewed as indicative of a precondition to a behavioural act (Paternoster & Simpson, 1996). For instance, in the information security literature, numerous studies position intention as the outcome variable of choice, including Anderson & Agarwal (2010); Bulgurcu *et al.* (2010); Johnston & Warkentin (2010); Siponen & Vance (2010); Johnston *et al.* (2015), among many others.

A second limitation of this study is also shared by Siponen & Vance (2010), and could be seen as a consequence of using a scenario-based research design. As Siponen & Vance (2010) explained, the participants in a study involving scenarios of policy or computer abuse violations may have already been involved in similar experiences and may feel compelled to adopt neutralization techniques to preserve their self-image rather than to justify the actions of the scenario characters. This confounding factor cannot be rigorously controlled in a scientific study that uses objective data (self-reported compliance or violation would not be reliable in this context), and no known research design could specifically account for this possibility. Siponen & Vance (2010) suggested that the expected number of previous computer abuse violators in their sample pool was likely insufficient to skew the results of their study. Because of the large sample size used in the present study, it is reasonable to infer the same expectation.

The third limitation concerns the cross-sectional design of this study. Because the factorial survey design is cross-sectional, it did not allow us to account for the temporal effects of drift or to infer causality in our model. Drift refers to a 'temporary period of irresponsibility or an episodic relief from moral constraint' (Maruna & Copes, 2005: 231), which could influence intentions to commit computer abuse. Siponen & Vance (2010) also reported the limitation of utilizing the factorial survey design. Both limitations could be overcome by utilizing a longitudinal design, which should be considered in future research.

Although data were collected from individual decision makers in individual scenario evaluations, we did not account for individual differences, which have been shown to exert a significant influence on an employee's computer security actions (Johnston *et al.,* 2016). Future research might control for many other individual-level factors, such as dispositional differences in the way that individuals perceive sanctions, threats and responses, as well as key differences in the way that security policy compliance messages are received and processed by individuals (Johnston *et al.,* 2015; Warkentin *et al.,* 2016).

CONCLUSION

The intentional abuse of computer systems by employees remains a serious problem for firms, their leadership and IT practitioners, which has lead scholars to focus on organizational information security. If practitioners and researchers could gain insights into how the relationship between organizations and their employees could lead to negative consequences, especially in the context of perceived injustice among employees, progress could be achieved in reducing the costly and disruptive computer abuse events that have been documented and are of considerable concern among managers. Our study provides such insights by demonstrating the direct influence that perceived injustice among employees exerts on their intentions to commit computer abuse and the role that techniques of neutralization and deterrence (through formal sanctions) have in moderating these intentions. Our theoretical and empirical contributions also include the introduction and integration of theories related to organizational justice perceptions, techniques of neutralization and deterrence as explanatory factors in the formation of motivations for employees' computer abuse intentions. Although further work is needed to understand the source of abusive activities and the factors that support or impede such behaviours, the results of our study provide important new knowledge to the prevailing discussion.

REFERENCES

Adams, J. (1965) Inequity in social exchange, In: Advances in Experimental Social Psychology, Berkowitz, L. (ed) vol. 2, pp. 267–299. Academic Press, New York.

Agnew, R. (1994) The techniques of neutralization and violence. *Criminology*, **32**, 555–580.

Agnew, R. & Peters, A.A.R. (1986) The techniques of neutralization: an analysis of predisposing and situational factors. *Criminal Justice and Behavior*, **13**, 81–97.

Ambrose, M., Seabright, M. & Schminke, M. (2002) Sabotage in the workplace: the role of organizational justice. *Organizational Behavior and Human Decision Processes*, **89**, 947–965.

Anderson, C.L. & Agarwal, R. (2010) Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, **34**, 613–643.

Ball, R. (1966) An empirical exploration of neutralization theory. *Criminologica*, **4**, 22–32.

Bandura, A. (1986) Social Foundations of Thought and Action: A Social Cognitive Theory. Prentice-Hall, Englewood Cliffs, NJ.

Bandura, A. (1999) Moral disengagement in the perception of inhumanities. *Personality and Social Psychology Review*, **3**, 193–209.

Bandura, A. (2002) Selective moral disengagement in the exercise of moral agency. *Journal of Moral Education*, **31**, 101–119.

Barlow, J.B., Warkentin, M., Ormond, D. & Dennis, A.R. (2013) Don't make excuses! Discouraging neutralization to reduce IT policy violation. *Computers & Security*, **39**, 145–159.

Beck, M. & Opp, K.D. (2001) The factorial survey and the measurement of norms. *Cologne Journal of Sociology and Social Psychology*, **53**, 283–306.

Benson, M. (1985) Denying the guilty mind: accounting for involvement in a white-collar crime. *Criminology*, **23**, 583–607.

Bies, R. & Moag, J.S. (1986) Interactional justice: communication criteria of fairness. *Research on Negotiation in Organizations*, **1**, 43–55.

Bies, R. & Tripp, T. (1998) Revenge in organizations: the good, the bad and the ugly, In: Dysfunctional Behavior in Organizations, Part B: Non-Violent Dysfunctional Behavior, Griffin, R., O'Leary-Kelly, A. & Collins, J. (eds), pp. 49–68. JAI Press, Stamford.

Bulgurcu, B., Cavusoglu, H. & Benbasat, I. (2010) Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, B.*, **34**, 523–548.

Campbell, M. (1988) Ethics and computer security: Cause and effect. Proceedings of the 1988 ACM Sixteenth Annual Conference on Computer Science, Atlanta, Georgia.

Cardinali, R. (1995) Reinforcing our moral vision: examining the relationship between unethical behaviour and computer crime. *Work Study*, **44**, 11–17.

Carte, T.A. & Russell, C.J. (2003) In pursuit of moderation: nine common errors and their solutions. *MIS Quarterly*, **27**, 479–501.

Chatterjee, S., Sarker, S. & Valacich, J. (2015) The behavioral roots of information systems security: exploring key factors related to unethical IT use. *Journal of Management Information Systems*, **31**, 49–87.

Choi, M., Levy, Y., Hovav, A. (2013) The role of user computer self-efficacy, cybersecurity countermeasures awareness, and cybersecurity skills influence on computer misuse. Workshop on Information Security and Privacy (WISP), Milan, Italy, December 14.

Clarke, R. (Ed) (1997) Situational Crime Prevention: Successful Case Studies, *2nd ed.* Albany, NY. Harrow and Heston.

Cohen-Charash, Y. & Spector, P. (2001) The role of justice in organizations: a meta-analysis. *Organizational Behavior and Human Decision Processes*, **86**, 278–321.

Coleman, J. (1994) The Criminal Elite: The Sociology of White-Collar Crime. St. Martins, New York.

Colquitt, J., Conlon, D., Wesson, M.J., Porter, C. & Ng, K. (2001) Justice at the millennium: a meta-analytic review of 25 years of organizational justice research. *Journal of Applied Psychology*, **86**, 425–445.

Cook, P. (1982) Research in criminal deterrence: laying the groundwork, In: Crime and Justice: A Review of Research, Morris, N. & Tonry, M. (eds) vol. 2, **211** pp. –268. The University of Chicago Press, Chicago.

Coopers, P. W. (2015) The Global State of Information Security Survey 2015.

Copes, H. (2003) Streetlife and the rewards of auto theft. *Deviant Behavior*, **24**, 309–332.

Crossler, R., Johnston, A., Lowry, P., Hu, Q., Warkentin, M. & Baskerville, R. (2013) Future directions for behavioral information security research. *Computers & Security*, **32**, 90–101.

D'Arcy, J. & 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**, 643–658.

D'Arcy, J., Herath, T. & Shoss, M. (2014) Understanding employee relations to stressful information security requirement: a coping perspective. *Journal of Management Information Systems*, **31**, 285–318.

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

Dutton, D.G. (1986) Wife assaulter's explanations for assault: the neutralization of self-punishment. *Canadian Journal of Behavioural Science/Revue canadienne des sciences du comportement*, **18**, 381–390.

Giacolone, R., Riordan, C. & Rosenfeld, P. (1997) Employee sabotage: toward a practitioner-scholar understanding, In: Antisocial Behavior in Organizations, Robert, A. & Greenberg, J. (eds), pp. 109–229. Sage, Thousand Oaks.

Greenberg, J. (1990) Employee theft as a reaction to underpayment inequity: the hidden cost of pay cuts. *Journal of Applied Psychology*, **54**, 81–103.

Greenberg, J. (1993) Stealing in the name of justice: informational and interpersonal moderators of theft to underpayment inequity. *Organizational Behavior and Human Decision Processes*, **54**, 81–103.

Greenberg, L. & Barling, J. (1999) Predicting employee aggression against coworkers, subordinates and supervisors: the roles of person behaviors and perceived workplace factors. *Journal of Organizational Behavior*, **20**, 897–913.

Harrington, S. (1996) The effects of ethics and personal denial of responsibility on computer abuse judgements and intentions. *MIS Quarterly*, **20**, 257–277.

Henle, C.A. & Blanchard, A.L. (2008) The interaction of work stressors and organizational sanctions on cyberloafing. *Journal of Managerial Issues*, **20**, 383–400.

Hinduja, S. (2007) Neutralization theory and online software piracy: an empirical analysis. *Ethics and Information Technology*, **9**, 187–204.

Hirschi, T. (1969) Causes of Delinquency. University of California Press, Berkley.

Hoffer, J. & Straub, D. (1989) The 9 to 5 underground: are you policing computer crimes? *Sloan Management Review*, **30**, 35–43.

Hollinger, R.C. (1991) Neutralizing in the workplace: an empirical analysis of property theft and production deviance. *Deviant Behavior*, **12**, 169–202.

Hu, Q., Xu, Z., Dinev, T. & Ling, H. (2011) Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM*, **54**, 54–60.

Ingram, J. & Hinduja, S. (2008) Neutralizing music piracy: an empirical examination. *Deviant Behavior*, **24**, 334–366.

Jasso, G. (2006) Factorial survey methods for studying beliefs and judgments. *Sociological Methods & Research*, **34**, 334–423.

Jasso, G. & Rossi, P.H. (1977) Distributive justice and earned income. *American Sociological Review*, **42**, 639–651.

Johnston, A.C. & Warkentin, M. (2010) Fear appeals and information security behaviors: an empirical study. *MIS Quarterly*, **34**, 549–566.

Johnston, A.C., Warkentin, M., McBride, M. & Carter, L.D. (2016) Dispositional and situational factors: influences on IS security policy violations. *European Journal of Information Systems*, **25**, 231–251.

Johnston, A.C., Warkentin, M. & Siponen, M. (2015) An enhanced fear appeal framework: leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly*, **39**, 113–134.

Kaspersky (2015) The threat within: 3 out of 4 companies affected by internal information security incidents. Available at http://usa.kaspersky.com/about-us/press-center/press-releases/2015/threat-within-3-out-4-companies-affected-internal-information-s

Klockars, C. (1974) The Professional Fence. Free Press, New York.

Leventhal, G. (1980) What should be done with equity theory? In: Social Exchange: Advances in Theory and Research, Gergen, K., Greenberg, M. & Willis, R. (eds), pp. 27–55. Plenum, New York.

Leventhal, G., Karuza, J. & Fry, W. (1980) Beyond fairness; a theory of allocation preferences, In: Justice and Social Interaction, Mikula, G. (ed), pp. 167–218. Springer-Verlag, New York.

Li, H., Sarathy, R., Zhang, J. & Luo, R. (2014) Exploring the effects of organizational justice, personal ethics and sanction on internet use policy compliance. *Information Systems Journal*, **24**, 479–502.

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

Lim, V. & Teo, T. (2005) Prevalence, perceived seriousness, justification and regulation of cyberloafing in Singapore: an exploratory study. *Information & Management*, **42**, 1081–1093.

Littell, R.C., Milliken, G.A., Stroup, W.W. & Wolfinger, R.D. (1996) SAS System for Mixed Models. SAS Institute, Inc., Cary, NC.

Liu, R.X. (2003) The moderating effects of internal and perceived external sanction threats on the relationship between deviant peer associations and criminal offending. *Western Criminology Review*, **4**, 191–202.

Maiese, M. (2003) Types of justice. In: Beyond Intractability, Burgess, G and Burgess, H. (eds.). Conflict Information Consortium, University of Colorado, Boulder. Posted: July 2003 http://www.beyondintractability.org/essay/types-of-justice.

Maruna, S. & Copes, H. (2005) What have we learned from five decades of neutralization research? In: Crime and Justice: A Review of Research, Tonry, M. (ed), vol. 32, pp. 221–320. The University of Chicago Press, Chicago.

McCusker, C. & Carnevale, P.J. (1995) Framing in resource dilemmas: loss aversion and the moderating effects of sanctions. *Organizational Behavior and Human Decision Processes*, **61**, 190–201.

McLean, R.A., Sanders, W.L. & Stroup, W.W. (1991) A unified approach to mixed linear models. *The American Statistician*, **45**, 54–64.

Minor, W. (1981) Techniques of neutralization: a reconceptualization and empirical examination. *Journal of Research in Crime and Delinquency*, **18**, 295–318.

Morris, R. & Higgins, G. (2009) Neutralizing potential and self-reported digital piracy: a multi-theoretical exploration among college undergraduates. *Criminal Justice Review*, **34**, 173–195.

Nagin, D.S. & Pogarsky, G. (2001) Integrating celerity, impulsivity, and extralegal sanction threats into a model of general deterrence: theory and evidence. *Criminology*, **39**, 865–891.

Paternoster, R. (2010) How much do we really know about criminal deterrence? *The Journal of Criminal Law and Criminology*, **100**, 765–823.

Paternoster, R. & Simpson, S. (1996) Sanction threats and appeals to morality: testing a rational choice model of corporate crime. *Journal of the Law and Society Association*, **30**, 549–583.

Piquero, A.R. & Hickman, M. (1999) An empirical test of Tittle's control balance theory. *Criminology*, **37**, 319–342.

Piquero, N.L., Tibbetts, S.G. & Blankenship, M.B. (2005) Examining the role of differential association and techniques of neutralization in explaining corporate crime. *Deviant Behavior*, **26**, 159–188.

Ponemon Institute (2013). 2014 State of Endpoint Risk. Available at http://www.lumension.com/Lumension/media/graphics/Resources/2014-state-of-the-endpoint/2014-State-of-the-Endpoint-Whitepaper-Lumension.pdf

Pogarsky, G. (2002) Identifying "deterrable" offenders: implications for research on deterrence. *Justice Quarterly*, **19**, 431–452.

Posey, C., Bennett, B., Roberts, T. & Lowry, P.B. (2011) When computer monitoring backfires: invasion of privacy and organizational injustice as precursors to computer abuse. *Journal of Information System Security*, **7**, 24–47.

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

Priest, T.B. & McGrath, J.H. (1970) Techniques of neutralization: young adult marijuana smokers. *Criminology*, **8**, 185–194.

Rossi, P.H. & Anderson, A.B. (1982) The factorial survey approach: an introduction, In: Measuring Social Judgments: The Factorial Survey Approach, Rossi, P.H. & Nock, S.L. (eds), pp. 15–67. Sage, Beverly Hills.

Sharma, S., and Warkentin, M. (2014) Exploring the role of the temporary workforce on information security policy compliance. Proceedings of the 9th Annual Symposium on Information Assurance, Albany, New York.

Sherizen, S. (1995) Can computer crime be deterred? *Security Journal*, **6**, 177–181.

Siponen, M. & Vance, A. (2010) Neutralization: new insights into the problem of employee information systems security policy violations. *MIS Quarterly*, **34**, 487–502.

Siponen, M. & 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**, 289–305.

Siponen, M., Vance, A. & Willison, R. (2012) New insights into the problem of software piracy: the effects of neutralization, shame, and moral beliefs. *Information & Management*, **49**, 334–341.

Skarlicki, D. & Folger, R. (1997) Retaliation in the workplace: the role of distributive, procedural and interactional justice. *Journal of Applied Psychology*, **82**, 434–443.

Skarlicki, D., Folger, R. & Tesluk, P. (1999) Personality as a moderator in the relationship between fairness and retaliation. *Academy of Management Journal*, **42**, 100–108.

Stahl, B.D., Doherty, N.F. & Shaw, M. (2012) Information security policies in the UK healthcare sector: a critical evaluation. *Information Systems Journal*, **22**, 77–94.

Straub, D. (1990) Effective IS security: an empirical study. *Information Systems Research*, **1**, 255–276.

Straub, D., Boudreau, M.-C. & Gefen, D. (2004) Validation guidelines for IS positivist research. *Communications of the Association for Information Systems*, **13**, 381–427.

Straub, D., Carlson, P. & Jones, E. (1992) Deterring highly motivated computer abusers: a field experiment in computer security, In: IT Security: The Needs for International Cooperation, Gable, G. & Caelli, W. (eds), pp. 309–324. Elsevier Science Publishers, Amsterdam.

Straub, D. & Nance, W.D. (1990) Discovering and disciplining computer abuse in organizational: a field study. *MIS Quarterly*, **14**, 45–62.

Straub, D. & Welke, R. (1998) Coping with systems risks: security planning models for management decision making. *MIS Quarterly*, **22**, 441–469.

Sweeney, P.D. & McFarlin, D.B. (1993) Workers' evaluations of the "ends" and the "means": an examination of four models of distributive and procedural justice. *Organizational Behavior and Human Decision Processes*, **55**, 23–40.

Sykes, G. & Matza, D. (1957) Techniques of neutralization: a theory of delinquency. *American Sociological Review*, **22**, 664–670.

Thurman, Q.C., St. John, C. & Riggs, L. (1984) Neutralization and tax evasion: how effective would a moral appeal be in improving compliance to tax laws? *Law & Policy*, **6**, 309–327.

Trevino, L. & Victor, B. (1992) Peer reporting of unethical behavior: a social context perspective. *Academy of Management Journal*, **35**, 38–64.

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

Vance, A., Lowry, P.B. & Eggett, D. (2015) Increasing accountability through user-interface design artifacts: a new approach to addressing the problem of access-policy violations. *MIS Quarterly*, **39**, 345–366.

Warkentin, M. & Willison, R. (2009) Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems*, **18**, 101–105.

Warkentin, M., Willison, R. & Johnston, A.C. (2011) The role of perceptions of organizational injustice and techniques of neutralization in forming computer abuse intentions. Proceedings of the 17th Americas Conference on Information Systems, Detroit, Michigan.

Warkentin, M., Walden, E.A., Johnston, A.C. & Straub, D. W. (2016) Neural correlates of protection motivation for secure IT behaviors: an fMRI exploration. *Journal of the Association of Information Systems*, **17**, 194–215.

Willison, R. (2002) Opportunities for computer abuse: assessing a crime specific approach in the case of Barings Bank, unpublished Ph.D. dissertation, University of London.

Willison, R. (2006) Understanding the perpetration of employee computer crime in the organisational context. *Information and Organization*, **16**, 304–324.

Willison, R., and Warkentin, M. (2010) The expanded security action cycle: A temporal analysis “Left of Bang”, Proceedings of the 2010 IFIP International Workshop on Information Systems Security Research, Dewald Roode Information Security Workshop, Boston, MA., 392–438.
Willison, R. & Warkentin, M. (2013) Beyond deterrence: an expanded view of employee computer abuse. *MIS Quarterly*, **37**, 1–20.

Biographies

Robert Willison is a senior lecturer at Newcastle University Business School. He earned his Ph.D. in IS from the London School of Economics and Political Science. He has served as a guest AE editor for *MIS Quarterly* and a guest editor for *European Journal of Information Systems*. His work has appeared in *MIS Quarterly*, *European Journal of Information Systems, Information and Organization, Information and Management* and *Communications of the ACM*. His broad area of research is IS security, with a focus on employee computer abuse.

Merrill Warkentin is a Professor of MIS and the Drew Allen Endowed Fellow in the College of Business at Mississippi State University. His research, primarily on the impacts of organizational, contextual and dispositional influences on individual behaviours in the context of information security and privacy, has appeared in *MIS Quarterly, Decision Sciences, Journal of the Association for Information Systems, European Journal of Information Systems, Decision Support Systems, Information Systems Journal* and others and he is the author or editor of seven books. He has authored or co-authored over 250 published manuscripts, including over 70 peer-reviewed journal articles, with over 10,000 citations. He serves or has served as Associate Editor of *MIS Quarterly, Information Systems Research, Decision Sciences, European Journal of Information Systems, Information and Management* and other journals. He has held officer and other leadership positions at AIS, DSI, IFIP and ACM. His work has been funded by NATO, NSF, NSA, DoD, Homeland Security, IBM and others. He has chaired several international conferences and was the Program Co-Chair for the 2016 AIS Americas Conference on Information Systems (AMCIS).

Allen C. Johnston is an Associate Professor and the Director of the MS in MIS program in the Collat School of Business at the University of Alabama at Birmingham (UAB). The primary focus of his research is in the areas of behavioural information security and his research can be found in such outlets as *MIS Quarterly, European Journal of Information Systems, Communications of the ACM, Journal of the Association for Information Systems, Journal of Organizational and End User Computing, Journal of Information Privacy and Security* and *The DATABASE for Advances in Information Systems*. He currently serves as AE for *European Journal of Information Systems, Decision Sciences,* and the Journal of Information Privacy and Security, serves on the Editorial Review Board for *The DATABASE for Advances in Information Systems*, and is a founding member of the IFIP Working Group on Information Systems Security Research (WG8.11/11.13).

APPENDIX: EXAMPLE SCENARIOS AND SURVEY INSTRUMENT

The survey respondent was presented with instructions, then read four unique scenarios (out of 36 possible versions), such as the following examples:

<u>Perceived Procedural Injustice, (No Perceived Distributive Injustice), Neutralization = Denial of Injury, Perceived Sanction Certainty = Low, Perceived Sanctioned Severity = High</u>

Joe works in a large financial institution where he analyzes investment candidates for his firm. He did the same job as the other analysts who received raises, and he also believed that his work quality was as good as theirs. Last year, Joe did not get a raise, although other analysts in his firm did. Joe did not believe that the raise process was fair. He thought it would not hurt anyone for him to know who received what raise, so Joe decided to steal a supervisor’s password (by looking in his desk drawer) so he could log on to the administrative server to see all the employee evaluations of all the analysts in his department. Joe believes his chances of getting caught and punished are low, but if caught, the punishment would be severe.

Perceived Distributive and Procedural Injustice (both), Neutralization = Metaphor of the Ledger, Perceived Sanction Certainty = Low, Perceived Sanctioned Severity = Low

Joe works in a large financial institution where he analyzes investment candidates for his firm. He did the same job as the other analysts who received raises, and he also believed that his work quality was as good as theirs. Last year, Joe did not get a raise, although other analysts in his firm did. Joe believed it was unfair that he did not also get a raise, and also felt that the raise process was unfair. Because Joe thought he had been a model employee for so many years, he figured it would be justified to break the rules just this one time. So Joe decided to steal a supervisor's password (by looking in his desk drawer) so he could log on to the administrative server to see all the employee evaluations of all the analysts in his department. Joe believed his chances of getting caught and punished are low, and if caught, the punishment would be minimal.

Perceived Distributive Injustice, (No Perceived Procedural Injustice), Neutralization = Denial of the Victim, Perceived Sanction Certainty = High, Perceived Sanctioned Severity = High

Joe works in a large financial institution where he analyzes investment candidates for his firm. He did the same job as the other analysts who received raises, and he also believed that his work quality was as good as theirs. Last year, Joe did not get a raise, although other analysts in his firm did. Joe did not believe this was fair. Joe decided to steal a supervisor's password (by looking in his desk drawer) so he could log on to the administrative server to see all the employee evaluations of all the analysts in his department. Joe felt justified in doing this because he felt that he was the actual injured party. Joe believed his chances of getting caught and punished are high, and if caught, the punishment would be severe.

Following each scenario, the respondent viewed the manipulation check (see examples below), the realism test and the measure of the latent construct – the dependent variable, behavioural intention to commit computer abuse. The behavioural intention questions were developed to be specific to the scenario framework used in this study.

1 Did Joe feel it was fair that he didn't get the same raise as the other analysts?
2 Did Joe feel it was not very likely he would be punished for getting access to the data?
3 Did Joe think that his actions wouldn't really hurt anyone?

How 'realistic' do you think the above scenario is?
0 (unrealistic) 1 2 3 4 5 6 7 8 9 10 (realistic)

	SD	D	N	A	SA
In that situation, I would do the same as Joe.	1	2	3	4	5
If I were Joe, I would have also looked at the data that way.	1	2	3	4	5
I think I would do what Joe did if this happened to me.	1	2	3	4	5