doi: 10.1111/isj.12063

Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: an empirical study of the influence of counterfactual reasoning and organisational trust

Paul Benjamin Lowry,* Clay Posey,† Rebecca (Becky) J. Bennett‡
& Tom L. Roberts§

*College of Business, City University of Hong Kong, P7718, Academic Building I, 83 Tat Chee Avenue, Kowloon Tong, Hong Kong, China, e-mail: Paul.Lowry.PhD@gmail.com,†Information Systems, Statistics and Management Science, Culverhouse College of Commerce, The University of Alabama, Box 870226, Tuscaloosa, AL 35487, USA, e-mail: cposey@cba.ua.edu,‡Department of Management, College of Administration and Business, Louisiana Tech University, 502 W. Texas Avenue, P.O. Box 10318, Ruston LA71272, USA, and e-mail: rbennett@latech.edu,§School of Accountancy and Information Systems, College of Administration and Business, Louisiana Tech University, P.O. Box 10318, 502 W. Texas Avenue, Ruston, LA 71272, USA e-mail: troberts@CAB.latech.edu

Abstract. *Research shows that organisational efforts to protect their information assets from employee security threats do not always reach their full potential and may actually encourage the behaviours they attempt to thwart, such as reactive computer abuse (CA). To better understand this dilemma, we use fairness theory (FT) and reactance theory (RT) to explain why employees may blame organisations for and retaliate against enhanced information security policies (ISPs). We tested our model with 553 working professionals and found support for most of it. Our results show that organisational trust can decrease reactive CA. FT suggests that explanation adequacy (EA) is an important factor that builds trust after an event. Our results also suggest that trust both fully mediates the relationship between EA and CA and partially mediates the relationship between perceived freedom restrictions related to enhanced ISPs and reactive CA. EA also had a strong negative relationship with freedom restrictions. Moreover, organisational security education, training and awareness (SETA) initiatives decreased the perceptions of external control and freedom restrictions and increased EA, and advance notification of changes increased EA. We also included 14 control variables and rival explanations to determine with more confidence what drove reactive CA in our context. Notably, the deterrence theory (DT)-based constructs* *of sanction severity, certainty and celerity had no significant influence on reactive CA. We provide support for the importance of respectful communication efforts and SETA programmes, coupled with maximising employee rights and promoting trust and fairness to decrease reactive CA. These efforts can protect organisations from falling victim to their own organisational security efforts.*

Keywords: fairness theory (FT), reactance theory (RT), deterrence theory (DT), counterfactual reasoning, reactive computer abuse (CA), explanation adequacy (EA), organisational trust, security education, training, and awareness (SETA), deterrence, security, organisation communication

INTRODUCTION

Securing sensitive organisational data has become increasingly vital to organisations. Although information security has long been necessary (Straub 1990), it has grown in importance with increased globalisation and computing complexity. Thus, recent studies have shown that firms' expenditures for security controls are rapidly rising (Gartner 2009; Brenner 2009). Global information security spending totalled approximately US$71 billion in 2014 and is expected to top US$86 billion by 2016 (Rivera and van der Meulen 2014; PWC 2015). This trend is illustrated by the US federal government, which has been decelerating spending on information technology (IT) while projecting nearly 9% annual spending growth on IT security between 2011 and 2016 (Peterson 2011). These expenditure increases in the private sector are likely a consequence of the rapid increase of security breaches and associated losses, resulting in damages averaging US$3.5 million per breach incident (Ponemon Institute 2014).

Although security agendas have traditionally focused on threats external to organisations, breaches stemming from insiders are considered to be among the greatest threats to organisational information security (D'Arcy and Devaraj 2012; Crossler *et al*. 2013; Posey *et al*. 2013; Vance *et al*. 2013; Willison and Warkentin 2013). For example, the percentage of attacks thought to stem from insiders increased by 10% from 2013 to 2014, with 72% of insider-led attacks over the decade between 2005 and 2014 coming from the 4-year span of 2010 to 2013 (PRC 2013). Not only do organisations risk direct losses from these breaches but they also spend 42 or more days on resolution efforts per abuse incident (PWC 2015; Ponemon Institute 2014).

In response to these threats, organisations have often developed and implemented stringent controls, information security policies (ISPs) and sanctions to deter individuals from engaging in such detrimental activities. Examples from the literature include monitoring and controls; formal security education, training and awareness (SETA) programmes; mandatory ISPs; and punishment (Boss *et al*. 2009; D'Arcy and Herath 2011; Chen *et al*. 2013). These initiatives align with the criminological foundation of deterrence theory (DT), which suggests that the perceived characteristics of sanctions deter individuals from criminal activity. Individuals are dissuaded from committing criminal acts if they have expectations of being caught (i.e. certainty of sanction), being punished severely (i.e. severity of sanction) and receiving such punishment swiftly (i.e. celerity of sanction; Paternoster 1987). We consider socio-technical rather than technical solutions because they can be more effective in managing organisational security (Crossler *et al*. 2013) and in thwarting computer abuse (CA)[1] (Willison and Warkentin 2013).

Although some research has shown that these increases in security efforts act via individuals' perceptions of sanctions to *decrease* employees' misuse of internal systems (D'Arcy *et al*. 2009; D'Arcy and Devaraj 2012), other research has pointed to an *increased* frequency of CA (or intentions; i.e. *reactive* CA) as a reaction to the imposition of ISP changes (Moore *et al*. 2008), to new ISPs seen as restrictive (Lowry and Moody 2014) or soon after the implementation of increased sanctions (Posey *et al*. 2011a). Two additional studies similarly found a negative relationship between the increased severity of sanctions and compliance intentions (Herath and Rao 2009a, 2009b). These findings indicate that scenarios exist where increased deterrence may not work in general or may backfire, resulting in reactive CA. Even in the best of circumstances, continual enhancements to ISPs are the increasing norm in organisations, and these enhancements can be stressful and disruptive to employees' daily work routines (D'Arcy *et al*. 2014). Hence, considering how to effectively roll out enhanced ISPs is an organisational imperative.

Consequently, we respond to the call by Willison & Warkentin (2013) for researchers to 'consider the thought processes of the potential offender and how these are influenced by the organizational context…' as related to CA and DT (p. 1). We improve the understanding of the enigmatic phenomenon of reactive CA by focusing on insiders' thought processes following enhancements or changes to their organisations ISPs. We focus on how employees reason about why the ISP enhancements/changes occurred and on their assignment of blame for such organisational actions. Our research relies on two foundations: reactance theory (RT; Brehm 1966; Lowry and Moody 2014) and fairness theory (FT; Folger and Cropanzano 2001).

Literature review of empirical deterrence research in preventing CA

First, we review key empirical journal articles in IS security involving deterrence against CA.[2] Our review also builds on reviews by D'Arcy & Herath (2011) and Willison & Warkentin (2013). It is important to first explain what we mean by CA. CA has been defined as 'the unauthorized and deliberate misuse of assets of the local organisation information system by individuals associated with the organization' (Straub 1990, p. 257), otherwise known as *organisational insiders*.[3]

[1] CA is generally defined as the deliberate misuse of organisational computing and information assets by organisational insiders (we more formally define CA in the next section).

[2] For concision and quality, we omit conference papers and book chapters as these are not as rigorously reviewed and thus have many inconsistencies in their operationalisation and findings.

[3] *Organisational insiders* refer to all individuals, such as full-time employees, part-time workers, temporary employees or contracted individuals, who have access to organisationally relevant information while fulfilling their organisational duties (Posey *et al*., 2013)

CA has also been termed *internal CA* to differentiate it from abuse external to an organisation (e.g. hacking), but we use the former term for concision.[4]

CA is not just an ‘IT problem’; it is also an organisation-wide problem because insiders represent a severe threat to organisational information resources that cannot be controlled by technology and the threat of punishment alone (Dhillon and Torkzadeh 2006; D’Arcy *et al*. 2009; Siponen *et al*. 2009). CA is a form of *organisational deviance*[5]; thus, many security professionals view it as more detrimental to organisational security than external attacks (Loch *et al*. 1992; Whitman 2003). Our review only includes organisational CA.[6]

Again, DT suggests that perceived or real sanctions, whether formal or informal, deter individuals from criminal activity (Paternoster 1989). Such sanctions are conceptualised in terms of certainty (how *likely*), severity (how *strong*) and celerity (how *swift*) (Paternoster 1989). DT predicts that individuals are dissuaded from committing crime if they have expectations of being caught (certainty), being punished severely (severity) and receiving such punishment swiftly (celerity) (Paternoster 1987; D’Arcy and Herath 2011).

Many studies, as summarised in Online Appendix B, have examined ways to deter CA using DT or DT-related constructs. The first trend that we note is that they have yielded mixed results, especially in terms of formal sanctions, as also concluded by D’Arcy & Herath (2011) and Willison & Warkentin (2013). A minority of studies show that both the severity and certainty of sanctions are effective in deterring CA (Straub and Nance 1990; Peace *et al*. 2003; Ugrin *et al*. 2008) but generally when not considering other factors. In other studies, when considering other factors, only severity (D’Arcy *et al*. 2009; Cheng *et al*. 2013) or certainty were significant (Kankanhalli *et al*. 2003; Herath and Rao 2009a; Herath and Rao 2009b; Li *et al*. 2010). Yet

[4] We further recognise that there is a distinction between malicious/criminal and non-malicious/non-criminal CA, and some researchers do not consider non-malicious/non-criminal activities as CA (e.g. Willison and Warkentin, 2013; Guo, 2013). Non-malicious behaviours include activities such as not backing up a computer, not changing a password when requested, not complying with ISPs, general carelessness and engaging in non-work-related computing (Moody and Siponen, 2013; Ugrin and Pearson, 2013; Guo, 2013). Although these are not criminal behaviours, they are non-compliant behaviours that have the potential for great damage to organisations and thus are routinely deterred through ISPs, monitoring and so on. Consequently, these non-malicious actions have received extensive coverage in the IS security literature; we include both forms of CA in our literature review as they both are of strong interest to the IS research community and to security practitioners. That being said, there is justifiable reason to suspect that DT may not apply well to non-criminal/non-malicious CA because DT was created for deterring malicious criminal acts (Willison and Warkentin, 2013); thus, it should work better to counter cyber espionage than non-malicious offenses such as not-backing up one’s computer.

[5] *Organisational deviance* refers to intentional actions by employees that violate company norms and in so doing harm or have the potential to harm an organisation (Robinson and Bennett, 1995).

[6] Namely, our review excludes studies that do not involve organisational employees or an organisational context (e.g., Gurung *et al*., 2009; Anderson and Agarwal, 2010); we thus also exclude consumer and student abuses such as digital piracy (e.g., Higgins, 2004; Higgins *et al*., 2005; Phau and Ng, 2010; Chan and Lai, 2011; Popham, 2011) and unauthorised file sharing (Hansen and Walden, 2013), unless it occurs in the workplace(e.g., Peace *et al*., 2003). Likewise, we omit hacking, cracking and cyberterrorism from external entities (Hollinger, 1993; Goode and Cruise, 2006). Importantly, we exclude studies focused on predicting ISP compliance that are not rooted in at least a portion of RT (e.g., Johnston and Warkentin, 2010; Ifinedo, 2012). However, we do include non-compliance studies as these are included in our definition of CA. Finally, a study on the mind-set of those who commit CA was omitted because no deterrence-related (informal or formal) constructs were used in its model (i.e., Posey *et al*., 2011b).

other studies found no formal sanctions to be effective (Siponen and Vance 2010; Hu *et al*. 2011; Vance and Siponen 2012). In two studies, severity even had the inexplicable, unpredicted effect of increasing CA (Herath and Rao 2009a; Herath and Rao 2009b). In a cross-cultural study, certainty was only effective for the Korean sample, and severity was only effective for the US sample (Hovav and D'Arcy 2012). Few of the studies used celerity in their models; the one that did found it to be ineffective is Hu *et al*. (2011). Finally, one study on cyberloafing[7] found mixed overall results for sanctions against it, depending on the specific cyberloafing involved, such as surfing for porn or shopping at work (Ugrin and Pearson 2013).

Despite informal sanctions – such as shame,[8] morality and norms – being a part of DT (Paternoster and Simpson 1996), fewer IS security studies have considered these. Two studies that considered shame found it to be ineffective (Siponen and Vance 2010; Hu *et al*. 2011). Several additional studies found norms or social influences to be more consistent and effective deterrents than formal sanctions (Lee *et al*. 2004; Herath and Rao 2009b; Li *et al*. 2010; Siponen *et al*. 2010; D'Arcy and Devaraj 2012; Cheng *et al*. 2013). Departing from these, Siponen & Vance (2010) created a two-part informal sanctions measure involving certainty and severity that generally dealt with social pressure at work and found it to have no significant effect. However, the same authors later found the same conceptualisation to be effective (Vance and Siponen 2012). Morality/ethics (e.g. moral reasoning or moral/ethical commitment) has also frequently been shown to be an effective informal deterrent against CA or an incentive towards ISP compliance (Myyry *et al*. 2009; D'Arcy and Devaraj 2012; Hovav and D'Arcy 2012; Vance and Siponen 2012; Lowry *et al*. 2014). Recently, accountability has been shown to be effective (Vance *et al*. 2013).

What then explains the inconsistent results of formal sanctions in IS security studies? One viable argument is that they have several operationalisation and contextualisation issues involving sanctions.[9] However, there are several other related issues in this literature.[10] Crucially,

[7] *Cyberloafing* is the misuse of the Internet at work, which is defined as any voluntary act of employees using their companies' Internet access during office hours to surf non-job related web sites for personal purposes or to check personal e-mail (Lim, 2002)

[8] Technically speaking, Paternoster and Simpson (1996) note informal sanctions as those that are formed from social pressures such as norms and morality. Shame is a special form of sanction in that it is entirely self-imposed and chosen. Nonetheless, it is a sanction related to DT.

[9] For example, sanctions were only highly effective when they were the only deterrent considered in a study (e.g., Straub and Nance, 1990; Peace *et al*., 2003; Ugrin *et al*., 2008) or when researchers created a second-order or formative construct of sanctions and did not consider severity, certainty and celerity separately (Lee *et al*., 2004; Siponen *et al*., 2010; D'Arcy and Devaraj, 2012; Barlow *et al*., 2013; Ugrin and Pearson, 2013).

[10] As illustration of inconsistent, and often questionable, operationalisation in the literature, Straub & Nance (1990) used investment in security countermeasures as a proxy for the certainty and severity of sanctions. Ugrin and Pearson (2008) implemented deterrence as separate, non-validated one-item measures similar to the severity and certainty of sanctions. Kankanhalli (2003) used security personnel hours as a surrogate for certainty. Lee *et al*. (2004) used ISPs, security awareness and security systems to represent overall sanctions. Siponen & Vance (2010) departed from common practice in that they combined the certainty and severity of formal sanctions into one measure; the certainty and severity of informal sanctions were one measure; the certainty and severity of shame were one measure. The same authors, repeated this measurement in (Vance and Siponen, 2012). Yet other studies departed from the tradition of measuring the sanctions elements (severity, certainty, celerity) separately and combined them into one construct (most of which did not go through established formative measurement procedures). In these studies, several found overall sanctions to be effective (Lee *et al*., 2004; Siponen *et al*., 2010; D'Arcy and Devaraj, 2012; Barlow *et al*., 2013; Ugrin and Pearson, 2013).

when this literature considered factors other than formal sanctions, the findings have been more consistent: informal sanctions such as norms and morality have almost always been effective, whereas shame is rarely effective. We thus concur with D'Arcy & Herath (2011) and Willison & Warkentin (2013) that IS security researchers need to consider more compelling informal factors that can deter CA.

In fact, we believe that other neglected organisational and personal factors could help explain anomalous results. One such surprising finding that begs for interpretation is the finding that sanction severity *increases* CA (Herath and Rao 2009b; Herath and Rao 2009a). Likewise, another study showed an *increased* frequency of CA soon after the imposition of changes to ISPs (Moore *et al*. 2008). What explains these counterintuitive findings? Clearly, something beyond DT is affecting insiders' CA behaviours. We propose that justice theory can help to explain such perplexing results. In fact, Willison & Warkentin (2013) note that not enough research has considered the topic of insider *motives* for CA, including those related to injustice.[11] Although they elegantly argued for considering organisational justice research, Willison & Warkentin (2013) were not the first to research this conclusion.

The limited studies that exist have shown much more consistent, positive results than the DT literature that has focused solely on formal sanctions. For example, Lim (2002) found that an employee's increased sense of justice in the workplace is associated with decreased cyberloafing. Workman (2009) provided a model based on protection motivation theory (PMT), psychological contract theory and justice theory to explain how procedural justice moderates PMT by encouraging appropriate security behaviours. Procedural justice was a positive moderator, and severity and vulnerability were also significant. Lowry *et al*. (2010a, 2014) found that new ISPs that threaten employees' personal sense of freedom (similar to injustice) can cause them to react negatively by decreasing their compliance intent. Posey *et al*. (2011a) used organisational justice constructs and RT to explain how organisational injustice and restrictions of privacy can spur CA. The study showed that perceived breaches of privacy and justice emanating from computer monitoring practices can lead to more self-reported CA. Interestingly, an IS study on mandatory compliance in ERP use showed that perceived fairness of punishment improved compliance intentions, but actual punishment received decreased perceptions of justice (Xue *et al*. 2011). Willison & Warkentin (2013) aptly note that while numerous organisational behaviour and management studies have considered various causes of such organisational deviance outside of DT, the IS literature is largely silent on this issue.

Given these potential explanations for anomalous responses to using DT to deter CA, we leverage FT and RT to explain this phenomena in our study. Additionally, we include trust in the organisation as a mediator for explaining CA. We believe trust is particularly salient because when one's trust is violated through a sense of injustice from an organisation, it is difficult to repair (Gillespie and Dietz 2009). Conversely, trust in one's organisation has been shown to have very positive results in promoting prosocial and compliant behaviour (Colquitt *et al*.

[11] They explicitly note the following: 'we argue that progress may be achieved by considering motives in relation to workplace disgruntlement…To address the problem of disgruntlement, we propose the use of an existing body of research which examines the issue of fairness within the organizational context. This body of research falls under the umbrella term organizational justice' (Willison and Warkentin, 2013, p. 11).

2007). Pivotally, research has inextricably tied justice, trust and trustworthiness together (Colquitt and Rodell 2011). In considering fairness and reactance, we do so in the balanced consideration of organisational trust.

BACKGROUND ON RT AND FT

We rely on both RT and FT to gain better insight into reactive CA, and we focus on the components employees are most likely to use in assigning blame following increases in internal information security efforts. Our study answers the call for investigations into intrapersonal factors that may drive specific forms of organisational deviance such as CA (Willison and Warkentin 2013; Crossler *et al*. 2013). If we can improve the understanding of how blame is assigned, organisations will be better able to prevent negative reactions to enhanced ISPs.

Reactance theory

Reactance theory (Brehm 1966; Lowry and Moody 2014) is based on the premise that because individuals relish the perception of environmental control, when that control (and related freedom) is infringed upon by others, individuals might 'act out' and engage in counterproductive behaviour to regain a sense of control (Bennett 1998). According to Brehm (1966, p. 378), 'If a person's behavioural freedom is reduced or threatened with reduction, the person will become motivationally aroused'. This arousal, termed *psychological reactance*, is directed towards 'the reestablishment of whatever freedom has already been lost or threatened' (p. 378). Because an employee can rarely re-establish behavioural freedom after it has been infringed upon by organisational policies, structures, actions and so on, 'he will feel that he can do what he wants, that he does not have to do what he doesn't want, and that at least in regard to the freedom in question, he is the sole director of his own behaviour' (p. 384). Such psychological reactance is particularly problematic when individuals are prohibited from engaging in workplace behaviours they were once permitted to perform, as is often the case with new ISPs that altogether ban certain users' actions (Lowry *et al*. 2010a; Lowry and Moody 2014). We posit that the same issues can occur when an organisation enhances its ISPs.

Similarly, researchers examining organisational justice have also explained that when employees believe they have been treated unjustly – whether by a lack of appropriate procedures (i.e. *procedural justice*), unequal distributions of outcomes (i.e. *distributive justice*), offenses to interpersonal sensitivity (i.e. *interpersonal justice*) or a lack of justifications for actions (i.e. *informational justice*) (Colquitt *et al*. 2001) – they are likely to engage in actions detrimental to the organisation. Such 'balancing of the justice scales' has been found in various organisational settings and results in harmful employee behaviours such as cyberloafing (Lim 2002), organisational deviance (Mitchell and Ambrose 2007), counterproductive workplace behaviours (Fox *et al*. 2001), retaliation (Skarlicki and Folger 1997) and sabotage (Ambrose *et al*. 2002). Clearly, the fairness with which employees believe they are treated has a substantial influence on potentially negative cognitions about and reactions to such organisational events.

Fairness theory

A recent advancement in the study of these reactions is FT (Folger and Cropanzano 2001; Folger and Cropanzano 1998; Mirchandani and Lederer 2014). Similar to but differentiating itself from studies leveraging organisational justice (e.g. Xue *et al*. 2011), FT analyses the process that employees use to assess organisational explanations for an event (e.g. a new decision, a new policy, layoffs or enhanced ISPs) as the basis for judging the fairness of that event. Individuals assign accountability or blame for organisational events that influence them based on counterfactuals, *whereas justice theory presumes that blame has already occurred*. Importantly, the assignment of blame is core to organisational justice.[12] A meta-analytic review revealed that FT can predict the results of organisational explanations for a wide variety of events (Shaw *et al*. 2003).

Fairness theory thus builds on procedural and interactional justice to demonstrate that even when ISPs are administered inconsistently or employees believe they are treated disrespectfully, employees may still perceive fairness depending on how blame for the event is assigned. For example, if employees are told that their access to external websites will be restricted, they may perceive this as annoying, unfair or limiting their freedoms, but if the announcement is preceded with an explanation that hackers have gained access to the system through external sites, then the related organisational event will more likely be judged as fair and will subsequently be accepted and followed. Without an adequate explanation, however, the event will more likely be judged as unfair, will be less likely to be accepted, and may even lead to reactive CA such as attempting to circumvent the restrictions or firewall or worse.

In assigning blame, individuals cognitively assess three separate but related event components: (1) Is the outcome of an event considered injurious, harmful or otherwise disadvantageous? (2) Can the action be attributed to someone or something's discretionary action? (3) Does the action violate sound principles or ethical standards? These three questions form the basis for what are termed the '*would*', '*could*' and '*should*' *counterfactuals* of FT (Folger and Cropanzano 2001), respectively. These act as a foil to which an employee compares the negative event, because the employee places '"what is" side by side with "what might have been"' (Folger and Cropanzano 2001, pp. 5–6). Hence, 'counterfactual reasoning is an effort to understand the event' (Gilliland *et al*. 2001, p. 671). If an event is not harmful, cannot be attributed to the volitional action of another or fails to violate norms or ethical standards, then an injustice has not taken place. Here, there would be an 'upward' counterfactual assessment, per FT terminology.

A '*would*' *counterfactual* is based on a hypothesised condition that *would* have resulted had a feasible, alternative decision been made as opposed to the event that occurred. This counterfactual assists the individual in answering the question 'Would my well-being have been better

[12] Folger & Cropanzano (2001) stated that 'the central topic of social justice is the assignment of blame' (p. 1). Further, 'When people identify an instance of unfair treatment, they are holding someone accountable for an action (or inaction) that threatens another person's material or psychological well-being. If there is adequate explanation, there is no social injustice. For this reason, the process of accountability, or how another social entity comes to be considered blameworthy, is fundamental to justice perceptions. When people ascertain the fairness of someone's actions, they are trying to decide whether to hold that person accountable for those actions' (p. 1).

off if this event had played out differently?' (Shaw *et al*. 2003, p. 447). The employee then evaluates the discrepancy between the actual and hypothetical scenarios. The magnitude of the difference has a direct bearing on perceived fairness. The larger the negative difference, the greater the likelihood that a decision will be seen as unfair (i.e. result in a downward counterfactual). The greater the harm perceived by the individual from an event, the more likely the individual is to entertain a strong downward 'would' counterfactual. Conversely, *ceteris paribus*, if the discrepancy is seen as favourable, it results in an upward 'would' counterfactual.

The other two counterfactuals determine whether blame is attributed to the actor and thus whether the unfavourable event becomes 'unfair'. A '*could*' *counterfactual* 'addresses whether the negative event was under the decision maker's discretionary control' (Gilliland *et al*. 2001, p. 671). Discretionary conduct involves another party's choices among feasible alternatives (Folger and Cropanzano 2001). 'Could' counterfactuals answer the questions 'Could the decision maker have acted differently; were there other feasible behaviours?' (Shaw *et al*. 2003, p. 447). *Ceteris paribus*, the more employees consider a negative outcome to be under their supervisors' discretionary control, the more likely they will judge decisions as unfair – resulting in a downward 'could' counterfactual. If employees understand that different actions were not possible and that the events were due to circumstances beyond the supervisor's control, they cannot realistically assign blame to the supervisor (Folger and Cropanzano 2001), and there will be an upward 'could' counterfactual.

Finally, '*should*' *counterfactuals* 'address moral or ethical conduct and suggest that [individuals] also evaluate whether the decision maker acted in accordance with appropriate standards' (Gilliland *et al*. 2001, p. 671). This assessment provides an individual with an answer as to whether the decision maker *should* have acted differently relative to a set of standards (Folger and Cropanzano 2001). Anything perceived as unethical or immoral will generate a downward 'should' counterfactual and will be more likely to generate perceptions of blame and hence solidify an unfairness judgement. Strong downward 'should' counterfactuals can also emanate from the decision maker's deviation from standards based on industry norms, training, expectations and so on; hence, supervisors implementing ISP changes should clearly explain industry surety standards to avoid downward 'should' counterfactuals. Often, upward 'should' counterfactuals result from organisations offering adequate explanations, whereby organisational agents thoroughly describe to employees the basis for organisational actions and how those actions follow accepted principles, whether internal and/or external to the organisation (Shaw *et al*. 2003). If industry norms or standards are not understood by employees, something else may take their place as the expectation to which 'should' is compared. No explanation for ISP changes will likely be perceived by employees as a downward counterfactual because of their comparison to the previously understood standard.

THEORY AND HYPOTHESES

Figure 1 summarises the organisation-focused model that we propose. We first explain that the more employees perceive external control for their supervisor's decision (i.e. upward 'could' counterfactual) and explanation adequacy (EA; i.e. upward 'should' counterfactual for

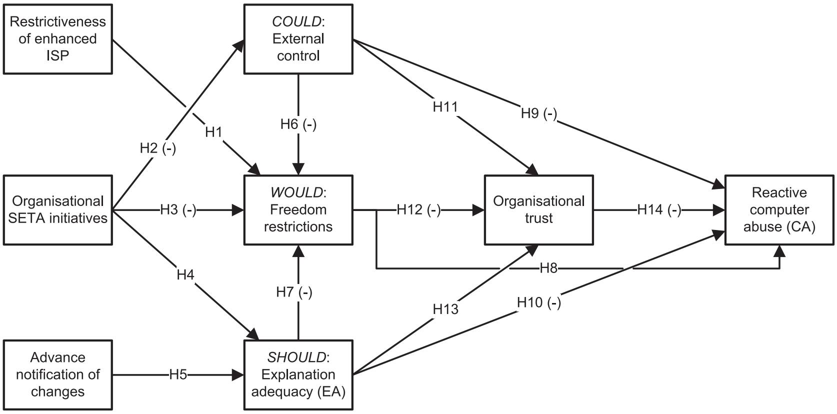
Restrictiveness of enhanced ISP
Organisational SETA initiatives
Advance notification of changes
COULD: External control
WOULD: Freedom restrictions
SHOULD: Explanation adequacy (EA)
Organisational trust
Reactive computer abuse (CA)
H1
H2 (-)
H3 (-)
H4
H5
H6 (-)
H7 (-)
H8
H9 (-)
H10 (-)
H11
H12 (-)
H13
H14 (-)

Figure 1. Model of organisation-driven predictors of reactive CA.

enhanced ISPs), the less likely they will be to commit reactive CA. In our context, *external control* is defined as the extent to which the internal decision maker is perceived to have control over negative events. Employees are unlikely to blame internal decision makers if they perceive that resolutions were beyond their control. The perception of external control should decrease reactive CA and increase employees' trust in the organisation.

Conversely, EA is the extent to which explanations provided by the organisation are clear, detailed and based on accepted standards. EA has been shown to lessen blame and to enhance fairness perceptions (Shaw *et al*. 2003) and is expected to increase employee trust. Thus, EA should decrease reactive CA. EA is an important concept in the study of organisational fairness because it also implies informational justice (Colquitt 2001; Kernan and Hanges 2002). In contrast, perceived increases in freedom restrictions in an enhanced ISP (i.e. downward 'would' counterfactual) should increase the likelihood of reactive CA.

Our model also considers the important role of organisational trust, along with these FT and RT components. External control and EA are predicted to increase organisational trust, whereas freedom restrictions are proposed to decrease it. Other forces we expect to affect employees' counterfactual thinking include the perceived restrictiveness of the enhanced ISP increasing perceived freedom restrictions, organisational SETA initiatives decreasing perceived external control and freedom restrictions but increasing EA and advance notification of changes increasing EA. Finally, we predict trust to decrease reactive CA. Although our focus is on organisationally driven predictors of CA, we introduce 14 additional individual-level control variables that add robustness to the testing of our underlying model.

The antecedents of counterfactual thinking when ISPs are enhanced

Enhanced security is a key part of ISPs designed to prevent CA: 'organisations have an increasing need to monitor and control members who may (either wittingly or unwittingly) jeopardise the security of organisational assets' (Alge *et al*. 2006, p. 221). We apply FT and the counterfactuals of 'could', 'would' and 'should' judgements in the context of enhanced ISPs typically perceived by employees as restrictive. Such unfavourable conditions can help set the stage for FT's counterfactual thinking process. Thus, enhanced ISPs increase the need for employees to understand the cause of the 'event' in order to assign blame, which determines whether the resulting counterfactual is 'upward' or 'downward'. Table 1 summarises how we applied counterfactual thinking from FT to our context. Our first three hypotheses further contextualise the three counterfactuals to enhanced ISPs that adversely affect employees by restricting their freedom. Following FT, the first counterfactual that must be considered is 'would'.

In terms of 'would' counterfactuals, other than inconvenience to one's work environment, enhanced ISPs may produce perceived harm (downward 'would' counterfactual) via restrictions to an employee's personal choice of actions or personal freedom at work (Lowry and Moody 2014). For example, increased monitoring or controls can threaten employees' sense of

Table 1. Counterfactual thinking in an organisational information security context

Counterfactual	General framing questions	Counterfactual directionality	Application in an organisational information security context
'*Would*'	Would it be less harmful personally had the initiative not taken place?	The degree of perceived harm is: – *Greater than* what existed prior to the initiative (downward) – *Less than* what existed prior to the initiative (upward)	Other than inconvenience to one's work environment, enhanced ISPs may produce perceived harm (downward counterfactual) via restrictions to an employee's personal freedom, restrictions that were not present before the change or those that were amplified by the change
'*Could*'	Despite the harm caused by the initiative, was it under the discretionary control of the organisation or were other restraints present?	The organisation: – *Chose freely* to engage in the initiative despite other feasible alternatives (downward) – Was under *external pressure* to engage in the initiative with no other feasible alternatives available (upward)	If the employee perceives that the organisation implemented enhanced ISPs due to external forces such as governmental mandates, an upward counterfactual will be produced; however, if the organisation is believed to have acted on its own accord, then a downward counterfactual will be present, and blame will be placed on the organisation
'*Should*'	Despite the harm caused by the initiative, was it based on reasonable standards?	The organisation's actions: – *Were not* based on sound principles and tenets (downward) – *Were* based on sound principles and tenets (upward)	Organisations that fail to honestly describe why the security initiative was undertaken risk the production of downward 'should' counterfactuals. Without such accounts, employees might not be able to adequately determine the actual foundations guiding the organisation in its actions. If these foundations are believed to be unreasonable or without solid grounding, organisations are more likely to be held accountable for the harm caused by the initiative than not

information privacy and compromise their dignity, empowerment, creativity and freedom (Alge *et al*. 2006; Posey *et al*. 2011a). Likewise, *freedom restrictions* occur when an organisation engages in control and oversight over employees' work practices related to collection, storage, dissemination and use of personal information (Alge *et al*. 2006; Lowry and Moody 2014). Suppose that a company creates and implements an ISP requiring employees to use 20-character, randomly generated passwords supplied by the IT department that are changed every 30 days. An employee might envision a 'would' counterfactual in which employees continue to be allowed to choose their own passwords that are six characters in length and last indefinitely. In this case, the perceived enhanced ISP would be considered unfavourable because of a cognitive discrepancy in which employees would view the ISP as restricting their freedom and increasing their workload but would have no understanding of whether the change was necessary. We thus predict

> H1: The more restrictive the enhanced ISPs are perceived to be by employees, the greater will be the perceptions of freedom restrictions (i.e. a downward 'would' counterfactual is generated).

Aside from setting the stage for counterfactual thinking, we posit that changes in ISPs are likely to create unrealistic or distorted counterfactuals because security itself can be highly technical and arcane; thus, logic and explanations might be inadequate because employees may simply not understand the fundamental issues involved (Furnell *et al*. 2006). A lack of understanding of security principles and standards can thus distort 'could' and 'should' counterfactuals.

However, organisations have the ability to decrease the discrepancy between reality and perception with SETA programmes. These programmes can be especially effective if they 'inform employees about their roles and expectations surrounding their roles, in the observance of information security requirements' (Fitzgerald *et al*. 2006, p. 51). These programmes are implemented (1) to make employees aware of *what* threats exist, (2) to train employees *how* to perform their jobs in a secure manner and (3) to educate employees about *why* these threats exist (D'Arcy and Hovav 2007; Crossler and Belanger 2009; D'Arcy *et al*. 2009). We thus define *organisational SETA initiatives* as the degree to which an organisation formally provides its employees with an awareness of what threats exist in the work environment, why these threats exist and how they can more securely engage in work activities.

Based on FT, we expect that employees who are successfully engaged in SETA initiatives will be better able to evaluate why enhanced ISPs are needed and, as a result, be better able to create more realistic counterfactuals and are less likely to feel that such changes are capricious and unfair. We also expect that the information provided by SETA programmes will make employees less resistant to and more knowledgeable about necessary ISP changes. SETA programmes are intended explicitly to provide justifications and explanations to employees on a planned basis. That is, SETA initiatives should provide the foundation for informing employees why ISPs are important and thus why companies and employees will benefit from internal security protocols. Convincing SETA initiatives help convey to employees that an organisation's security is actually under the control of the organisation (not outside forces) and explain the standards that should be followed in order for employees to protect their organisations' information. Thus, we predict

> H2: Organisational SETA initiatives will decrease insiders' perceptions of external control related to enhanced ISPs (downward 'could' counterfactuals generated).

> H3: Organisational SETA initiatives will decrease insiders' perceptions of freedom restrictions related to enhanced ISPs (upward 'would' counterfactuals generated).

> H4: Organisational SETA initiatives will increase insiders' perceptions of EA related to enhanced ISPs (upward 'would' counterfactuals generated).

A final antecedent to the counterfactual process is advance notice, which is an explicit fairness-process trigger in FT (Folger and Cropanzano 2001). Research has shown that advance notice is a vital component of fair systems (Hovorka-Mead *et al*. 2002; Alder *et al*. 2006) and a central principle to procedural due process (Folger *et al*. 1992). Procedures are considered unfair if decision makers implement them without regard for the legitimate concerns of those affected – such as sufficient time to prepare for the adverse consequences of a decision (Brockner *et al*. 1994). In fact, fair warning is such an important aspect of the notion of fair labour practices that the US Congress passed the Worker Adjustment and Retraining Notification Act in 1988 requiring most employers with 100 or more employees to provide 60-calendar-day advance notification of plant closings and mass layoffs (US Dept. of Labor 2009). The law notes that not providing advance warning is capricious. Similarly, an ISP change is more likely to be seen as unfair if it is rolled out without warning or explanation.

From an FT perspective, this process occurs primarily because the lack of a timely explanation or the complete lack of an explanation increases the likelihood and salience of downward 'should' counterfactuals. Without prior notification and explanation, a decision is more likely to be seen by employees as having unwarranted and preventable consequences, and they may form the opinion that management '*should*' have given them adequate time to respond to the decision but capriciously chose not to. Conversely, a timely explanation will be perceived by employees as being more considerate and respectful because employees will perceive that management could have waited until the last minute to tell them but instead gave them early warning (Folger and Cropanzano 2001).

Notably, research has shown that the effect of an organisation's assurance to its employees of proper and necessary treatment is most prominent in promoting individuals' acceptance of a change and is greater when carried out 'early in the change sequence' as opposed to later (Lind and van den Bos 2002, p. 210). Conversely, employees who do not receive prior notification of a negative event often believe they were treated inappropriately and engage in negative behaviours (Greenberg 1990, 1993). This perception of poor treatment increases employees' downward 'should' counterfactuals because their desire for proper treatment and organisational conduct was not met (Folger and Cropanzano 2001). That is, management '*should*' have planned in advance and given employees advance warning of the impending change. Thus, we predict

H5: Employees who receive advance notification of changes to organisational ISPs will have increased perceptions of EA (i.e. upward ‘should’ counterfactual) with respect to those changes.

Researchers have also noted that the counterfactuals underlying the blame assignment for an event may affect each other and that they do not necessarily occur simultaneously or in a specific order (Folger and Cropanzano 2001). Given that the ‘would’ counterfactual (i.e. the harm produced by the event) is the component of FT experienced directly by the individual, we argue that both the ‘could’ and ‘should’ counterfactuals have the ability to influence the ‘would’ counterfactual process. For example, when employees perceive a lessening of freedom, they want to blame organisational actors for the harm they experience, but the perceived unfairness of the action ‘could’ be decreased if the perceived restrictions were felt to be due to circumstances lying outside the actor’s discretion, such as external control. Additionally, the unfairness perception could be lessened if the organisational agent adequately articulates good reasons for the organisational event. Therefore,

H6: The more employees perceive external control (i.e. upward ‘could’ counterfactual) for enhanced ISPs, the more freedom restriction perceptions (i.e. downward ‘would’ counterfactual) will be attenuated.

H7: The more employees perceive EA (i.e. upward ‘should’ counterfactual) for enhanced ISPs, the more freedom restriction perceptions (i.e. downward ‘would’ counterfactual) will be attenuated.

Influence of FT counterfactuals on reactive CA

New ISPs create ‘events’ (e.g. loss of access to the internet, restriction of personal computing resources, mandatory password changes) that can negatively affect organisational members via changes to daily routines and job tasks (Stanton and Stam 2006) and restrict their freedom (Lowry and Moody 2014), leading to increased job stress (Moore *et al*. 2008). Again, we assume the same issues will occur with enhanced ISPs. Importantly, RT shows that when employees perceive their freedoms as being threatened, they are more likely to resist these restrictions by engaging in negative organisational actions (Brehm and Brehm 1981; Lowry and Moody 2014). Crucially, new ISPs that threaten employees’ freedoms are associated with reactance against the new ISPs (Lowry and Moody 2014). If this pattern holds in our context of enhanced ISPs, then downward ‘would’ counterfactuals based on loss of freedom and restrictions at work should be associated with increased reactive CA.

H8: The more employees perceive freedom restrictions (i.e. downward ‘would’ counterfactual) from enhanced ISPs, the more likely they will be to commit reactive CA.

In terms of ‘could’ counterfactuals and reactive CA, if an employee perceives that the organisation implemented enhanced ISPs because of external forces such as governmental mandates, an upward counterfactual will be produced; however, if the organisation is believed to have acted on its own accord, then a downward counterfactual will be present and blame will be placed on the organisation (Folger and Cropanzano 2001) for this loss of freedom, increasing the likelihood of reactance to the organisation per RT (Lowry and Moody 2014). The former case would be more likely to result in lowered perceptions of discretion because the supervisor would seem to have had no discretionary power to institute changes in the company’s ISPs. Thus, we predict

> H9: The more employees perceive external control (i.e. upward ‘could’ counterfactual) for enhanced ISPs, the less likely they will be to commit reactive CA.

Finally, in terms of ‘should’ counterfactuals and reactive CA, organisations that fail to honestly describe why the enhanced ISPs were created risk the production of downward ‘should’ counterfactuals. Without such accounts, employees might not be able to adequately determine which foundations guided the organisation’s actions (Folger and Cropanzano 2001). If these foundations are believed to be unreasonable or without solid grounding (e.g. SETA initiatives), organisations are more likely to be held accountable for the loss of freedom caused by the initiative than not. Interestingly, FT explains that if there is no information/explanation for a change or deviation from standards, employees feel a sense of violation in that they feel they are owed an explanation (Folger and Cropanzano 2001). Again, per RT, employees will then be more likely to react against the organisation for this capricious loss of freedoms (Lowry and Moody 2014), especially when they believe the organisation owes them an explanation.

Suppose, for example, that an employee works with sensitive materials and receives training on the importance of using encryption to protect those materials. Such an employee is less likely to generate a downward ‘should’ counterfactual if he or she is told that all email communication in the nuclear energy industry must use a particular encryption standard. However, an employee without awareness of this standard or its purpose is more likely to generate negative ‘should’ counterfactuals because this deviation from usual practice will not make sense. If organisational agents explain why such standards are important, individual employees will be more likely to perceive an upward counterfactual through EA. Thus, we predict

> H10: The more employees perceive EA (i.e. upward ‘should’ counterfactual) for enhanced ISPs, the less likely they will be to commit reactive CA.

Using FT (counterfactuals) to predict organisational trust

When negative events such as increased security monitoring occur in organisations, employees will search for the cause of the unpleasant outcome (Heider 2013; Weiner 1985). Attribution theory (Weiner 1985) suggests that one of the important factors individuals look to in making sense of their discomfort is the event’s locus of causality. Causes can be attributed to internal factors (e.g. ‘my manager arbitrarily decided to change the rules’) or to external factors (e.g. government standards require a change in security protocol; Heider 2013). If the cause is external, employees will be likely to hold the organisation less accountable and continue to trust it (Tomlinson and Mryer 2009).

Hence, the amount of volitional control the organisational agent is perceived to have is also a factor in making attributions for bothersome enhanced ISPs. If the organisation is seen as choosing to introduce an enhanced ISP of its own volition, employees will be more likely to see the organisation as the cause of the restricted freedom, hold it more accountable and consequently trust it less. If, however, the organisation is seen as having little control over the implementation of the enhanced ISP (e.g. following a government-mandated security protocol), employees will attribute less blame and grant more trust to the organisation going forward. As Tomlinson & Mryer (2009) proposed in their model of trust repair, negative outcomes affect future trustworthiness via attributions in the cognitive sense-making process. *Organisational trust* is defined here as 'one's expectations, assumptions, or beliefs about the likelihood that [an organisation's] future actions will be beneficial, favourable, or at least not detrimental to one's interests' (Robinson 1996, p. 576). We thus propose that upward 'could' counterfactuals will result in enhanced organisational trust.

> H11: The more employees perceive external control (i.e. upward 'could' counterfactuals) for as a result of enhanced ISPs, the greater the likelihood of increased organisational trust.

When employees perceive that ISPs restrict their freedom, their organisational trust can be undermined. Importantly, it does not matter whether these violations are objectively legal and legitimate, but whether freedom is restricted (Lowry and Moody 2014) and how legitimate or fair these restrictions are (Folger and Cropanzano 2001). Again, we posit that this rationale applies to enhanced ISPs. One's organisational trust is likely to be undermined by strong freedom restrictions because this increased lack of control conflicts with a typical employee's intrinsic motivations (Alge *et al*. 2006) as such acts are often perceived as unfair (Alge 2001) and because such acts occasion feelings of a lack of dignity, threat and exploitation (Staw *et al*. 1981). Similarly, Posey *et al*. (2011a) showed a relationship between organisational privacy invasion of employees, perceived injustice and increased CA.

Once trust is undermined, the negative results last and are exceedingly difficult to mend (Lewicki *et al*. 1998; Gillespie and Dietz 2009). Although trust repair is difficult in interpersonal relationships, it is often more difficult in an organisational context (Gillespie and Dietz 2009). As the literature on trust repair has shown, repairing broken trust, such as the result of perceived freedom violations, requires a time-consuming, transparent and direct multistage process involving the offender admitting to the wrong and trying to make amends (Lewicki *et al*. 1998; Gillespie and Dietz 2009). Thus, when freedom restrictions are the result of ongoing institutional practices and procedures – where no wrongdoing is perceived or admitted by management – organisational trust is continually undermined and attempts at repairing this trust are thwarted.

> H12: The more employees perceive freedom restrictions (i.e. negative 'would' counterfactuals) as a result of enhanced ISPs, the greater the likelihood of decreased organisational trust.

We argue that EA is driven by factors such as organisational SETA initiatives and advance notification of changes. EA has been shown to enhance perceptions of fairness because it reduces attribution of blame to supervisors for the bothersome consequences of enhanced ISPs. Information adequacy is a key aspect of interactional justice, and fairness judgments are a key predictor of organisational trust and perceived support (Alder *et al*. 2006). Employee trust will increase as management conducts activities with clear and open communication (Alder *et al*. 2006). Organisational explanations for new ISPs that employees regard as adequate, thorough, reasonable and timely are likely to be perceived as candid communication. This openness is another key facet in employees' development of trust in their organisations (Whitener *et al*. 1998). The building and maintaining of organisational trust is particularly important when introducing and changing organisational security practices such as monitoring and surveillance because these activities already tend to produce feelings of distrust (Chan 2003; Stanton and Stam 2006). Moreover, as Stanton & Stam (2006) noted, 'precipitous changes in the organisation's monitoring and surveillance policies and practices are the ones most likely to raise eyebrows and erode the trust that employees have in their organization' (p. 75). Thus, we predict

H13: The more employees perceive EA (i.e. upward 'should' counterfactuals) as a result of enhanced ISPs, the greater the likelihood of increased organisational trust.

Using organisational trust to prevent reactive CA

In summary, organisational change events such as alterations to internal security measures have the potential to negatively influence trust and subsequent behaviours (Siponen 2000; D'Arcy *et al*. 2009), yet this is a little-considered phenomenon in CA research. Notably, a key outcome of the counterfactual process in our model is organisational trust, which is an essential element in determining how employees respond to negative organisational events (Brockner *et al*. 1997). For example, the effects of employee disagreements with managers (Korsgaard *et al*. 2002), perceived psychological contract breaches (Robinson 1996) and organisational downsizing (Mishra and Spreitzer 1998) are all influenced by individual organisational trust perceptions. Hence, organisations can leverage organisational trust to enhance their security initiatives.

The organisational deviance literature has shown how trust can decrease both counterproductive (Colquitt *et al*. 2007) and antisocial (Thau *et al*. 2007) behaviours within firms. Trust influences individuals' willingness to accept the decisions made by their organisations (Rousseau and Tijoriwala 1999) and to reciprocate with organisational citizenship behaviours (Van Dyne *et al*. 2000; Korsgaard *et al*. 2002). Trust perceptions are also essential in individuals' assessments of organisational change, an area in which individuals may be more likely to perceive breaches of contract (Robinson 1996).

Employees who trust their organisation are more likely to behave beneficially towards it because they believe it is looking out for them (Korsgaard *et al*. 2002; Dirks and Ferrin 2002). Individuals who have little trust in their organisation are more likely to engage in counterproductive behaviours (Colquitt *et al*. 2007; Thau *et al*. 2007). Organisational trust exists when employees believe their organisation's actions 'will be beneficial, favourable, or at least not detrimental to one's interests' (Robinson 1996, p. 576); conversely, employees who do not experience such beliefs are more likely to engage in self-serving behaviours (Kelley and Thibault 1978) because they expect that the organisation will not act in their best interests (Thau *et al*. 2007). Thus, we predict

> H14: Employees with higher organisational trust will be less likely to engage in reactive CA than those with lower organisational trust.

RESEARCH METHODOLOGIES

Preliminary testing

A pre-test and a pilot test were performed on the survey instrument. For the pre-test, eight faculty members and doctoral students from a large Southeastern US university and one faculty member from a large Midwestern US university analysed the survey instrument for content and item wording. Following the review, minor changes were made to the survey instrument where necessary.

A pilot test was then conducted with a large bank in the Southwestern USA. In this test, 47 employees responded to the web-based survey, producing a response rate of 19% over a 1-month period. The results from the pilot test suggested no changes to item wording.

Data collection

An online panel comprising 533 full-time employees from the banking, financial and insurance industries was used to obtain data for the testing of our research model.[13] Several approaches were used to prevent common-method variance (CMV) (Podsakoff *et al*. 2003): survey items were presented in a randomised fashion; the IVs and DV were separated temporally; several measures used different scales and anchors; we designed all scales with careful wording based on existing scales and made adjustments based on feedback from academic and security experts and from the pilot test; and finally, we included a marker variable to assess CMV in order to assist in the reduction of possible common-method biases (Podsakoff *et al*. 2003). To better focus the data context, we asked respondents to answer in terms of their 'organisation's most recent ISP change'.

[13] We chose this industrial sample frame for a couple of reasons: (1) We wanted to control for some of the possible variability that may occur if we included other industries in which computer use, ethics and computer abuse might manifest differently. For example, there would likely be substantial differences between education, manufacturing, retail and financial services. (2) We also felt that the financial services industry was particularly compelling to focus on because of the ongoing ethical issues and abuses exhibited by this industry during the several years of the world financial crisis. Even today, large banks and financial services firms (e.g., HSBC, Citi, Goldman Sachs, AIG, Bank of America, etc.) are still in the process of paying hundreds of billions of dollars for their rampant abuses, and many are still in the process of being investigated.

For the survey administration, we used a third-party, online survey administration and market research company. The company has an international database of millions of prequalified potential respondents who work directly in various business fields, which allowed us to reach a large participant sample. These respondents were compensated directly by the market research firm, allowing for true anonymity.

This approach allowed us to target directly only those who met our demographic needs and to filter out everyone else automatically (Fraley 2007). Another advantage of our online panel is that data collected over the internet via a panel of respondents is more reflective of the broader population than data collected in more restricted settings (Birnbaum 2004; Fraley 2007). Moreover, an internet panel allows researchers examining topics of a sensitive nature (e.g. reactive CA) to receive responses that are less inhibited by social desirability effects because anonymity can be ensured (Bennett and Robinson 2000; Posey *et al*. 2011a).

Panel participation was restricted to those over 20 years of age who were employed full-time in US firms related to financial services. The majority (71.8%) of the respondents were between the ages of 35 and 59 years. All respondents had to use their organisation's computer systems to complete their daily work. Of the participants, 306 were female (57.4%), 223 were male (41.8%) and 4 were unreported (0.8%); 193 participants were managers (36.2%), and 77 participants worked in IT (14.4%).

Construct measurement and control variables

Appendix A summarises the information about construct measurement. All constructs were based on established measures, except for policy restrictions and advanced notification of change, which we developed. Importantly, we screened for employees familiar with their organisation's ISPs. We asked respondents whether they experienced major changes that involved increases in monitoring, increased restrictions in employee access and the like. Respondents were asked to reflect on the most recent security changes in their organisation, to describe those changes and to state why they believed the changes were necessary. Further, we asked the respondents about all the communication methods their organisations used to inform them about the changes (e.g. email, one-on-one meetings, group-based meetings, written notice). Our new variable, restrictiveness of enhanced ISP, is based on the qualitative descriptions respondents provided while completing this section of the survey.

Moreover, to test the model robustly for other potential explanations for CA, we included 14 control variables. Four of these were multi-item scales that we included in our validity analysis: *negative affectivity* and DT measures of sanction severity, certainty and celerity (D'Arcy and Devaraj 2012; D'Arcy *et al*. 2009). This approach allowed us to better determine the actual contribution to explaining CA derived from our key IVs. The remainder comprised a series of one-item control variables: professional tenure (years), organisational tenure (years), age, computer use (hours at work), education level, manager (yes/no), IT employee (yes/no), gender (male/female), income ($) and organisational size (number of employees).

ANALYSIS AND RESULTS

Before testing our model, we modelled our data based on the theoretical literature and then conducted a pre-analysis and data validation according to the latest standards for five purposes: (1) to determine whether the indicators were formative or reflective and to properly model the first-order and second-order factors; (2) to establish the factorial validity of the measures by examining convergent and discriminant validity through AVEs; (3) to establish that multicollinearity was not a problem with any of the measures; (4) to check for common-method bias; and (5) to establish reliability. Given that these procedures are well known, and for concision, we have placed the details on these in the Online Appendix C.

Summary of pre-analysis, validity and reliability

Our pre-analyses showed that our data exhibited strong factorial validity of the constructs and that they lacked mono-method bias. All our reflective constructs exhibited high levels of reliability (Fornell and Larcker 1981; Nunnally and Bernstein 1994). Table 2 summarises all the constructs' means, standard deviations (SDs) and reliability values, along with their AVEs where applicable. The results of our validation procedures showed that our data met or exceeded the validation standards expected in research (Straub *et al*. 2004), particularly for the PLS analysis of reflective constructs (Gefen and Straub 2005) and formative constructs (Diamantopoulos and Siguaw 2006; Petter *et al*. 2007; Cenfetelli and Bassellier 2009; MacKenzie *et al*. 2011).

We used PLS regression via SmartPLS version 2.0 (Ringle *et al*. 2005) for model analysis because PLS is especially adept at validating mixed models of formative and reflective indicators and because component-based structural equation modelling techniques are more appropriate for theory development than covariance-based techniques (Chin *et al*. 2003; Gefen and Straub 2005; Reinartz *et al*. 2009; Lowry and Gaskin 2014). To do so, we generated a bootstrap with 500 resamples and used the default setting of mean replacement for the missing

Table 2. Summary of construct means, standard deviations and reliabilities

Latent construct	# Items	Mean	SD	Reliability	AVE
SETA initiatives	3	5.307	1.521	0.919	0.860
EA	5	5.325	1.460	0.906	0.781
Organisational trust	7	5.191	1.239	0.894	0.618
Freedom restrictions	5	2.886	1.353	0.850	0.640
GDT: Severity of sanctions	4	4.821	1.436	0.911	0.788
GDT: Certainty of sanctions	7	4.381	1.303	0.768	0.363
GDT: Celerity of sanctions	4	4.701	1.327	0.888	0.721
CA (composite measure)	9	1.578	1.078	0.969	0.761
Negative affect (formative measure)	10	2.465	0.996	n/a	n/a
External control	3	3.162	1.784	0.936	0.831
Advance notification (yes/no)	1	0.520	0.500	n/a	n/a
Restrictiveness of enhanced ISP (0 to 3)	1	1.750	0.817	n/a	n/a

Both advance notification and ISP restrictiveness were single-item measures for which reliability and AVE cannot be computed.

values algorithm. Table 3 summarises our measurement model statistics. Figure 2 summarises the testing of the theoretical paths in the model, along with the five control variables that were significant. The variance explained is indicated for each construct as R^2. Table 4 summarises the hypotheses, the path coefficients and the *t*-values for each path.

Mediation analysis

To verify whether organisational trust plays a role as a partial mediator in the model as we predicted, we used Sobel analysis and augmented it with standard errors (SEs) calculated from bootstrapping in PLS to overcome some of the natural limitations of Sobel analysis, as described by Lowry & Gaskin (2014). We ruled out considering the mediation relationships with

Table 3. Latent variable correlations and square roots of AVEs for constructs

Latent construct	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)
Negative affect (1)	n/a									
SETA (2)	−0.090	0.927								
External control (3)	0.195	−0.095	0.911							
EA (4)	−0.096	0.391	−0.161	0.884						
GDT: Certainty (5)	0.082	0.251	0.062	0.081	0.623					
GDT: Severity (6)	−0.030	0.327	−0.067	0.221	0.609	0.878				
GDT: Celerity (7)	−0.044	0.326	−0.044	0.346	0.579	0.802	0.849			
Organisational trust (8)	−0.239	0.463	−0.126	0.541	−0.017	0.188	0.276	0.786		
Freedom restrictions (9)	0.280	−0.252	0.202	−0.451	0.216	0.014	−0.031	−0.657	0.800	
CA (10)	0.332	−0.179	0.139	−0.227	0.022	−0.095	−0.079	−0.371	0.394	0.872

AVE square roots are represented as bold and underlined diagonal elements; off-diagonal elements represent the correlations between constructs; AVEs could not be computed for negative affect because it is a formative measure.

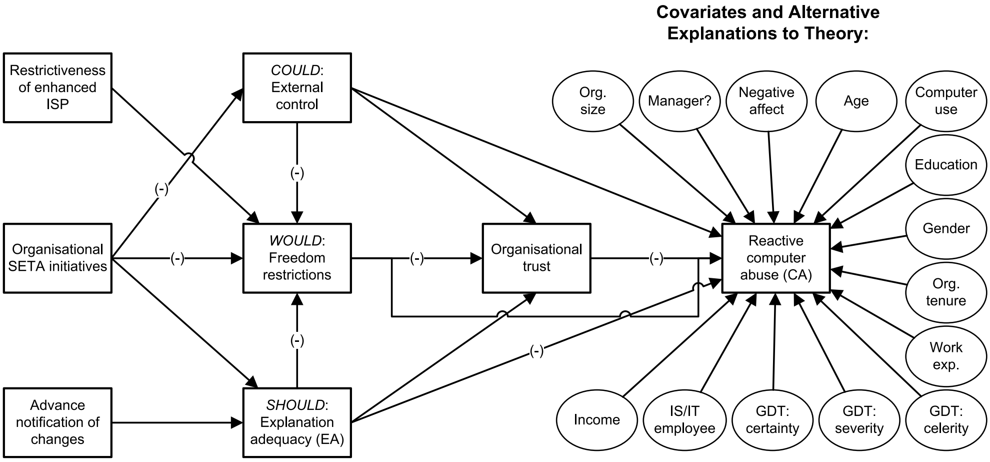
Covariates and Alternative Explanations to Theory:
Restrictiveness of enhanced ISP
COULD: External control
Organisational SETA initiatives
WOULD: Freedom restrictions
Organisational trust
Reactive computer abuse (CA)
Advance notification of changes
SHOULD: Explanation adequacy (EA)
(-)
Org. size
Manager?
Negative affect
Age
Computer use
Education
Gender
Org. tenure
Work exp.
Income
IS/IT employee
GDT: certainty
GDT: severity
GDT: celerity

Figure 2. Model testing results.

Table 4. Summary of path coefficients and significance levels (*n* = 533)

Tested model paths	(β)	*t*-statistic	Supported?
Tested hypothesis relationships			
H1. Restrictiveness of enhanced ISP →Freedom restrictions (downward 'would')	0.064	2.052*	Yes
H2. SETA initiatives→(–) External control (upward 'could')	(−0.099)	2.503*	Yes
H3. SETA initiatives → (–) Freedom restrictions (downward 'would')	(−0.091)	2.513*	Yes
H4. SETA initiatives → EA (upward 'should')	0.325	8.798***	Yes
H5. Advance notification → EA (upward 'should')	0.240	7.977***	Yes
H6. External control (upward 'could') → (–) Freedom restrictions (downward 'would')	0.129	3.611***	Yes; reverse
H7. EA (upward 'should') → (–) Freedom restrictions (downward 'would')	(−0.390)	10.227***	Yes
H8. Freedom restrictions (downward 'would' → Reactive CA	0.159	4.251***	Yes
H9. External control (upward 'could') → (–) Reactive CA	(−0.018)	0.663 (n/s)	No
H10. EA (upward 'should') → (-) Reactive CA	(−0.023)	0.604 (n/s)	No
H11. External control (upward 'could') → Organisational trust	0.027	1.052 (n/s)	No
H12. Freedom restrictions (downward 'would' → (–) Organisational trust	(−0.508)	16.066***	Yes
H13. EA (upward 'should') → Organisational trust	0.334	9.844***	Yes
H14. Organisational trust → (–) Reactive CA	(−0.117)	3.222**	Yes
Control variables			
Organisational size → Reactive CA	(−0.044)	1.315 (n/s)	No
Manager → Reactive CA	0.092	2.869**	Yes
Negative affect → Reactive CA	0.300	7.074***	Yes
Age → Reactive CA	(−0.169)	4.989***	Yes
Computer use at work → Reactive CA	(−0.134)	3.566***	Yes
Education → Reactive CA	(−0.012)	0.425 (n/s)	No
Gender → Reactive CA	(−0.071)	2.178*	Yes
Organisational tenure → Reactive CA	0.052	1.883 (n/s)	No
Work experience → Reactive CA	(−0.027)	0.910 (n/s)	No
GDT: Celerity of sanctions → Reactive CA	0.056	1.086 (n/s)	No
GDT: Severity of sanctions → Reactive CA	(−0.080)	1.775 (n/s)	No
GDT: Certainty of sanctions → Reactive CA	0.066	0.856 (n/s)	No
IS/IT employee → Reactive CA	0.030	0.831 (n/s)	No
Income → Reactive CA	(−0.025)	0.617 (n/s)	No

n/s = not significant.
*$p < 0.05$; **$p < 0.01$; ***$p < 0.001$.

external control and EA because both of these started with no significant relationship with reactive CA when the mediator (organisational trust) was not present. By contrast, freedom restrictions had a highly significant direct relationship with reactive CA when organisational trust was not included in the model (β = 0.217, *t* = 6.289). When the mediator of organisational trust was included in the model, the direct relationship between freedom restrictions and reactive CA remained significant but dropped in magnitude (β = 0.159, *t* = 4.250).

Given this foundation, we used bootstrapping to gather the needed SE for the path between freedom restrictions and organisational trust (SE = 0.031614) and the path between organisational trust and reactive CA (SE = 0.036416). Using the beta coefficients and these

SEs yielded a Sobel test statistic of $z = -2.708$, with a two-tailed probability of 0.007. Given the drop in the magnitude of the original beta coefficient for the path between freedom restrictions and reactive CA, the Sobel test statistic is statistically significant evidence that organisational trust indeed acts as a partial mediator in our model.

DISCUSSION

The results of our study show substantial support for FT and RT and organisational trust in explaining reactive CA in response to new restrictive ISPs. Most of our hypothesised relationships were supported. Organisational trust was shown to be a major driver that can decrease reactive CA within organisations (H14 supported). EA provides an upward 'should' counterfactual, which thereby builds organisational trust (H13 supported). We had previously envisioned EA as a parallel driver that decreases CA (H10 rejected), but our results showed that, instead, EA is a major driver of organisational trust, and this trust both fully mediates the relationship between EA and CA and partially mediates the relationship between freedom restrictions and reactive CA. However, EA and its related fairness perceptions remain crucial to our model because of its strong positive relationship with organisational trust.

Regarding other forms of counterfactual reasoning, perceived freedom restrictions related to enhanced ISPs directly undermined organisational trust (H12 supported) and increased reactive CA (H8 supported). EA also had a strong negative relationship with freedom restrictions (H7 supported). As expected, the more restrictive the enhanced ISPs were perceived to be by employees, the higher the perception of freedom restrictions (H1 supported). Likewise, organisational SETA initiatives decreased perceptions of external control (H2 supported) and freedom restrictions (H3 supported) and increased EA (H4 supported). Finally, advance notification of changes in ISPs increased EA (H5 supported).

To test the robustness of our predictions, we included 14 control variables and rival explanations to determine with more confidence what drove reactive CA in our context. Most notably, the GDT-based constructs of sanction severity, certainty and celerity had no significant influence on reactive CA. We believe that including the GDT items was particularly useful because GDT has previously been purported to decrease CA (D'Arcy *et al*. 2009; D'Arcy and Devaraj 2012) but has not been studied with organisational trust and EA. Our findings concur with extant research indicating that sanctions may be less influential in preventing CA than more salient individual and organisational factors.

Our study had two other interesting control variable results. First, those who had negative affect towards their organisations reported more reactive CA after the enhanced ISPs were implemented, as did managers. Second, those who were older, more experienced with computers and female were less likely to commit reactive CA.

In terms of unsupported results, external control had no influence on organisational trust (H11 rejected) or on reactive CA (H9 rejected). More curious was that the relationship between external control and freedom restrictions was positive but not in the predicted negative direction (H6 significant but in the wrong direction). However, based on this evidence alone, we cannot interpret these results as a direct rejection of upward 'could' counterfactuals in our context.

Instead, we believe external control itself could be less positive for counterfactuals in an ISP context than FT would otherwise maintain. In a context of freedom restrictions from ISPs, it could be the case that the origin of the rules in the government or other external sources does not represent a mental relief for employees but instead heightens the perception that people outside the organisation could be involved in overseeing one's data, thus increasing the perception of freedom restrictions. Researchers need to consider this possibility to determine whether it is possible to create upward 'could' counterfactuals in organisational ISPs contexts.

Implications for research and practice

Notwithstanding the external control results, the overall results of our study make a strong case for our RT- and FT-based research model and for the conclusion that organisations can improve or undermine their overall ISP efforts simply by how respectfully and fairly they treat their employees with respect to rolling out enhanced ISPs.

In addition to the related justice theory (e.g. Xue *et al*. 2011), FT provides a particularly interesting theoretical contribution to the literature. The distinction is that FT emphasises the formation of blame attributions based on counterfactuals, whereas justice theory presumes that blame *has already occurred*. Our paper is clearly in the former camp. Notably, if an insider perceives that the increases (1) were due to external factors, (2) do not cause personal harm, and/or (3) are well explained such that he or she can easily grasp the principles upon which the security efforts were based, then the insider cannot reasonably assign blame to the organisation for its actions. If no blame is assigned to the organisation by the insider, reactive CA should be unlikely. However, if blame is assigned, reactive CA is more likely. Thus, rather than assuming that all enhanced ISPs will be perceived as negative or unjust by employees, we argue that it is the combination of all three counterfactuals that best engenders reactance. FT thus builds on procedural and interactional justice to demonstrate that even when ISPs are administered inconsistently or employees perceive being treated disrespectfully, they may still perceive fairness depending on how blame for the event is assigned.

The study also empirically validates the importance of SETA programmes for organisations in developing and implementing ISPs. We show that SETA is not just useful for teaching employees what not to do concerning ISPs but it also provides them with a knowledge foundation that increases their perception of EA. As a corollary, insiders are more likely to perceive changes in ISPs as unfair and capricious when they do not understand the foundation and the reasons for these ISPs.

What this means in practice is that SETA programmes built on the *what*, *how* and *why* comparative framework suggested by security researchers (Whitman and Mattord 2009) serve at least two main functions: (1) the programmes provide the foundation from which insiders can better gauge organisational communication efforts regarding security initiatives, and (2) the programmes build the organisational trust beliefs of insiders because they demonstrate the competence and/or the benevolence of the organisation. Inconsistent communication received by insiders could be detrimental to the effectiveness of the information security initiatives. SETA programmes thus can be useful in neutralising the natural organisational blame predicted by FT.

Likewise, providing advance notification is a respectful and helpful method for managers to use (Folger and Cropanzano 2001) because it allows enhanced ISPs to be more thoroughly understood and supported. These results imply how important communication about ISPs is to employees. Employees whose organisations make the effort to discuss ISP changes prior to their implementation should perceive a greater degree of EA than those who are informed after the fact. This action, which appears to be underestimated or overlooked by many firms (i.e. a surprising 41% of our sample), strongly relates to the variance exhibited of EA.

Limitations and future research

The results of our analysis of the exploratory control variables point to several limitations of our study as well as to several research opportunities. First, counter explanations and other theories remain untested. Future research could explore, for example, the relationship between our model and covariates from justice theory (Xue *et al*. 2011), the elaboration likelihood model (Lowry *et al*. 2012) and other models. Second, our data provide strong indications that employees who have high negative affectivity are more likely to commit CA than those with low negative affectivity. Although we have offered no theoretical basis for this link, the results are relatively unsurprising because they are consistent with the organisational deviance literature (e.g. Robinson and Bennett 1995; Robinson and Greenberg 1998). This pathway displays an alarming strength in our model: it has a stronger beta coefficient than the counterinfluence of organisational trust. This result suggests that negative affectivity and CA can be combined to play an especially pernicious role in organisations. If true, then several issues emerge concerning what can be carried out to screen out employees with high negative affectivity during the hiring process or to reform the negative attitudes of existing employees. These possibilities raise serious human resource management concerns.

The exploratory results showing that age and computer use have strong negative effects on CA are also interesting and deserve more attention. At first glance, one might be tempted to conclude that the negative link with age relates to maturity. This could be the case, but two other possibilities should be considered in future research. It could be that these are simply predictors of organisational commitment, which could be an outcome of procedural justice (Mirchandani and Lederer 2014); thus, organisational commitment is a factor that should be considered in future models. A second, troubling counter explanation is that the growing younger generation is more prone to CA. If true, this would be an alarming security trend. The negative link with heavy computer use at work is also curious. It is possible that heavier computer users are more committed to their jobs or simply understand ISPs better than average employees and thus are more trusting of organisational efforts concerning ISPs. Another possibility is that heavy computer users are busier and less prone to the idleness that is necessarily involved in many forms of CA. All these possibilities deserve further exploration.

There are also several limitations and opportunities related to the development and testing of our model. Although the EA is central to our study and FT, we did not control for how this information was actually provided to insiders. Organisations may choose from a variety of explanation delivery methods (e.g. face-to-face communication, group involvement and email). These methods might moderate the influence of EA on trust following security enhancements

(Shapiro *et al*. 1994). Hence, a computer-mediated communication study that experimentally controls for the method of communication would be a valuable addition to this body of research. Because our theory is causal but our current study is not, this would provide a valuable test of the true causal nature of the theory.

We also believe that a similar, important research effort would be to determine how the approaches utilised in organisational SETA programme efforts influence insiders' perceptions of EA and beliefs about ISPs. Specifically, research has shown that the manner in which messages are framed can significantly affect their intended outcomes (Shropshire *et al*. 2010; Barlow *et al*. 2013). These possibilities require further investigation.

Another limitation is that our context involved full-time working employees in the USA. It is highly likely that the key constructs involved in determining EA (i.e. fairness, organisational trust, freedom restrictions and so forth) could be influenced by cultural differences. Little cross-cultural organisational security research has been conducted, yet it is a highly promising area of inquiry (Crossler *et al*. 2013). In other computing contexts, US employees have been shown to be highly individualistic, valuing individual freedom of choice at work more than employees in collectivistic societies, such as in China (e.g. Zhang *et al*. 2007; Dinev *et al*. 2009; Lowry *et al*. 2010b; Avison *et al*. 2011). The unique Chinese cultural construct of *guanxi* (i.e. special connections of power, trust and favour granting in Chinese business culture) is also a compelling consideration that might be even more salient in studying Chinese organisations (Martinsons 2008; Huang *et al*. 2011).

Finally, although our theory proposes causation and temporal precedence, survey data cannot control well for time and cannot establish causation. We asked for the respondents' current perceptions and current/recent CA behaviours. Only longitudinal data or experimentation can empirically establish the temporal order of these factors. Likewise, we were unable to ensure that all our respondents had experienced similar organisational disincentives within similar periods. Rather, our findings represent the expressions of individuals from various organisational environments and internal security cultures. This fact, however, gives our study greater generalisability because of the broad nature of the sample and the respondents' organisational experiences. However, with regard to the links between specific disincentives and behaviours, longitudinal or experimental research would be illuminating.

CONCLUSIONS

Although organisations devote many resources (e.g. financial and human capital) to security programmes and activities, some of these activities backfire into reactive CA because organisations do not properly consider their employees in the security equation. To shed light on this issue, we used RT and FT to explain the factors influencing employees' reactive CA that occurs from enhanced restrictive ISPs. To test the robustness of our predictions, we included 14 control variables and rival explanations to determine with greater confidence what drove reactive CA in our context. Most notably, the GDT-based constructs of sanction severity, certainty and celerity had no significant influence on reactive CA. Our results thus largely support the efficacy of applying FT to explain reactive CA in organisations in the context of enhanced ISPs.

ACKNOWLEDGEMENTS

We greatly appreciate Rob Folger for providing extensive feedback on this study and manuscript; particularly for his insights on how to best implement FT in an organisational security context involving reactive CA.

REFERENCES

Alder, G.S., Ambrose, M.L. & Noel, T.W. (2006) The effect of formal advance notice and justification on Internet monitoring fairness: much about nothing? *Journal of Leadership and Organizational Studies*, **13**, 93–108.

Alge, B.J. (2001) Effects of computer surveillance on perceptions of privacy and procedural justice. *Journal of Applied Psychology*, **86**, 797–804.

Alge, B.J., Ballinger, G.A., Tangirala, S. & Oakley, J.L. (2006) Information privacy in organizations: empowering creative and extrarole performance. *Journal of Applied Psychology*, **91**, 221–232.

Ambrose, M.L., Seabright, M.A. & Schminke, M. (2002) Sabotage in the workplace: the role of organizational injustice. *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.

Avison, D., Fitzgerald, G. & Powell, P. (2011) Editorial. *Information Systems Journal*, **21**, 477–478.

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.

Bennett, R.J. (1998) Perceived powerlessness as a cause of employee deviance. In: Dysfunctional Behavior in Organizations: Violent and Deviant Behavior, Griffin, R.W., O'Leary-Kelly, A.M. & Collins, J.M. (eds.), pp. 221–239. JAI Press, Stamford, CT.

Bennett, R. J. & Robinson, S.L. (2000) Development of a measure of workplace deviance. *Journal of Applied Psychology*, **85**, 349–360.

Birnbaum, M.H. (2004) Human research and data collection via the Internet. *Annual Review of Psychology*, **55**, 803–832.

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

Brehm, J.W. (1966) A Theory of Psychological Reactance. Academic Press, New York, NY.

Brehm, S.S. & Brehm, J.W. (1981) Psychological Reactance: A Theory of Freedom and Control. Academic Press, New York, NY.

Brenner, B. (2009) Global state of information security survey 2010. *CIOMagazine*, *CSOMagazine*, *and PricewaterhouseCoopers*, Retrieved date: March 21, 2013. URL: http://nouvelstrategies.com/E/Management-Awareness/Entries/2010/4/1_PWC_Global_State_of_Information_Security_2010.html

Brockner, J., Konovsky, M., Cooper-Schneider, R., Folger, R., Martin, C. & Bies, R.J. (1994) Interactive effects of procedural justice and outcome negativity on victims and survivors of job loss. *Academy of Management Journal*, **37**, 397–409.

Brockner, J., Siegel, P.A., Daly, J.P., Tyler, T. & Martin, C. (1997) When trust matters: the moderating effect of outcome favorability. *Administrative Science Quarterly*, **42**, 558–583.

Cenfetelli, R.T. & Bassellier, G. (2009) Interpretation of formative measurement in information systems research. *MIS Quarterly*, **33**, 689–707.

Chan, M. (2003) Corporate espionage and workplace trust/distrust. *Journal of Business Ethics*, **42**, 45–58.

Chan, R.Y.K. & Lai, J.W.M. (2011) Does ethical ideology affect software piracy attitude and behaviour? An empirical investigation of computer users in China. *European Journal of Information Systems*, **20**, 659–673.

Chen, Y., Ramamurthy, K.R. & Wen, K.-W. (2013) Organizations' information security policy compliance: stick or carrot approach? *Journal of Management Information Systems*, **29**, 157–188.

Cheng, L., Li, Y., Li, W., Holm, E. & Zhai, Q. (2013) Understanding the violation of IS security policy in organizations: an integrated model based on social control and deterrence theory. *Computers & Security*, **39**, 447–459.

Chin, W.W., Marcolin, B.L. & Newsted, P.R. (2003) A partial least squares latent variable modeling approach for measuring interaction effects: results from a Monte Carlo simulation study and an electronic-mail emotion/ adoption study. *Information Systems Research*, **14**, 189–217.

Colquitt, J.A. (2001) On the dimensionality of organizational justice: a construct validation of a measure. *Journal of Applied Psychology*, **86**, 386–400.

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

Colquitt, J.A. & Rodell, J.B. (2011) Justice, trust, and trustworthiness: a longitudinal analysis integrating three theoretical perspectives. *Academy of Management Journal*, **54**, 1183–1206.

Colquitt, J.A., Scott, B.A. & LePine, J.A. (2007) Trust, trustworthiness, and trust propensity: a meta-analytic test of their unique relationships with risk taking and job performance. *Journal of Applied Psychology*, **92**, 909–926.

Crossler, R.E. & Belanger, F. (2009) The effects of security education training and awareness programs and individual characteristics on end user security tool usage. *Journal of Information System Security*, **5**, 3–22.

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

D'Arcy, J. & Devaraj, S. (2012) Employee misuse of information technology resources: testing a contemporary deterrence model. *Decision Sciences*, **43**, 1091–1124.

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., 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.

D'Arcy, J. & Hovav, A. (2007) Towards a best fit between organizational security countermeasures and information systems misuse behaviors. *Journal of Information System Security*, **3**, 3–30.

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

Dhillon, G. & Torkzadeh, G. (2006) Value-focused assessment of information system security in organizations. *Information Systems Journal*, **16**, 293–314.

Diamantopoulos, A. & Siguaw, J. A. (2006) Formative versus reflective indicators in organizational measure development: a comparison and empirical illustration. *British Journal of Management*, **17**, 263–282.

Dinev, T., Goo, J., Hu, Q. & Nam, K. (2009) User behaviour towards protective information technologies: the role of national cultural differences. *Information Systems Journal*, **19**, 391–412.

Dirks, K.T. & Ferrin, D.L. (2002) Trust in leadership: meta-analytic findings and implications for research and practice. *Journal of Applied Psychology*, **87**, 611–628.

Fitzgerald, T.C., Coins, B.C. & Herold, R.C. (2006) Information security and risk management. In: Official (ISC) 2 Guide to the CISSP CBK, Tipton, H. F. & Henry, K. (eds.), pp. 1–92. Auerbach, Clearwater, FL.

Folger, R. & Cropanzano, R. (1998) Organizational Justice and Human Resource Management. Sage Publications, Thousand Oaks, CA.

Folger, R. & Cropanzano, R. (2001) Fairness theory: justice as accountability. In: Advances in Organizational Justice, Greenberg, J. & Cropanzano, R. (eds.), pp. 1–55. Stanford University Press, Stanford, CA.

Folger, R., Konovsky, M.A. & Cropanzano, R. (1992) A due process metaphor for performance appraisal. In: Research in Organizational Behavior, Staw, B. M. & Cummings, L. L. (eds.), pp. 129–177. JAI Press, Greenwich, CT.

Fornell, C. & Larcker, D.F. (1981) Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, **18**, 39–50.

Fox, S., Spector, P.E. & Miles, D. (2001) Counterproductive work behavior (CWB) in response to job stressors and organizational justice: some mediator and moderator tests for autonomy and emotions. *Journal of Vocational Behavior*, **59**, 291–309.

Fraley, R.C. (2007) Using the Internet for personality research: what can be done, how to do it, and some concerns. In: Handbook of Research Methods in Personality Psychology, Robins, R.W., Fraley, R.C. & Krueger, R.F. (eds.), pp. 130–148. Guilford, New York, NY.

Furnell, S.M., Jusoh, A. & Katsabas, D. (2006) The challenges of understanding and using security: a survey of end-users. *Computers and Security*, **25**, 27–35.

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

Gillespie, N. & Dietz, G. (2009) Trust repair after an organization-level failure. *Academy of Management Review*, **34**, 127–145.

Gilliland, S.W., Groth, M., Baker, R. C., Dew, A.E., Polly, L.M. & Langdon, J.C. *et al*. (2001) Improving applicants' reactions to rejection letters: an application of fairness theory. *Personnel Psychology*, **54**, 669–703.

Goode, S. & Cruise, S. (2006) What motivates software crackers? *Journal of Business Ethics*, **65**, 173–201.

Greenberg, J. (1990) Employee theft as a reaction to underpayment inequity: the hidden cost of pay cuts. *Journal of Applied Psychology*, **75**, 561–568.

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

Guo, K.H. (2013) Security-related behavior in using information systems in the workplace: a review and synthesis. *Computers and Security*, **32**, 242–251.

Gurung, A., Luo, X. & Liao, Q. (2009) Consumer motivations in taking action against spyware: an empirical investigation. *Journal of Information Management and Computer Security*, **17**, 276–289.

Hansen, J. & Walden, E. (2013) The role of restrictiveness of use in determining ethical and legal awareness of unauthorized file sharing. *Journal of the Association for Information Systems*, **14**, 521–549.

Heider, F. (2013) The Psychology of Interpersonal Relations. Psychology Press, New York, NY.

Herath, T. & Rao, H.R. (2009a) Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, **47**, 154–165.

Herath, T. & Rao, H.R. (2009b) Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, **18**, 106–125.

Higgins, G., Wilson, A. & Fell, B. (2005) An application of deterrence theory to software piracy. *Journal of Criminal Justice and Popular Culture*, **12**, 166–184.

Higgins, G.E. (2004) Can low self-control help with the understanding of the software piracy problem? *Deviant Behavior*, **26**, 1–24.

Hollinger, R.C. (1993) Crime by computer: correlates of software piracy and unauthorized account access. *Security Journal*, **4**, 2–12.

Hovav, A. & D'Arcy, J. (2012) Applying an extended model of deterrence across cultures: an investigation of information systems misuse in the US and South Korea. *Information and Management*, **49**, 99–110.

Hovorka-Mead, A.D., Ross Jr., W.H., Whipple, T. & Renchin, M.B. (2002) Watching the detectives: seasonal student employee reactions to electronic monitoring with and without advance notification. *Personnel Psychology*, **55**, 329–362.

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.

Huang, Q., Davison, R.M. & Gu, J. (2011) The impact of trust, guanxi orientation and face on the intention of Chinese employees and managers to engage in peer-to-peer tacit and explicit knowledge sharing. *Information Systems Journal*, **21**, 557–577.

Ifinedo, P. (2012) Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory. *Computers and Security*, **31**, 83–95.

Jaworski, B.J. & MacInnis, D.J. (1989) Marketing jobs and management controls: toward a framework. *Journal of Marketing Research*, **26**, 406–419.

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

Kankanhalli, A., Teo, H.-H., Tan, B.C.Y. & Wei, K.-K. (2003) An integrative study of information systems security effectiveness. *International Journal of Information Management*, **23**, 139–154.

Kelley, H.H. & Thibault, J. (1978) Interpersonal Relations: A Theory of Interdependence. Wiley, New York, NY.

Kernan, M.C. & Hanges, P.J. (2002) Survivor reactions to reorganization: antecedents and consequences of procedural, within-group, and informational justice. *Journal of Applied Psychology*, **87**, 916–928.

Korsgaard, M.A., Brodt, S.E. & Whitener, E.M. (2002) Trust in the face of conflict: the role of managerial trustworthy behavior and organizational context. *Journal of Applied Psychology*, **87**, 312–319.

Lee, S.M., Lee, S.G. & Yoo, S. (2004) An integrative model of computer abuse based on social control and general deterrence theories. *Information and Management*, **41**, 707–718.

Lewicki, R.J., McAllister, D.J. & Bies, R.J. (1998) Trust and distrust: new relationships and realities. *Academy of Management Review*, **23**, 438–458.

Li, H., Zhang, J. & Sarathy, R. (2010) Understanding compliance with internet use policy from the perspective of rational choice theory. *Decision Support Systems*, **48**, 635–645.

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

Lind, E.A. & van den Bos, K. (2002) When fairness works: toward a general theory of uncertainty management. *Research in Organizational Behavior*, **24**, 181–223.

Loch, K.D., Carr, H.H. & Warkentin, M. (1992) Threats to information systems: today's reality, yesterday's understanding. *MIS Quarterly*, **16**, 173–186.

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

Lowry, P.B. & Moody, G.D. (2014) Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organizational information security policies. *Information Systems Journal*, **forthcoming**.

Lowry, P.B., Moody, G.D., Vance, A., Jensen, M., Jenkins, J.L. & Wells, T., et al (2012) Using an elaboration likelihood approach to better understand the persuasiveness of website privacy assurance cues for online consumers. *Journal of the American Society for Information Science and Technology*, **63**, 755–766.

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

Lowry, P.B., Teh, N., Molyneux, B. & Bui, S.N. (2010a) Using theories of formal control, mandatoriness, and reactance to explain working professionals' intent to comply with new IT security policies. *The Dewald Roode Workshop on Information Systems Security Research, IFIP WG8.11/WG11.n, 2010*, pp. 278–316. IFIP WG 8.11 / 11.13, October 8–9, Waltham, MA.

Lowry, P.B., Zhang, D., Zhou, L. & Fu, X. (2010b) Effects of culture, social presence, and group composition on trust in technology-supported decision-making groups. *Information Systems Journal*, **20**, 297–315.

MacKenzie, S.B., Podsakoff, P.M. & Podsakoff, N.P. (2011) Construct measurement and validation procedures in MIS and behavioral research: integrating new and existing techniques. *MIS Quarterly*, **35**, 293–334.

Martinsons, M.G. (2008) Relationship-based e-commerce: theory and evidence from China. *Information Systems Journal*, **18**, 331–356.

Mirchandani, D.A. & Lederer, A.L. (2014) Autonomy and procedural justice in strategic systems planning. *Information Systems Journal*, **24**, 25–59.

Mishra, A.K. & Spreitzer, G.M. (1998) Explaining how survivors respond to downsizing: the roles of trust, empowerment, justice, and work redesign. *Academy of Management Review*, **23**, 567–588.

Mitchell, M.S. & Ambrose, M.L. (2007) Abusive supervision and workplace deviance and the moderating effects of negative reciprocity beliefs. *Journal of Applied Psychology*, **92**, 1159–1168.

Moody, G.D. & Siponen, M. (2013) Using the theory of interpersonal behavior to explain non-work-related personal use of the Internet at work. *Information and Management*, **50**, 322–335.

Moore, A.P., Cappelli, D.M. & Trzeciak, R.F. (2008) The 'Big Picture' of Insider IT Sabotage Across U.S. Critical Infrastructures, pp. 17–52. Software Engineering Institute: Carnegie Mellon University, Pittsburgh, PA.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T. & Vance, A. (2009) What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems*, **18**, 126–139.

Nunnally, J.C. & Bernstein, I.H. (1994) Psychometric Theory. McGraw-Hill, New York, NY.

Paternoster, R. (1987) The deterrent effect of the perceived certainty and severity of punishment: a review of the evidence and issues. *Justice Quarterly*, **4**, 173–217.

Paternoster, R. (1989) Decision to participate in and desist from four types of common delinquency: deterrence and the rational choice perspective. *Law and Society Review*, **23**, 7–40.

Paternoster, R. & Simpson, S. (1996) Sanction threats and appeals to morality: testing a rational choice model of corporate crime. *Law and Society Review*, **30**, 549–584.

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

Peterson, D. (2011) Deltek: Cybersecurity spending should grow. Retrieved date: June 6, 2012, URL: http://www.washingtonpost.com/business/capitalbusiness/deltek-cybersecurity-spending-should-grow/2011/12/05/gIQApTQtiO_story.html

Petter, S., Straub, D.W. & Rai, A. (2007) Specifying formative constructs in information systems research. *MIS Quarterly*, **31**, 623–656.

Phau, I. & Ng, J. (2010) Predictors of usage intentions of pirated software. *Journal of Business Ethics*, **94**, 23–37.

Podsakoff, P.M., MacKenzie, S.B., Lee, J.Y. & Podsakoff, N. P. (2003) Common method biases in behavioral research: a critical review of the literature and recommended remedies. *Journal of Applied Psychology*, **88**, 879–903.

Ponemon Institute (2014) 2014 cost of data breach study: global analysis. *Ponemon Institute and IBM*, *May 2014*, *pp.1–28.*, Retrieved date: November 20, 2014, URL: http://www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/

Popham, J. (2011) Factors influencing music piracy. *Journal of Criminal Justice Studies*, **24**, 199–209.

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

Posey, C., Bennett, R.J. & Roberts, T.L. (2011b) Understanding the mindset of the abusive insider: an examination of insiders' causal reasoning following internal security changes. *Computers and Security*, **30**, 486–497.

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

PRC (2013) Chronology of data breaches security breaches 2005–present. Retrieved date: November 4, 2014, URL: http://www.privacyrights.org/data-breach

PWC (2015) The Global State of Information Security Survey 2015. *PricewaterhouseCoopers*, Retrieved date: November 4, 2014, URL: http://www.pwc.com/gx/en/consulting-services/information-security-survey/

Reinartz, W., Haenlein, M. & Henseler, J. (2009) An empirical comparison of the efficacy of covariance-based and variance-based SEM. *International Journal of Research in Marketing*, **26**, 332–344.

Ringle, C.M., Wende, S. & Will, S. (2005) SmartPLS 2.0 (M3) Beta. Retrieved date: September 17, 2010, URL: http://www.smartpls.de

Rivera, J. & van der Meulen, R. (2014) Gartner says worldwide security market to grow 8.7 percent in 2015. *Gartner*, Retrieved date: November 12, 2014, URL: http://www.gartner.com/newsroom/id/2512215

Robinson, S.L. (1996) Trust and breach of the psychological contract. *Administrative Science Quarterly*, **41**, 574–599.

Robinson, S.L. & Bennett, R.J. (1995) A typology of deviant workplace behaviors: a multidimensional scaling study. *Academy of Management Journal*, **38**, 555–572.

Robinson, S.L. & Greenberg, J. (1998) Employees behaving badly: dimensions, determinants and dilemmas in the study of workplace deviance. In: Trends in Organizational Behavior, Rousseau, D.M. & Cooper, C.L. (eds.), pp. 1–30. Wiley, New York, NY.

Robinson, S.L. & O'Leary-Kelly, A.M. (1998) Monkey see, monkey do: the influence of work groups on the antisocial behavior of employees. *Academy of Management Journal*, **41**, 658–672.

Rousseau, D.M. & Tijoriwala, S.A. (1999) What's a good reason to change? Motivated reasoning and social accounts in promoting organizational change. *Journal of Applied Psychology*, **84**, 514–528.

Shapiro, D.L., Buttner, E.H. & Barry, B. (1994) Explanations: what factors enhance their perceived adequacy? *Organizational Behavior and Human Decision Processes*, **58**, 346–368.

Shaw, J.C., Wild, E. & Colquitt, J.A. (2003) To justify or excuse?: A meta-analytic review of the effects of explanations. *Journal of Applied Psychology*, **88**, 444–458.

Shropshire, J., Warkentin, M. & Johnston, A.C. (2010) Impact of negative message framing on security adoption. *Journal of Computer Information Systems*, **51**, 41–51.

Siponen, M. (2000) A conceptual foundation for organizational information security awareness. *Information Management and Computer Security*, **8**, 31–41.

Siponen, M., Mahmood, M.A. & Pahnila, S. (2009) Are employees putting your company at risk by not following information security policies? *Communications of the ACM*, **52**, 145–147.

Siponen, M., Pahnila, S. & Mahmood, M.A. (2010) Compliance with information security policies: an empirical investigation. *IEEE Computer*, **43**, 64–71.

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

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

Stanton, J.M. & Stam, K.R. (2006) The Visible Employee: Using Workplace Monitoring and Surveillance to Protect Information Assets – Without Compromising Employee Privacy or Trust. Information Today, Inc., Medford, NJ.

Staw, B.M., Sandelands, L.E. & Dutton, J.E. (1981) Threat rigidity effects in organizational behavior: a multilevel analysis. *Administrative Science Quarterly*, **26**, 501–524.

Straub, D.W. (1990) Effective IS security. *Information Systems Research*, **1**, 255–276.

Straub, D.W., Boudreau, M.C. & Gefen, D. (2004) Validation guidelines for IS positivist research. *Communications of the Association for Information Systems*, **13**, 380–427.

Straub, D.W. & Nance, W.D. (1990) Discovering and disciplining computer abuse in organizations: a field study. *MIS Quarterly*, **14**, 45–60.

Thau, S., Crossley, C., Bennett, R.J. & Sczesny, S. (2007) The relationship between trust, attachment, and antisocial work behaviors. *Human Relations*, **60**, 1155–1179.

Tomlinson, E.C. & Mryer, R.C. (2009) The role of causal attribution dimensions in trust repair. *Academy of Management Review*, **34**, 85–104.

Ugrin, J.C., Pearson, J.M. & Odom, M.D. (2008) Cyberslacking: self-control, prior behavior and the impact of deterrence measures. *Review of Business Information Systems*, **12**, 75–87.

Ugrin, J.C. & Pearson, M.J. (2013) The effects of sanctions and stigmas on cyberloafing. *Computers in Human Behavior*, **29**, 812–820.

US Dept. of Labor (2009) Other workplace standards: notices for plant closings and mass layoffs. *U.S. Department of Labor*, Retrieved date: February 12, 2013, URL: http://www.dol.gov/compliance/guide/layoffs.htm

van der Meulen, R. (2009) Security software and services spending will outpace other IT spending areas in 2010. *Gartner*, Retrieved date: March 21, 2013, URL: http://www.gartner.com/newsroom/id/1167612

Van Dyne, L., Vandewalle, D., Kostova, T., Latham, M.E. & Cummings, L.L. (2000) Collectivism, propensity to trust and self-esteem as predictors of organizational citizenship in a non-work setting. *Journal of Organizational Behavior*, **21**, 3–23.

Vance, A., Lowry, P.B. & Eggett, D. (2013) Using accountability to reduce access policy violations in information systems. *Journal of Management Information Systems*, **29**, 263–289.

Vance, A. & Siponen, M. (2012) IS security policy violations: a rational choice perspective. *Journal of Organizational and End-User Computing*, **24**, 21–41.

Vardi, Y. (2001) The effects of organizational and ethical climates on misconduct at work. *Journal of Business Ethics*, **29**, 325–337.

Watson, D., Clark, L.A. & Tellegen, A. (1988) Development and validation of brief measures of positive and negative affect: the PANAS scales. *Journal of Personality and Social Psychology*, **54**, 1063–1070.

Weiner, B. (1985) An attributional theory of achievement motivation and emotion. *Psychological Review*, **92**, 548–573.

Whitener, E.M., Brodt, S.E., Korsgaard, M.A. & Werner, J.M. (1998) Managers as initiators of trust: an exchange relationship framework for understanding managerial trustworthy behavior. *Academy of Management Review*, **23**, 513–530.

Whitman, M.E. (2003) Enemy at the gate: threats to information security. *Communications of the ACM*, **46**, 91–95.

Whitman, M.E. & Mattord, H.J. (2009) Principles of Information Security. Thomson Course Technology, Boston, MA.

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

Workman, M. (2009) How perceptions of justice affect security attitudes: suggestions for practitioners and researchers. *Information Management and Computer Security*, **17**, 341–353.

Xue, Y., Liang, H. & Wu, L. (2011) Punishment, justice, and compliance in mandatory IT settings. *Information Systems Research*, **22**, 400–414.

Zhang, D., Lowry, P.B., Zhou, L. & Fu, X. (2007) The impact of individualism-collectivism, social presence, and group diversity on group decision making under majority influence. *Journal of Management Information Systems*, **23**, 53–80.

Biographies

Dr Paul Benjamin Lowry is a full professor of Information Systems at the Department of Information Systems, City University of Hong Kong, where he is also the associate director of the MBA programme. He received his PhD in Management Information Systems from the University of Arizona. He has published articles in *MISQ, ISR, JMIS, JAIS, ISJ, EJIS, IJHCS, JASIST, I&M, CACM, Information Sciences, DSS, IEEETSMC, IEEETPC, SGR, Expert Systems with Applications, JBE, Computers & Security, CAIS*, and others. He serves as an AE at *MIS Quarterly (regular guest), European Journal of IS, Information & Management, Communications of the AIS*, and the *Information Security Education Journal*. He is an SE at *AIS-Transactions on HCI*. He has also served as an ICIS, ECIS, and PACIS track chair. His research interests include *behavioural security issues* (e.g., interface design to improve security, IT policy compliance, deception, computer abuse, accountability, privacy, whistle blowing, and protection motivation), *HCI* (e.g., heuristic evaluation, self-disclosure, collaboration, culture, communication, and hedonic systems use), *E-commerce* (e.g., trust, distrust, and branding), and *Scientometrics*.

Dr Clay Posey is an assistant professor of Management Information Systems in the Culverhouse College of Commerce at the University of Alabama. He received his DBA from Louisiana Tech University and has research interests in behavioral information security, online self-disclosure, and research methods among others. His research has been presented at various national and international conferences and has been published in several academic journals including but not limited to *MIS Quarterly, European Journal of Information Systems, Information & Management, DATA BASE for Advances in Information Systems, and Computers & Security.* He is currently an associate editor for *Information & Management* and is a member of the IFIP Working Group 8.11/11.13 on Information Systems Security Research.

Dr Rebecca J. Bennett is the Herbert McElveen professor and department head of Management at Louisiana Tech University in Ruston, Louisiana. Prior to coming to Louisiana Tech, Dr Bennett was a professor of Management and the associate director of the Family Business Center at the University of Toledo. She received her BA in Psychology, cum laude, at Washington University and her MS and PhD degrees in Organizational Behavior from Northwestern University. She is well known for her interest in the 'dark side' of organizations, and her research on employee deviance and responses to offenses in the workplace has been published in academic journals and books and has been presented across the USA and internationally. Because of her expertise, Dr Bennett was asked to be a member of an advisory panel conducted by the Space and Naval Warfare Systems Center Atlantic (SPAWAR) and the Special Security Center (SSC) in the Office of the Director of National Intelligence in August, 2010 to review the Federal Security Clearance Process Adjudicative Guidelines.

Dr Tom L. Roberts is the Clifford R. King professor of Information Systems and Director of the Center for Information Assurance at Louisiana Tech University. He received his PhD in Information Systems from Auburn University. His research interests include behavioral information security, information assurance, privacy and online disclosure, information quality, and collaborative systems. His research has appeared in outlets such as *MIS Quarterly, Journal of Management Information Systems, European Journal of Information Systems, Journal of the Association for Information Systems, IEEE Transactions on Software Engineering, Computers & Security*, and others.

SUPPORTING INFORMATION

Additional supporting information may be found in the online version of this article at the publisher's web site.

APPENDIX A. MEASUREMENT SCALES

Respondents were asked to reflect on the most recent ISP changes implemented by their organisation prior to answering the survey questions. Specifically, respondents encountered the following statement during the survey completion process: 'Please think of the last information security policy and/or procedure implemented by your organization and answer the following questions. Such policies or procedures may include, but are not limited to, an employee-monitoring policy on the computer system and restricted employee access to the system.'

Construct (source)	Items	Source(s)
Organisational trust	OT1. I believe my organisation has high integrity. OT2. I can expect my organisation to treat me in a consistent and predictable fashion. (r)OT3. My organisation is not always honest and truthful. OT4. In general, I believe my organisation's motives and intentions are good. (r)OT5. I don't think my organisation treats me fairly.	Robinson (1996)

(Continues)

APPENDIX A. (Continued)

Construct (source)	Items	Source(s)
	OT6. My organisation is open and upfront with me.	
	(r)OT7. I am not sure if I fully trust my organisation.	
Freedom restrictions	FR1. I feel that my organisation's computer-system security policies and practices are an invasion of privacy.	Alge *et al*. (2006), based on their privacy invasion measure
	FR2. I feel uncomfortable about the types of information that my organisation collects about its employees' use of the computer system.	
	FR3. The way that my organisation monitors its employees' use of the computer system makes me feel uneasy.	
	FR4. I feel personally invaded by the methods used by my organisation to collect information about its employees' use of the computer system.	
	(r)FR5. I have little reason to be concerned about my privacy here in my organisation when using the computer system.	
Computer abuse	CA1. I have damaged computer property belonging to my employer (e.g., hardware, software, data files, etc.).	Robinson & O'Leary-Kelly (1998)
	CA2. I have deliberately bent or broke a computer-related rule or policy.	Robinson & O'Leary-Kelly (1998)
	CA3. I have adjusted data in the computer system to make my activity appear more in line with organisational computer guidelines, policies, and/or rules.	Jaworski & MacInnis (1989)
	CA4. I have gone against management decisions regarding what management deems as appropriate computer system use.	Vardi (2001)
	CA5. I have sabotaged portions of the computer system.	Robinson & Bennett (1995)
	CA6. I have intentionally made errors in the computer system.	Robinson & Bennett (1995)
	CA7. I have covered up mistakes in the computer system.	Robinson & Bennett (1995)
	CA8. I have taken computer-system resources without proper approval (e.g., hardware, software, data files).	Robinson & Bennett (1995)
	CA9. I have misused my computer-system access privilege(s).	Robinson & Bennett (1995)
	CA10. I have accessed files or viewed data in the computer system without being given authorisation to do so.	Robinson & Bennett (1995)
Organisational SETA initiatives	My organisation…	Adapted from Whitman & Mattord (2009)
	SETA1. …makes certain its employees are fully aware of what specific security risks/threats it experiences.	
	SETA2. …trains its employees on how to perform their job duties in a secure manner.	
	SETA3. …educates and explains to its employees why specific security risks/threats exist.	
Explanation adequacy	In its explanation of the information security measures, to what extent…	Adapted from Colquitt (2001); Greenberg (1993); and Shapiro *et al*. (1994)
	EA1. …has the organisation been candid in its communications with you?	
	EA2. …has the organisation explained the recent security measures thoroughly?	
	EA3. …were the organisation's explanations regarding the recent security measures reasonable?	
	EA4. …has the organisation communicated details of the recent security measures in a timely manner?	

(Continues)

APPENDIX A. (Continued)

Construct (source)	Items	Source(s)
Negative affect	To what degree do the following attributes describe you? NA1. Scared NA2. Afraid NA3. Upset NA4. Distressed NA5. Jittery NA6. Nervous NA7. Ashamed NA8. Guilty NA9. Irritable NA10. Hostile	Watson *et al.* (1988)
Advanced notification of changes	Were you told of the information security measure change before or after its implementation?	Authors; one-item

(r) = reverse coded; unless noted otherwise, all scale items are based on a 7-point Likert-type scale from 1 = strongly disagree to 7 = strongly agree; computer abuse items were captured on a 7-point Likert-type scale from 1 = never to 7 = very frequently.

Qualitative coding for 'restrictiveness of enhanced ISP'

In consulting Rob Folger, we qualitatively derived the measure of 'restrictiveness of enhanced ISP' as follows: in terms of qualitative open-response to our survey, respondents were asked to reflect on the most recent security changes in their organisation, to describe those changes and to state why they believed the changes were necessary. Further, we asked the respondents about all the communication methods their organisations used to inform them about the changes (e.g. email, one-on-one meetings, group-based meetings, written notice). Our restrictiveness variable was based on the qualitative descriptions respondents provided while completing this section of the survey in which they were required to describe how the enhanced policy affected their job and what the actual restrictions were. The authors engaged in simple coding on a scale of 0 to 3 as to how many restrictions they listed; we recoded any in which there was not full agreement to achieve 100% interrater reliability. The coding was simple as follows (with actual quotes from the respondents given as examples). '0' was given for those who did not know or could not think of any new enhancements vs. restrictions that have been in place; '1' was given for a minor restriction (e.g. 'Tougher password requirements'; 'Updating Software Protection'); '2' was given for two distinct restrictions or one major restriction (e.g. 'Web site blocking, software changes'; 'Stripping inappropriate attachments from emails, and denying access to inappropriate web sites.'); '3' was given for multiple substantial efforts (e.g. 'We recently had an online instruction/quiz regarding security on our systems. We were advised of appropriate uses of the internet. Also, employees are monitored regarding sites visited and email usage.'; 'Restricted access; changing passwords frequently, internet and email monitoring').

Control variables to Test rival explanations to our research model

Latent construct	Prompt and items	Source(s)
Negative affect	To what degree do the following attributes describe you? NA1. Scared NA2. Afraid NA3. Upset NA4. Distressed NA5. Jittery NA6. Nervous NA7. Ashamed NA8. Guilty NA9. Irritable NA10. Hostile	Watson *et al*. (1988)
Certainty of sanction	Since the most recent internal computer-system security policies, procedures, and/or rules referred to above were implemented, how do you feel about your organization's overall computer-system security guidelines, policies, and/or rules? CS1. My organization is aware of everything I do on their computer system. CS2. I am closely monitored while using my organization's computer system. CS3. My organization closely monitors my performance for errors on their computer system. CS4. It is likely that employees will be caught for computer-rule violations or abuse of computer privileges. CS5. My organization is aware of what I do on a daily basis in my work on their computer system. CS6. I am constantly being checked for computer-rule violations. CS7. I feel that I am constantly being watched to see that I obey all computer rules pertaining to my job	Adapted from D'Arcy & Devaraj (2012); and D'Arcy *et al*. (2009)
Severity of sanction	SS1. It is likely that employees will be punished for computer-rule violations or abuse of computer privileges. SS2. Sanctions for violating computer rules and procedures about my job are severe. SS3. Even if someone is discovered violating a computer rule pertaining to their job, severe sanctions are rarely imposed. SS4. It is likely that employees would be fired for computer-related violations. SS5. My organization would take strict action against employees caught misusing the computer system.	Adapted from D'Arcy & Devaraj (2012); and D'Arcy *et al*. (2009)
Celerity of sanction	CEL1. My organization's response to computer-system violations by employees is (would be) instantaneous. CEL2. My organization (would) takes immediate action against employee violations of the computer system. CEL3. Very little time (would) elapse between detection of computer-system violations and my organization's response to them. CEL4. My organization's response process to employee violations of the computer system is (would be) very timely.	Adapted from D'Arcy & Devaraj (2012); and D'Arcy *et al*. (2009)
Age	Please indicate your age range, as follows:	n/a

(Continues)

(Continued)

Latent construct	Prompt and items	Source(s)
	• Between 20 and 24 • Between 25 and 29 • Between 30 and 34 • Between 35 and 39 • Between 40 and 44 • Between 45 and 49 • Between 50 and 54 • Between 55 and 59 • Between 60 and 64 • Older than 65	
Gender	Please indicate your gender: • Female • Male	n/a
Professional tenure	How many years have you worked in your current profession?	n/a
Organisational tenure	How many years have you worked at your current organisation?	n/a
Computer Use	How many hours (in an average workday) do you use a computer? • Less than 45% • Between 45 and 54% • Between 55 and 64% • Between 65 and 74% • Between 75 and 84% • Between 85 and 94% • Greater than 95%	n/a
Education	Indicate your level of completed education: • High School • Some College • Undergraduate degree • Masters degree • Doctorate/Professional degree	n/a
Manager	Are you a supervisor, manager, or executive in your current position? • Yes • No	n/a
IS/IT Employee	Are you an information systems (IS) or information technology (IT) employee in your current position? • Yes • No	n/a
income ($)	Please indicate your current level of income: • Less than $25,000 • Between $25,000 and $49,999 • Between $50,000 and $74,999 • Between $75,000 and $99,999 • Between $100,000 and $124,999 • Greater than $125,000	n/a

(Continues)

(Continued)

Latent construct	Prompt and items	Source(s)
Organisation size	Please indicate the approximate size of your current organisation: • Small organization – 1 to 100 computers • Medium organization – 100 to 1,000 computers • Large organization – 1,000 to 10,000 computers • Very large organization – More than 10,000 computers	n/a

(r) = reverse coded; unless noted otherwise, all scale items are based on a 7-point Likert-type scale from 1 = strongly disagree to 7 = strongly agree; computer abuse items were captured on a 7-point Likert-type scale from 1 = never to 7 = very frequently.