Inquiry into the Management of Child Sex Offender Information

Dr Craig Horne

CONTACT DETAILS

Phone:
Email:

Organisation Name:
Organisation Postion:

Address:
Suburb:
State:
Postcode:
Your age group:

YOUR SUBMISSION

Submission:
Dear Members of Victorian Parliament,

As a member of the general public, I would like to offer my support to the public disclosure of child sex offender details. With a PhD in information security strategy, I am an expert in the management and security of information, and I am qualified to advise when information should remain confidential or otherwise.

For a deterrent to be effective in controlling the behaviour of rational people, it must be swift, severe, and certain (D'Arcy & Herath 2011). To expand, deterrence theory states that formal sanctions, such as custodial sentences imposed by the courts, ensure that potential offenders consider both the risks and the costs of their intended illegal activity before engaging in it (Gibbs 1975). Informal sanctions such as public disapproval also affect potential offenders (Piquero & Tibbetts 1996).

The impacts from child predation on citizens in the State of Victoria can be varied and powerful. The police resources required to investigate and court costs to prosecute, the financial cost of decades of incarceration, and the lifelong impacts on the victim and their loved ones are profound.

The impacts on the predator are also profound. A rational offender will forever have to live with shame, a conviction, and will therefore find it difficult to find any employment that requires a police check. The financial risk can be mitigated with a JobSeeker Payment. The shame will never go away because the victim can never be un-violated.

On balance, the interests of Victorian citizens have to be balanced against the interests of the offender. There is a strong body of evidence to show that deterrence is reliable and effective. In relation to disclosure in a public register, this sanction should be imposed immediately upon verdict (swift), published in every newspaper in the country (severe), and unable to be overturned on appeal (certain).

The members of Parliament of Victoria are not elected because they are weak of character. They should resolve to improve the lives and future prospects of all Victorian children by making the hard decision to publicly disclose the identities of child sex predators. I hope the leaders of this great State of Victoria consider this submission useful and it helps in guiding decisions.

Sincerely,

Dr Craig A Horne

References:

D'Arcy, J., and Herath, T. 2011. "A Review and Analysis of Deterrence Theory in the Is Security Literature: Making Sense of the Disparate Findings," European Journal of Information Systems (20:6), pp 643-658.
Gibbs JP (1975) Crime, Punishment, and Deterrence. Elsevier, New York.
Piquero A and Tibbetts S (1996) Specifying the direct and indirect effects of low self-control and situational factors in offenders decision making: toward a more comparative model of rational offending. Justice Quarterly 13(3), 481–510.

Are you interested in appearing before the committee in person to talk about your submission?
Yes

FILE ATTACHMENTS

File1: 5f3e7618a52ca-DArcy Herath A Review n Analysis of Deterrance .pdf
File2:
File3:

Confidentiality:

Signature:
Craig Horne

www.palgrave-journals.com/ejis/

RESEARCH ARTICLE

A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings

John D'Arcy[1] and
Tejaswini Herath[2]

[1]Department of Management, 351 Mendoza College of Business, University of Notre Dame, Notre Dame, 46556 Indiana, U.S.A;
[2]Department of Finance, Operations and Information Systems, Brock University, St. Catharines, ON, Canada L2S 3A1

Correspondence: John D'Arcy, Department of Management, 351 Mendoza College of Business, University of Notre Dame, Notre Dame, 46556 Indiana, U.S.A.
Tel: (574) 631 1735;
Fax: (574) 631 5255;
E mail: jdarcy1@nd.edu

Abstract

Deterrence theory is one of the most widely applied theories in information systems (IS) security research, particularly within behavioral IS security studies. Based on the rational choice view of human behavior, the theory predicts that illicit behavior can be controlled by the threat of sanctions that are certain, severe, and swift. IS scholars have used deterrence theory to predict user behaviors that are either supportive or disruptive of IS security, and other IS security-related outcome variables. A review of this literature suggests an uneven and often contradictory picture regarding the influence of sanctions and deterrence theory in general in the IS security context. In this paper, we set out to make sense of the discrepant findings in the IS deterrence literature by drawing upon the more mature body of deterrence literature that spans multiple disciplines. In doing so, we speculate that a set of contingency variables and methodological and theoretical issues can shed light on the inconsistent findings and inform future research in this area. The review and analysis presented in this paper facilitates a deeper understanding of deterrence theory in the IS security domain, which can assist in cumulative theory-building efforts and advance security management strategies rooted in deterrence principles.

European Journal of Information Systems (2011) **20,** 643 658.
doi:10.1057/ejis.2011.23; published onl ne 14 June 2011

Keywords: deterrence theory; rational choice theory; IS security compliance; IS security policy violations; IS misuse; computer abuse

Received: 28 June 2010
Revised: 22 April 2011
Accepted: 11 May 2011

Introduction

Information security is a serious concern for both businesses and society as a whole. Estimates of the financial impact of compromises to information security range from 'tens, if not hundreds of billions of dollars' (United Nations, 2005, p. xxiii) to over one trillion dollars each year worldwide (Mercuri, 2003). The Computer Security Institute's annual surveys indicate over US$2 billion in losses to organizations due to computer crime and related activities between 1997 and 2007, and the overall number of types of attacks nearly doubled during this period.

Organizations have responded to the growing list of security threats through a combination of technical, administrative, and physical controls. Despite these efforts, information security breaches continue to plaque organizations. Consequently, information security has become a focal area for practitioners and academics. Industry surveys indicate that ensuring information security is a top management priority in many organizations (Ernst & Young, 2009; PwC/CSO/CIO, 2010). Within the information systems (IS) research community, a sizeable body of research that focuses on various aspects of information security management has emerged, including a significant effort to investigate the relationship between IS security and the behavior of employees (e.g., D'Arcy *et al*, 2009; Herath & Rao, 2009a, b; Bulgurcu *et al*, 2010; Siponen & Vance, 2010).

Much of the behavioral IS security research has focused on the antecedents of employees' IS security policy compliance/non-compliance and abuse or misuse of IS resources (Warkentin & Willison, 2009). Deterrence theory is a prominent theoretical perspective in this work. Rooted in classic criminology (Beccaria, 1963), the theory assumes that people make reasoned decisions toward perpetrating or abstaining from crime based on the maximization of their benefits and the minimization of cost. Classic deterrence theory focuses on formal (legal) sanctions and posits that the greater the perceived certainty, severity, and celerity (swiftness) of sanctions for an illicit act, the more individuals are deterred from that act (Gibbs, 1975). Extensions to the classic deterrence model include informal sanctions such as social disapproval, self-disapproval (e.g., shame), and moral inhibition (Piquero & Tibbetts, 1996). Contemporary deterrence theory posits that individuals include the perceived risks and costs of both formal and informal sanctions in deciding whether or not to engage in an illicit activity (Pratt *et al*, 2006).

Siponen *et al* (2008) reviewed the IS security literature for the period 1990 2004 and found deterrence theory as the single most cited theory referenced in six papers. Our own literature review (see online Supplementary Appendix Tables A1 A3) identified additional and more recent papers that utilized deterrence theory in the IS security context. Interestingly, despite its strong theoretical foundation in criminology and empirical support in predicting illicit behavior in organizational settings (Paternoster & Simpson, 1996; Pratt *et al*, 2006), deterrence theory has received mixed support in the IS security literature.

For example, Straub (1990) used investment in security countermeasures (i.e., security policies, security staff hours, and technical controls) as proxies for perceived certainty and severity of formal sanctions and found that use of countermeasures was associated with reduced incidence of computer abuse, thereby supporting the basic tenets of deterrence theory. A study by D'Arcy *et al* (2009) at the individual level found that perceived severity, but not certainty, of formal sanctions was negatively associated with IS misuse intention. Conversely, a pair of studies by Herath and Rao (2009a, b) found that perceived certainty of detection, but not perceived severity of penalty, was positively associated with IS security policy compliance intention. Additional studies found that deterrence-based countermeasures and/or deterrence constructs themselves (i.e., perceived certainty and/or severity of formal or informal sanctions) did not have a significant influence on employee behavior (Lee *et al*, 2004; Pahnila *et al*, 2007; Siponen & Vance, 2010) or that their influence was contingent on individual and contextual factors (Harrington, 1996; D'Arcy & Hovav, 2009). In sum, extant research provides inconsistent and sometimes contradictory findings for deterrence theory in the IS security context.

We find the equivocality of this body of work perplexing and contend that it is time to critically assess deterrence theory in the IS literature similar to its reviews in other disciplines (e.g., Williams & Hawkins, 1986; Paternoster, 1987; Pratt *et al*, 2006). As Robey & Boudreau (1996) point out, 'inconsistencies within a body of research … typically motivate efforts to restore order by resolving or explaining the observed discrepancies (p. 170)'. They note three common strategies for resolving inconsistent findings across studies: (1) identifying contingency variables; (2) evaluating methodological issues; and (3) conducting better reviews of substantive research questions. We follow a similar approach in this paper and speculate that a set of contingency variables and methodological and theoretical issues can help explain the discrepant findings of deterrence-based studies in the IS security context. Our aim is to provide a holistic analysis of this body of work and shed light on the application of deterrence theory to IS security research. On a broader scale, we hope that our analysis of one of the more popular theories in the IS security literature can assist in cumulative theory-building efforts in this area.

It should be pointed out that gaining a deeper understanding of deterrence in the IS security realm also has strong practical implications. For example, ISO/IEC 27002, one of the most widely adopted standards for information security management, draws heavily from deterrence theory in recommending policies, guidelines, and awareness programs that clearly define consequences and sanctions for employees that misuse company resources (Theoharidou *et al*, 2005). The standard also prescribes monitoring of system access and audit mechanisms based on the premise that increased detection certainty deters security violations. Given the IS security community's faith in deterrent countermeasures, both researchers and practitioners have a vested interest in knowing whether in fact deterrence does work, and if so, under what conditions is it a viable IS security management strategy.

Scope of the study

Before moving forward, we need to clarify a couple of terms and address the scope of this paper. First, research on the deterrent impact of sanctions spans the disciplines of economics, law, sociology, social psychology, criminology, and others. We use the term *deterrence literature* rather loosely to refer to this collective work, although we draw largely from the criminological deterrence literature for much of our discussion. We use the term *IS deterrence literature* in a narrower sense to refer to those studies that assessed the impact of sanctions in the IS context (i.e., using an IS-related outcome variable).

Second, our categorization of the IS deterrence literature is limited to studies that included a *direct* relationship between sanctions (measured via objective, perceptual, or proxy measures) and behaviors that are either destructive or supportive of IS security, or a related IS security outcome variable. Hence, studies that assessed the indirect or moderating influence of sanctions (e.g., Workman & Gathegi, 2007; Liao *et al*, 2009; Bulgurcu *et al*, 2010) are excluded. Our goal is to analyze those IS studies that explicitly tested deterrence theory as opposed to capturing every possible study that included a sanction construct. Our search for IS deterrence studies mainly included major IS journals. In addition, we included two often-cited articles from IS conference proceedings and three studies from non-IS journals that used IS-related outcome variables. Considering that IS deterrence studies sometimes appear in non-IS journals, we do not claim to have an exhaustive list. However, we believe to have included the most prominent IS deterrence studies and thus have an encompassing view of this research stream.

Lastly, the classic conceptualization of deterrence theory includes three components of sanctions certainty, severity, and celerity. Interestingly, deterrence studies have rarely included celerity of sanctions (either formal or informal), citing measurement difficulties and its lack of theoretical importance (Nagin & Pogarsky, 2001; Paternoster, 2010) (see Pogarsky & Piquero, 2004 for an exception). Similarly, celerity of formal or informal sanctions is not included in the operational definition of deterrence theory in any of the IS deterrence studies that we reviewed. Hence, we consider perceived certainty and severity of sanctions as the two major components of disincentives in deterrence theory for this paper.

The paper proceeds as follows. Next, we present 'Contingency variables' that are relevant to IS deterrence studies and thus potentially contribute to the differential outcomes in this literature. This is followed by a discussion of 'Methodological issues' that may also contribute to the disparate findings. Thirdly, we identify 'Additional substantive issues' that provide insight into the IS deterrence literature. We then offer 'Research guidelines and opportunities' that pertain to the previous three sections. The paper concludes with a summary of key points and contributions.

Contingency variables

Implicit in the majority of IS deterrence studies (see Harrington, 1996 and D'Arcy & Hovav, 2009 for exceptions) is the assumption that the impact of sanctions is uniform across individuals. To the contrary, deterrence research has shown that the deterrent effect of sanctions differs radically from individual to individual (Tittle, 1980; Mann *et al*, 2003; Pratt *et al*, 2006).

As theoretical developments have established that deterrence considerations are conditional on a host of personal and contextual factors (Jacobs, 2010), one could conceivably come up with numerous variables that influence the relationships specified by deterrence theory. Our goal is not to provide an exhaustive list but rather to identify a set of key contingency variables that can further elaborate deterrence theory in the IS security context. We discuss five such variables in the following sections.

Individual factors

Self-control One individual characteristic that has received a great deal of attention in the deterrence literature is level of self-control. Empirical results have linked low self-control to numerous criminal and deviant activities (see Pratt & Cullen, 2000 for meta-analytic review) including software and digital piracy (Higgins *et al*, 2005; Zhang *et al*, 2006). More pertinent to the current analysis, there is support for the moderating influence of self-control on the relationships specified by deterrence theory. The theoretical argument is that low self-control individuals are more prone to engage in illicit activities in an impulsive manner and therefore are less responsive to the threat of punishment (Pogarsky and Piquero, 2004). Stated differently, sanction threats are thought to 'fall on deaf ears' for these individuals. Piquero & Tibbetts (1996) provide evidence to support this position, as they found that individuals with low self-control were less concerned with the threat of formal sanctions for shoplifting and drunk driving. There is a counterargument, however, and some evidence that the deterrent effect of sanctions is not contingent on self-control (Wright *et al*, 2004; Cochran *et al*, 2008). That said, the prevailing sentiment and bulk of empirical evidence supports the position that those with lower self-control are less deterrable (Pratt *et al*, 2006). Within the IS deterrence literature, empirical validation of a contingent effect of self-control on the sanctions-to-behavior relationship does not exist. Hence, we encourage researchers to account for this moderating influence and investigate whether self-control increases or decreases the influence of sanctions in the IS security context.

Computer self-efficacy (CSE) Another individual difference variable that should be considered for its contingent effects is CSE. The IS literature distinguishes between two levels of CSE: general and task-specific. General CSE refers to an individual's overall confidence in his/her ability to use computers while task-specific CSE refers to one's confidence toward specific IS tasks or applications, such as using a spreadsheet (Marakas *et al*, 2007).

Within the deterrence literature, evidence suggests that the deterrent effect of formal sanctions is lesser for those with greater skills and abilities related to criminal and deviant activities (Tittle, 1980; Pogarsky *et al*, 2004). The rationale is that high self-efficacy in this regard leads certain individuals to believe that they can circumvent security measures and get away with it, with little consideration for the threat of punishment (Jacobs, 2010). This line of thinking is supported by laboratory research which found that people take more risks and have a lower regard for threats in situations in which they feel more competent (Kruegar & Dickson, 1994).

On the flip side, research suggests that when people perceive lesser skills and ability to control a given outcome, they are more receptive to exogenous appeals such as the threat of punishment (Workman & Gathegi, 2007). Extending this to the IS security context, it is reasonable to expect that the deterrent impact of formal sanctions will be weaker for users with higher CSE. D'Arcy & Hovav (2009) tested this assertion using a general CSE measure and found that security awareness efforts and computer monitoring (proxies for perceived formal sanctions) had less influence on IS misuse intentions for high CSE individuals. Hence, there is evidence that a general level of CSE attenuates the relationships between formal sanctions and behavior, at least for certain misuse behaviors that are disruptive of IS security.

Moral beliefs A third contingency variable is personal moral beliefs. Moral beliefs refer to the extent to which one perceives an illicit act to be morally offensive (Paternoster & Simpson, 1996). Note that this definition does not constitute an 'organized and fully developed ethical system' (Paternoster & Simpson, 1993, p. 45) but instead one's moral evaluation of a particular behavior within a particular context. Contemporary deterrence studies have typically operationalized moral belief in this manner and found strong evidence of its influence on various forms of illicit behavior including corporate crime (Pratt *et al*, 2006; Smith *et al*, 2007).

The deterrent effect of sanctions is also thought to vary based on moral considerations such that those individuals with strong moral beliefs are already effectively restrained from criminal/deviant behavior and therefore the threat of punishment is irrelevant, or at least much weaker (Silberman, 1976; Pratt *et al*, 2006). Other, less morally inhibited individuals are more influenced by the threat of punishment. Empirical results generally support the notion that moral beliefs moderate the impact of punishment threats (e.g., Paternoster & Simpson, 1996; Workman & Gathegi, 2007; Cochran *et al*, 2008) although we should point out that the evidence is not universal (e.g., Klepper & Nagin, 1989; Schoepfer & Piquero, 2006).

Within the IS security realm, D'Arcy *et al* (2009) investigated the moderating effect of moral beliefs on the relationships between perceived certainty and severity of formal sanctions and IS misuse intention. Their results suggest that the contingent effect of moral beliefs in deterrence theory is more nuanced in the IS security context. Specifically, they found that perceived certainty of formal sanctions, but not perceived severity, was a significant deterrent to IS misuse for individuals with high moral commitment scores (i.e., stronger more beliefs). On the other hand, perceived severity of formal sanctions, and not perceived certainty, was a significant deterrent for individuals with low moral commitment scores.

Given the considerable evidence that moral beliefs have some form of moderating influence within deterrence theory, the absence of an individual morality construct from the majority of IS deterrence studies (see online Appendix Table A1) offers some explanation for the inconsistent findings in this body of work.

Contextual factors

Beyond individual factors, the deterrence literature suggests that contextual factors have important moderating influences in deterrence theory (Mann *et al*, 2003). As with the individual difference variables, there are numerous contextual characteristics such as employee position, opportunities of the position, and characteristics of the work that could conceivably moderate the deterrence theory relationships (Paternoster & Simpson, 1996; Smith *et al*, 2007). Based on available theoretical and empirical evidence, we identified virtual status and employee position as two contextual variables that are relevant to our analysis of the IS deterrence literature.

Virtual status Virtual status refers to the degree of work that an employee performs from dispersed locations compared to within the primary or central workplace (Wiesenfeld *et al*, 1999). A common arrangement in which employees work virtually is telecommuting, also known as remote work. From a deterrence perspective, deindividuation theory provides evidence that the threat of sanctions may be less effective against virtual workers. Deindividuation is the psychological separation of the individual from others (Zimbardo, 1969). It was originally considered a group phenomenon in which individuals that were immersed in a crowd experienced loss of individuality, leading to decreased self-control. However, Zimbardo's research demonstrated that deindividuation is not limited to group settings and includes situations where individuals' contributions are less identifiable, as in dispersed settings.

Deindividuation theory argues that, due to the psychological separation of self from others and a social environment (e.g., workplace) that provides the context for legitimate behavior, individuals have a greater tendency to perceive themselves as extricated from responsibility for their actions, which in turn facilitates deviant behavior. Concomitant with this is that external constraints that would typically regulate deviant behavior are rendered less effective (Postmes & Spears, 1998). Research suggests that virtual workers may experience deindividuation as a result of being temporally and spatially dispersed from other organizational members (McCloskey & Igbaria, 2003). IS researchers have used deindividuation theory to describe the sense of anonymity, depersonalization, and psychological distance that individuals can experience when using information technology (Loch & Conger, 1996; Pinsonneault & Heppel, 1998; Chidambaram & Tung, 2005). Based on the tenets of deindividuation theory, a reasonable assumption is that employees that spend more time in virtual mode are less receptive to sanction threats pertaining to the improper use of IS resources.

D'Arcy & Hovav (2009) tested this assertion by assessing the moderating influence of virtual status on the relationships between three security countermeasures (proxies for perceived formal sanctions) security policies, security awareness program, and computer monitoring and IS misuse intention. The results suggest that the deterrent effects of security awareness programs and computer monitoring are weaker for employees that spend more working days outside the office. Hence, there is theoretical and empirical support that virtual status is a contingent factor that should be considered in IS deterrence frameworks.

Employee position Another contextual variable that may moderate the deterrence theory relationships is employee position. The rationale is that different types of employees (e.g., contract/permanent, full-time/part-time, manager/non-manager) have different stakes in the organization and thus will not be uniformly receptive to the threat of sanctions (Tittle, 1980; Smith *et al*, 2007). In discussing the impact of sanction threats on different types of employees, deterrence researchers have focused particularly on managers/non-managers, suggesting that formal sanctions may have a stronger impact on managers as they have more negative consequences to consider if they are caught and punished (Paternoster & Simpson, 1996; Smith *et al*, 2007). Interestingly, in our survey of both the general and IS deterrence literatures, we found no direct tests of this assertion. However, as discussed next, our analysis suggests that the contingent influence of manager/non-manager should be considered in IS deterrence models.

Further analyses of employee position and moral beliefs as contingency variables

To further the previous discussion, we conducted additional assessment of the potential contingent influences of employee position and moral beliefs using datasets from D'Arcy *et al* (2009) and Herath & Rao (2009a, b). We emphasize that the following are convenience-type analyses performed in a somewhat cursory manner using data at our disposal. These limitations notwithstanding, we offer them as additional support for our earlier arguments.

First, in terms of employee position, we tested for the moderating influence of manager *vs* non-manager using the D'Arcy *et al* (2009) dataset. As part of their extended deterrence model, D'Arcy *et al* posited inverse relationships between (1) perceived certainty of formal sanctions and IS misuse intention, and (2) perceived severity of formal sanctions and IS misuse intention. For the current analysis, we coded the respondents as either manager (coded as 1) or non-manager (coded as 0) and added two latent interaction variables (Perceived Certainty × Employee Position) and (Perceived Severity × Employee Position) to the D'Arcy *et al* model. The analysis was conducted using the SmartPLS 2.0 software.

The results indicated that neither latent interaction variable was significantly associated with IS misuse intention, thereby suggesting that manager/non-manager does not moderate the deterrent effect of formal sanctions on IS misuse. For completeness sake, we ran the same model but this time with perceived certainty and severity of formal sanctions as a single composite measure. This was created by multiplying each perceived certainty measure by its associated perceived severity measure. The impetus for the composite measure is the ongoing debate in the deterrence literature as to whether perceived certainty and severity of sanctions are best modeled as additive or multiplicative (Cochran *et al*, 2008).

The results of the second analysis indicated that (Perceived Sanctions * Employee Position) was moderately associated with IS misuse intention ($\beta=0.09$, $P<0.05$). To further explore this effect, we split the sample into management ($n=61$) and non-management ($n=208$) subgroups and ran separate models for each group. The results indicated that for the management subgroup, perceived formal sanctions had a much stronger inverse relationship with IS misuse intention ($\beta=$ 0.47, $P<0.01$) than for the non-management subgroup ($\beta=$ 0.15, $P<0.05$) and this difference was significant ($P<0.01$). Hence, our analysis provides suggestive evidence that the influence of perceived formal sanctions on IS misuse intention is more poignant for managers.

For a second analysis, we considered the role of moral beliefs when analyzing the divergent findings regarding the relative influences of perceived certainty and severity of formal sanctions in D'Arcy *et al* (2009) and Herath & Rao (2009a, b). Recall that D'Arcy *et al* found that perceived severity of formal sanctions was significantly associated with IS misuse intention, while perceived certainty of formal sanctions was only significant for a subsample of individuals with high moral commitment scores. Conversely, Herath and Rao's studies (both used the same sample) indicated a significant inverse relationship between perceived certainty of detection and IS security policy compliance intention, while perceived severity of penalty was not significant.

There are several possible explanations for these contrasting results, some of which we discuss in later sections. However, in terms moral beliefs, if we consider D'Arcy *et al*'s high moral commitment subsample results (i.e., perceived certainty of formal sanctions is a stronger deterrent for higher morality individuals), it could be that Herath and Rao's sample contained a higher percentage of individuals with strong moral beliefs.

To further this line of thinking, we draw upon a prominent theory from the ethics and morality literature, namely Kohlberg's (1969) Theory of Cognitive Moral Development. Kohlberg's theory postulates that moral judgment is developed through six stages which are embedded within three broad categories: preconventional, conventional, and principled (Myyry *et al*, 2009). Individuals are thought to move through the stages in an irreversible sequence such that their moral reasoning becomes more sophisticated over time. Younger people and immature adults have primarily preconventional orientations. Preconventional morality individuals have a strong fear of punishment and thus obey rules to avoid punishment. From a deterrence perspective, perceived severity of formal sanctions is presumably a particularly salient concern. Individuals at the conventional morality stage are more sensitive to the norms and laws that guide behavior and are also strongly influenced by significant others' expectations and in particular a desire to avoid social disapproval. Thus, the fear of getting caught and accused of a socially undesirable act (i.e., certainty of punishment) is likely to be a stronger inhibitor to illicit conduct than the threat of severe punishment for these individuals. Research indicates that most adults are at the conventional level of moral development (Trevino *et al*, 2006).

Turning to the D'Arcy *et al* and Herath and Rao studies, a comparison of the demographic characteristics of the two samples indicates a higher percentage of older respondents in Herath and Rao. We used D'Arcy *et al's* age groupings as cutoff points and found that 60% of their sample was over 34 years old *vs* 78% for Herath and Rao. Using the next cutoff point, 27% of D'Arcy *et al's* sample was over 44 years old *vs* 43% for Herath and Rao. Now, to the extent that having a higher percentage of older respondents equates to more respondents at the conventional morality stage, along with the general notion that moral development increases with age, it is reasonable to assume that Herath and Rao's sample contained a higher percentage of respondents with stronger moral beliefs compared with D'Arcy *et al's* full sample. If this is true, Herath and Rao's finding that perceived certainty of detection has the stronger deterrent effect is in accord with D'Arcy *et al's* results for the high moral commitment subsample. Hence, the seemingly contradictory findings of these studies make more sense when we integrate the moderating influence of morality into deterrence theory.

Table 1 summarizes the key points from the discussion of contingency variables and offers recommendations for researchers. These and other recommendations are discussed further in the 'Research guidelines and opportunities' section of the paper.

Methodological issues

A second strategy for resolving inconsistent findings across studies is to evaluate methodological issues (Robey & Boudreau, 1996). As such, we conducted an in-depth review of the IS deterrence literature and focused on methodological differences. Based on our analysis, we speculate that sampling differences (e.g., different countries/cultures, student *vs* employees), response rate issues

Table 1 Contingency variables key points and recommendations

Contingency variable	*Key points and recommendations*
Self control	• Low self control weakens the deterrent effect of formal sanctions (Piquero & Tibbetts, 1996; Pogarsky & Piquero, 2004) • We recommend measuring self control (see Grasmick *et al*, 1993 for scale) and testing for its moderating influence in IS deterrence studies
CSE	• Individuals have lower regard for formal sanctions in situations in which they have higher self efficacy (Kruegar & Dickson, 1994; Pogarsky *et al*, 2004) • We recommend measuring CSE and testing for its moderating influence in IS deterrence studies, especially when research samples contain respondents with varying degrees of computer skills and abilities • Domain specific measures (e.g., self efficacy toward IS security related behaviors) are recommended over a general CSE measure to better isolate the influence of sanction constructs (see Bulgurcu *et al*, 2010 for an example)
Moral beliefs	• Moral beliefs moderate the deterrent effect of sanctions (Pratt *et al*, 2006) • We recommend measuring moral beliefs (or a related individual morality construct) and testing for its moderating influence in IS deterrence studies • See D'Arcy *et al* (2009) for a single item moral belief measure or Li *et al* (2010) for a multi item measure
Virtual status	• Virtual work may weaken the deterrent effect of sanctions (Postmes & Spears, 1998; D'Arcy & Hovav, 2009) • We recommend measuring virtual status, or a related measure of time spent in virtual mode, and testing for its moderating influence in IS deterrence studies • Virtual status is particularly relevant in research contexts where the virtual component of the workforce is strong
Employee position	• Different types of employees have different stakes in the organization and therefore are more/less receptive to the threat of sanctions (Tittle, 1980; Smith *et al*, 2007) • Evidence that formal sanctions have a stronger deterrent effect on managers • We recommend testing for the moderating influence of employee type especially manager *vs* non manager in IS deterrence studies

(e.g., non-response bias), survey characteristics (e.g., anonymous *vs* non-anonymous, online *vs* paper), statistical analysis techniques, and use of intentions *vs* actual behaviors as outcome variables all contributed to the inconsistent findings. We regard these as general research issues that are pertinent to a comparative analysis of any body of empirical studies. We limit our remaining discussion of methodological issues to those that are specific to deterrence constructs (i.e., formal and informal sanctions) and thus can help inform the inconsistencies in the IS deterrence literature.

As shown in online Appendix Tables A1 and A2, there are quite different treatments and operationalizations of the deterrence constructs across studies. Treatment variations include separate analysis of the perceived certainty and severity of sanction measures, combined indexes of the two, and inclusion of informal sanction constructs. In terms of operationalization, there is little consistency in the measurement of certainty and severity of sanctions. We speculate that each of these issues contributed to the differential findings in the IS deterrence literature and therefore warrant further discussion.

Operational definitions of deterrence theory

The deterrence literature provides two dominant approaches for modeling the theoretical effects of perceived sanction threats additive and multiplicative (Cochran *et al*, 2008). The additive approach models perceived certainty and severity of sanctions separately. The multiplicative approach models sanctions as the product of their perceived certainty and severity.

The additive approach is the most common in the deterrence literature, largely due to scholars' strong interest in the certainty component alone in deterrence theory (Paternoster, 2010). Advocates of the multiplicative approach argue that the *product* of perceived certainty and severity of sanctions is theoretically important because rational actors jointly consider the risk and cost of perceived punishment (Grasmick & Bursik, 1990). Specifically, perceived severity acts as a deterrent only when there is a high certainty of punishment. Likewise, certainty of punishment will have a greater deterrent effect when that punishment is perceived to be severe. Along these same lines, contemporary deterrence theory considers informal sanctions such as shame and embarrassment as more or less certain and severe and hence the total cost of these informal sanctions is the product of their certainty and severity (Cochran *et al*, 2008). Empirical results support the interaction of perceived certainty and severity of sanctions, at least for formal sanctions (e.g., Grasmick & Bryjak, 1980; Bachman *et al*, 1992; Antia *et al*, 2006).

Research also supports an interaction between perceived formal and informal sanctions (either in their additive or multiplicative forms) in the deterrence process (Paternoster & Simpson, 1993; Elis & Simpson, 1995). For example, Bachman *et al* (1992) found that perceived certainty of formal sanctions interacted with social censure (a form of informal sanction) in predicting sexual assault intentions among male college students.

As stated earlier, the question of whether the additive or multiplicative functional form is more appropriate for modeling the effects of perceived formal and informal sanctions is an ongoing debate in the deterrence literature (Cochran *et al*, 2008). We therefore take no stance on this issue. It is noteworthy, however, that a literature survey of deterrence studies found differing results for the influences of formal sanctions based on their functional form (i.e., additive or multiplicative) (Mendes & McDonald, 2001). As shown in online Appendix Table A2, IS deterrence studies have utilized both additive and multiplicative measures for formal and informal sanctions. We speculate that this contributed to the inconsistent results across these studies.

Also, even for those IS deterrence studies that utilized multiplicative sanction measures, the potential interactive effects of the perceived certainty and severity dimensions, as well as those of formal and informal sanctions as a whole, have not been directly addressed. We speculate that such interaction effects exist and can further explain some of the inconsistent findings. For example, for those studies that found a significant influence for perceived severity of sanctions (e.g., D'Arcy *et al*, 2009), one plausible explanation is that they contained a larger percentage of respondents who had equally high perceptions of getting caught.

Another issue involving the operational definition of deterrence theory is whether or not informal sanctions are included. Including informal sanctions in deterrence models has been shown to largely diminish the influence of formal sanctions (Pratt *et al*, 2006). A cursory review of the IS deterrence results shows a similar trend, as those studies that included both formal and informal sanctions (e.g., Higgins *et al*, 2005; Li *et al*, 2010; Siponen & Vance, 2010) do not provide strong support for formal sanctions. This may be partially due to the aforementioned interactive influences of formal and informal sanctions in the deterrence process.

A final related point is that some deterrence scholars have considered shame a separate construct (with its own certainty and severity dimensions) in addition to formal and informal sanctions (Grasmick & Bursik, 1990; Cochran *et al*, 2008). The rationale for separating shame from other informal sanctions is that it is a self-imposed cost that is quite influential in the deterrence process (Paternoster & Simpson, 1996). This influence is both direct and as a mediator between formal sanctions and behavior (Rebellon *et al*, 2010). We speculate that the omission of shame as an independent construct from the majority of IS deterrence studies (see Siponen & Vance, 2010 for exception) contributed to their mixed results. For example, involvement in certain negative computing-related behaviors may elicit different levels of anticipated shame across individuals. This unmeasured aspect of the deterrence process likely influenced respondents' projected and/or actual behaviors in IS deterrence studies.

Objective *vs* perceptual sanction measurement

A second methodological issue worthy of attention is that of perceptual *vs* objective measurement of formal sanctions. Several IS deterrence studies have utilized objective sanction measures based on the premise that objective sanctions correspond directly with individuals' perceptions of risk (Straub, 1990). Although the use of objective sanction measures is well-established in the criminological deterrence literature, especially for macro-level studies using aggregate data (Williams & Hawkins, 1986), we caution researchers against making direct comparisons of results of studies that utilized objective sanction measures to those that used perceptual measures. This is because perceptions of sanction characteristics can vary independently of objective sanction characteristics (Paternoster, 1987; Pogarsky *et al*, 2004).

This issue comes to light when examining the divergent findings of Kankanhalli *et al* (2003) and D'Arcy *et al* (2009) regarding the deterrent effect of formal sanction severity. Kankanhalli *et al* measured deterrent severity by asking IS managers to select their organization's most severe form of punishment meted out for IS security abuse. They did not find a significant relationship between deterrent severity and IS security effectiveness and concluded that 'organizations should focus their attention on deterrent and preventive efforts rather than deterrent severity' (p. 150). D'Arcy *et al* measured sanction severity via a direct, perceptual measure that asked respondents to assess how severe their punishment would be for engaging in IS misuse (composite of four scenarios). They found a significant negative relationship between perceived severity of formal sanctions and IS misuse intention and thereby concluded that organizations should emphasize severity of punishment in efforts to deter IS misuse. If we consider that objective sanction measures may not be directly proportional to individuals' perceptions of sanction threat, a plausible explanation for these contrasting findings is that the predefined severity categories in Kankanhalli *et al* (see online Appendix Table A3) do not directly correspond with the self-directed, perceptual severity measurement in D'Arcy *et al* More specifically, the more severe forms of punishment offered as response options in the Kankanhalli *et al* study (i.e., dismissal from appointment, prosecution in court) may not invoke fear in users. Considering that until recently convicted computer criminals have received relatively light sentences (Workman & Gathegi, 2007), this assertion has some credence.

In addition to the above studies, both Lee *et al* (2004) and D'Arcy & Hovav (2009) used various security countermeasures as proxies for perceived formal sanctions while Harrington (1996) used both general and IS-specific codes of ethics for the same purpose. In reviewing these studies, it is noteworthy that each found relatively weak influences of the deterrence constructs on the behavioral outcome variable. In Lee *et al* (2004), only the influence of security system was significant, while Harrington (1996) found only a slight influence of IS codes of ethics on one of five computer abuse behaviors. Similarly, none of D'Arcy *et al's* (2009) deterrence constructs were significant across both IS misuse behaviors examined. We speculate that the weak support for deterrence theory in these studies can be partially attributed to the use of objective sanction measures that may or may not be perceptually received by users. While perceptual measures are not an option in many organizational level studies that rely on aggregate data, they are conducive to individual level studies and provide a more direct test of deterrence theory. Hence, we advise researchers to utilize perceptual sanction measures in lieu of or in addition to objective sanction measures in individual level IS deterrence studies.

Self *vs* other-referenced perceived sanction measures

Another methodological issue that can potentially inform the mixed results in the IS deterrence literature is the different operationalizations of perceived certainty and severity of sanctions. In particular, more personalized sanction measures (i.e., what is the chance that *you* would be caught/arrested/punished) have been shown to produce stronger deterrent effects than those that are more general in nature and/or reference the sanction risk of others (Paternoster & Simpson, 1993; Bouffard *et al*, 2010). For example, some studies asked respondents to estimate the certainty and severity of punishment for 'people in general' or 'people like yourself', while others asked respondents to estimate these sanction risks for themselves (Grasmick & Bryjak, 1980). Comparisons of the two approaches have consistently shown that the self-reference measures produced results that are more supportive of deterrence theory.

In terms of the current analysis, this measurement distinction can provide insight into the divergent findings regarding the influence of perceived severity of formal sanctions in D'Arcy *et al* (2009) and Herath & Rao (2009a, b). Recall that in their full sample analysis, D'Arcy *et al* found support for perceived severity of formal sanctions in reducing IS misuse intention, while Herath and Rao found that perceived severity of penalty did not positively influence IS security policy compliance intention. In reviewing the measurement items in these studies (see online Appendix Table A3), two of the three items in Herath and Rao's perceived severity scale are 'other-reference' measures in that they pertain to the organization's disciplinary procedures for employees in general who violate security policies. D'Arcy *et al's* perceived severity measure consists of two items that gauge the perceived severity of punishment toward the specific scenario character. This is a more personalized measure if we assume that respondents projected themselves into the scenario situations (as instructed). Hence, a plausible explanation for the mixed findings is that Herath and Rao's measure was more 'other-referenced' while D'Arcy *et al's* was more 'self-referenced'.

Fixed *vs* open values for perceived severity of sanctions

Another issue involving the measurement of perceived severity of sanctions is how its value is estimated. Deterrence researchers have cautioned against the use of measures that provide a predefined list of possible penalties for respondents to choose from because such measures 'assume that a particular punishment has the same meaning for all people' (Grasmick & Bryjak, 1980, p. 475). The fallacy of this approach is that what is felt as extremely costly for one individual (e.g., $1000 fine) may be considered insignificant for another. As such, perceived severity measures that ask respondents to estimate their own values are recommended over those that supply fixed values (Bouffard *et al*, 2010). An example would be an item that asks respondents 'how severe would the formal punishment be' with response options ranging from 'not severe at all' to 'very severe'.

A review of the measurement items in online Appendix Table A3 reveals three individual level studies with perceptual severity of formal sanction measures that contain fixed penalty values: Higgins *et al* (2005), Pahnila *et al* (2007), and Siponen *et al* (2007). Each of these studies utilized adapted versions of the same measurement item that contained fixed penalty responses that ranged from 'no fine' to '5-year jail time'. Interestingly, the influence of perceived severity of formal sanction was not significant in Higgins *et al* (2005); the item was integrated into a composite (formal and informal) sanction measure in the other two studies, so we cannot disentangle its independent influence in these cases. We do note, however, that the combined sanction construct was not significant in Pahnila *et al* (2007) and marginally significant (and arguably below substantive significance) in Siponen *et al* (2007) Taken together, these findings are consistent with the notion that evaluations of the fixed perceived severity values were not constant across respondents, which may have diluted the statistical influence of perceived severity of formal sanctions in these studies.

Conceptual overlap among deterrence constructs

Yet another pertinent issue involving the perceived severity of sanction measure is its potential overlap with other deterrence theory constructs. In Paternoster's (1987) review of perceptual deterrence literature, he noted that Grasmick & Bryjak (1980) measured perceived severity of formal sanctions with an item that asked 'how big a problem that punishment would create for your life', while Paternoster & Iovanni (1986) used an identical measure to assess an informal sanction called perceived stigmatization from others. Likewise, Pogarsky & Piquero (2004) used a very similar measure to capture perceived risk of social disapproval and embarrassment. The difficultly in interpreting responses to items that ask 'how big a problem in your life' would getting caught/arrested/punished, etc. create is in ascertaining whether respondents answered in terms of formal punishment *per se*, in terms of the perceived informal consequences such as shame, embarrassment, or social disapproval, or in terms of some combination of these.

This issue may be particularly relevant to contemporary deterrence models that contain both formal and informal sanction constructs, as their independent influences can become obscured and lead to ambiguous results. Recent IS security literature (Higgins *et al*, 2005; Siponen & Vance, 2010) has considered informal sanctions such as social and self disapproval in line with contemporary deterrence theory. For instance, Siponen & Vance (2010) found that none of their deterrence constructs formal sanctions, informal sanctions, shame were significant predictors of IS security policy violation intention. Although the authors suggest that the inclusion of neutralization constructs within their model likely explains the nonsignificance of the deterrence constructs (i.e., the deterrent effect of sanctions may be overshadowed when employees invoke neutralization techniques), we also speculate that their measurement of perceived severity of formal sanctions (i.e., 'how much a problem would it create in your life if you were formally reprimanded') (see online Appendix Table A3) in relation to the other deterrence constructs may provide some explanation. It is plausible that the formal sanction severity item responses overlapped to some degree with those of the informal sanction and shame constructs, which may have partially offset the independent influences of all three deterrence constructs.

Table 2 provides a summary of key points and recommendations pertaining to the methodological issues discussed in this section.

Additional substantive issues

As a third and final approach in evaluating the inconsistent findings across IS deterrence studies, we assessed the deterrence literature in search of potential issues, beyond those addressed in the previous sections, that could provide additional insights. This is in line with Robey & Boudreau's (1996) strategy of conducting better reviews on substantive research questions that is suggested for resolving inconsistent findings across studies.

Positive *vs* negative outcome variable

The first issue involves the application of deterrence theory to positive *vs* negative user behavior. By negative behavior, we are referring to behavior that is considered disruptive of IS security, such as IS misuse in D'Arcy *et al* (2009) or security policy violation in Siponen & Vance (2010). By positive behavior, we are referring to behavior that is supportive of IS security such as policy compliance in Herath & Rao (2009a, b). The original conceptualization of deterrence theory focused on predicting a specific set of intentions, namely those directed at lawbreaking (Gibbs, 1975). Indeed, our own review (albeit not exhaustive) of the deterrence literature indicates that deterrence theory has mostly been used to predict negative outcome variables in the form of criminal/deviant behavior. One notable exception, detailed in

Table 2 Methodological issues key points and recommendations

Methodological issue	*Key points and recommendations*
Operational definitions of deterrence theory	• Additive *vs* multiplicative measures of perceived sanctions may produce differing results (Mendes & McDonald 2001) • Assessing formal sanctions and informal sanctions in the same model tends to weaken the deterrent influence of formal sanctions (Pratt *et al*, 2006) • We recommend more inclusive multiplicative deterrence models that account for interactions between formal and informal sanctions and shame, and their individual certainty and severity dimensions
Objective *vs* perceptual sanction measurement	• Perceptions of sanction characteristics can vary independently of objective sanction characteristics (Paternoster, 1987; Pogarsky *et al*, 2004) • We caution against direct comparisons of results of IS deterrence studies that used objective sanction measures to those that used perceptual sanction measures • We recommend using perceptual sanction measures in lieu of or in addition to objective sanction measures in individual level IS deterrence studies
Self *vs* other referenced perceived sanction measures	• Personalized sanction measures (i.e., what is the chance that *you* would be caught) have stronger inverse relationships with criminal/deviant behavior compared with more general measures that reference others' sanction risk (Bouffard *et al*, 2010) • We do not recommend a particular approach but caution against direct comparisons of self *vs* other referenced sanction measures • Self referenced sanction measures should produce results that are more supportive of deterrence theory (Paternoster & Simpson, 1993; Bouffard *et al*, 2010)
Fixed *vs* open values for perceived severity of sanctions	• Perceived severity of sanction measures that supply fixed values (e.g., $1000 fine) are problematic because they assume the penalty is equally costly to all respondents (Grasmick & Bryjak, 1980; Bouffard *et al*, 2010) • We recommend asking respondents to estimate their own value as opposed to supplying a predefined list of possible penalties • For example, an item that asks 'how severe would the formal punishment be' with response options ranging from 'not severe at all' to 'very severe'
Conceptual overlap among deterrence constructs	• Formal sanction measures that ask 'how big a problem in your life' would getting caught/ punished/arrested, etc. may be interpreted in terms of both formal and informal sanctions (Paternoster, 1987) • We recommend extensive pretesting and validation of formal and informal sanction measures to limit conceptual overlap and ensure they are tapping distinct constructs

Paternoster & Simpson (1996), is a study of compliance intentions among Australian nursing home managers. The researchers in that study found that perceived formal sanctions had a negligible influence on intention to comply with nursing home regulations, causing them to conclude that 'there is a stark failure of deterrence to explain compliance with regulatory law' (p. 552).

A handful of IS deterrence studies have used deterrence theory to predict positive user behaviors. The premise being that individuals' fear of sanctions can promote desirable compliance behaviors in an organization (Herath & Rao, 2009a, b). Interestingly, similar to the Australian nursing home study, studies that used positive outcome variables have generally shown a weak deterrent effect for sanctions. For example, sanctions were not a significant predictor of IS security policy compliance intention in Pahnila *et al* (2007) and had very weak statistical influence in Siponen *et al* (2007). Similarly, only one of the three formal sanction proxy variables was a significant predictor of IS security intention in Lee *et al* (2004). Herath and Rao's studies did show more promising results as perceived certainty of detection significantly predicted policy compliance intention. However, perceived severity of penalty did not have a deterrent effect in their studies. Similarly, Li *et al* (2010) found that perceived detection probability, but not perceived formal sanction severity, was significantly associated with Internet usage policy compliance intention.

Considering the relatively weak influence of sanctions in studies of positive outcome variables, it could be that deterrence theory is more suitable for predicting negative user behaviors, similar to its application in the bulk of the deterrence literature. Social control theory, for example, argues that attachment to conventional norms, and not so much the threat of sanctions, is really what drives conformity (Cao, 2004). Along these lines, Herath & Rao (2009a) found that both the expectations from relevant others such as supervisors, peers, and IS personnel, and the perceived behavior of similar others, were significant contributors to employee intentions to comply with security policies.

There is also evidence that sanctions have an indirect influence on IS security policy compliance through variables such as attitude, perceived behavioral control, and subjective norms (Liao *et al*, 2009; Bulgurcu *et al*, 2010). Hence, the influence of sanctions on positive behaviors may be more indirect while their influence on negative behaviors is direct. At this point we cannot determine if positive behavior is indeed 'one step removed' from the predictive reach of deterrence theory. Future research is needed to achieve clarity on this issue.

Benefit portion of the rational decision process/severity of the behavior

As a second issue, we posit that a more comprehensive theoretical lens that considers both positive and negative incentives can provide insight into the inconsistent IS deterrence findings. According to rational choice theory, an individual determines how he/she will act by balancing the perceive costs and benefits of the act (Simpson *et al*, 2002). In the criminal/deviant behavior context, such behavior will occur when the perceived benefits of the act outweigh its perceived costs (Pratt *et al*, 2006). Deterrence theory is essentially a subset of rational choice theory that pertains to the perceived cost portion of the rational decision process.

As shown in online Appendix Tables A1 and A3, with the exception of Li *et al* (2010), IS deterrence research is limited to the cost portion of rational decision process by assessing the deterrent effect of formal and/or informal sanctions. Accounting for the unmeasured benefit portion of the rational decision process may shed light on the differential influences of sanctions across IS deterrence studies. This is because perceived benefits likely vary depending on the behavior in question, which in turn affects the magnitude of the sanctions-to-behavior relationship. For instance, in terms of IS security policy compliance/non-compliance studies, research indicates that employees routinely violate security policies because they want to expedite their own work and increase their productivity (Predd *et al*, 2008; Li *et al*, 2010). Hence, time saving presumably has a strong influence on the benefit portion of the cost-benefit assessment for security policy compliance decisions, and perhaps overrides the perceived cost of sanctions if one considers that policy violations are often handled internally without involving legal action or law enforcement (CSO/CERT/Deloitte, 2010). This may explain why formal sanctions have shown weaker deterrent effects in most studies of IS security policy compliance/non-compliance.

On the other hand, the perceived cost portion of the rational decision process may weigh heavier for those less common behaviors that are more disruptive of IS security, such as intentional abuse of IS resources, because employees likely perceive stronger negative consequences (i.e., stiffer penalties) for engaging in such activity. This is in line with findings that the threat of punishment is more important in deterring serious criminal activity than in deterring minor offenses (Paternoster, 1987; Pogarsky & Piquero, 2004).

Certain IS deterrence studies support this notion, as formal sanction constructs have been shown to negatively influence software piracy (e.g., Gopal & Sanders, 1997), computer sabotage (Harrington, 1996), and unauthorized access intentions (Skinner & Fream, 1997) three behaviors that are illegal. That said, the evidence is less than convincing because it is difficult to discern how severe the respondents perceived the different behaviors. A quick glance at the negative outcome variables in online Appendix Tables A1 and A3 indicates a diversity of behaviors that may be construed as more or less serious by users depending on a number of circumstances. At any rate, evidence in the deterrence literature suggests that more severe negative user behaviors are more amenable to deterrent techniques and therefore we encourage researchers to be mindful of this when executing IS deterrence investigations. Failure to do so may lead to an erroneous conclusion that 'deterrence does not work' in the IS security context.

Generalizability of deterrence theory constructs

Another issue involves the generalizability of deterrence constructs, and deterrence theory in general, across specific behaviors. In an early paper, Silberman (1976) proposed a general theory of criminal deterrence based on the notion that deterrence is built around perceived sanctions that pertain to a set of behaviors rather than a specific act. To this end, Silberman argued for the use of general indices of perceived sanctions and criminal/deviant behavior in deterrence studies. Comparisons of studies with composite indices to those with offense-specific items support this generalized notion of deterrence theory in that the former produced consistently larger inverse correlations between the deterrence constructs and criminal/deviant behavior (Paternoster, 1987; Pratt *et al*, 2006). Similarly, certain IS deterrence studies have used general indices and found that they significantly predicted a variety of IS misuse behaviors (Skinner & Fream, 1997; D'Arcy *et al*, 2009).

However, a counterargument can be made that a general theory of deterrence, and its associated indices of deterrence constructs, is not suitable across all behaviors in the IS security realm. Take, for example, the broad classification of IS misuse behaviors *vs* the more specific security policy violations. Perhaps these are distinct phenomena, especially from the user perspective, because a misuse of IS resources is not necessarily a violation of security policy. Hence, a generalized deterrence framework that explains IS abuse/misuse may not translate to the narrower domain of security policy violations.

In surveying the results in online Appendix Tables A1 and A3, there is evidence that a general theory of deterrence, at least in terms of the relative influences of

Table 3 Additional substantive issues key points and recommendations

Additional substantive issue	*Key points and recommendations*
Positive *vs* negative outcome variable	• Deterrence theory was originally conceptualized to predict criminal and deviant behavior (Gibbs, 1975) • Evidence suggests that deterrence theory is a better predictor of negative behaviors such as abuse of IS resources as opposed to positive (compliant) behaviors • Impact of sanctions on compliant behaviors may be indirect (e.g., Liao *et al*, 2009; Bulgurcu *et al*, 2010)
Benefit portion of the rational decision process	• Rational choice theory posits that the decision to engage in illicit behavior is a function of the perceived costs and benefits of the act (Simpson *et al*, 2002) • IS deterrence literature has largely excluded the perceived benefit portion of the rational decision process • We recommend measuring the perceived benefits of the behavior(s) under investigation in conjunction with perceived sanctions in IS deterrence studies
Severity of the behavior	• Perceived costs and benefits of an act will likely vary depending on its perceived severity in the mind of the user • Evidence suggests that more severe negative user behaviors are more amenable to the threat of sanctions (Paternoster, 1987; Pogarsky & Piquero, 2004) • Perceived benefits may have a stronger influence than perceived sanctions for lesser severity behaviors, such as minor security policy violations • Perceived sanctions may have a stronger influence than perceived benefits for more serious behaviors, such as intentional abuse of IS resources
Generalizability of deterrence theory constructs	• Some evidence of the usefulness of general indices of deterrence constructs in IS deterrence literature (Skinner & Fream, 1997; D'Arcy *et al*, 2009) • Studies of software/digital piracy suggest that the deterrent influence of perceived certainty and severity of formal sanctions is not consistent across all user behaviors • We recommend exploring the differential influences of perceived certainty and severity of formal and informal sanctions on different user behaviors to better illuminate deterrence theory in the IS context

perceived certainty and severity of formal sanctions, is not suitable across all IS security-related behaviors. In particular, in three of the four studies of software/digital piracy in which both perceived certainty and severity of formal sanctions were included as separate constructs, only perceived certainty was significant. Another study by Hollinger (1993) included only the perceived certainty construct and found that it was significantly associated with software piracy but not unauthorized access. Corroborating these findings, there is suggestive evidence that perceived certainty of formal sanctions is a key predictor of software and digital piracy, while perceived severity is not.

This raises some doubt regarding the utility of a generalized theory of deterrence across a variety of user behaviors. At the very least there is evidence that the application of deterrence theory to piracy behavior is unique from other user behaviors. Hence, researchers may need to develop more nuanced arguments for hypotheses concerning deterrence constructs in the IS security context. This and other issues raised in this section are summarized in Table 3.

Research guidelines and opportunities

In the previous sections, we identified a set of contingency variables and methodological and theoretical issues that can help explain the inconsistent findings in the IS deterrence literature. In doing so, we uncovered several issues that should be considered by researchers going forward in this area. To this end, the following subsections present pertinent research guidelines and opportunities related to the key facets of the paper.

Contingency variables

IS researchers utilizing deterrence theory should be aware of various contingency factors that may influence their findings. Failure to do so may lead to ambiguous results or results that are contrary to what is expected. We have identified five such contingency variables that should be considered for inclusion in IS deterrence models: self control, CSE, moral beliefs, virtual status, and employee position. Researchers can include these as covariates or as moderator variables depending on theoretical considerations. Either way, accounting for such contingent influences will better isolate the deterrent effects of sanction constructs.

Given the strong theoretical and empirical support for moral beliefs as a moderator in deterrence theory, we consider its inclusion essential in any IS deterrence model. We also recommend accounting for virtual status in research contexts where the virtual component of the workforce is strong. Likewise, accounting for CSE is important when research samples contain respondents with varying degrees of computer skills and abilities. As research indicates that task-specific CSE measures that are closely aligned with the domain under study have stronger predictive power than a general CSE measure (Marakas *et al*, 2007), we recommend measuring self-efficacy in the IS security context or in the specific context of the behavior under investigation. A good example of this is Bulgurcu *et al's* (2010) measure of self-efficacy to comply with security policy.

Beyond the five contingency factors presented in this paper, there are others that should be considered for future studies. For example, Harrington (1996) found that the individual personality trait denial of responsibility moderated the influence of both general and IS-specific codes of ethics on computer abuse intentions. The deterrence literature also provides evidence the prior criminal experience erodes the deterrent effect of sanctions (Pogarsky & Piquero, 2004; Wright *et al*, 2004).

Moving forward, we encourage IS researchers to integrate individual and situational variables with formal and informal sanction constructs to develop more comprehensive IS deterrence models. Such efforts are in line with calls from criminologists to continue refining deterrence theory by understanding the conditions under which the threat of sanctions is likely to influence behavior (Pratt *et al*, 2006; Jacobs, 2010). We caution, however, against integrating individual and situational variables into IS deterrence frameworks without a fundamental rationale for their inclusion. The integration should be well justified on theoretical grounds and the different theories or their constructs should be compatible and operate at the same level of abstraction (Thornberry, 1989).

Methodological issues

We submit that in large part the disparate findings in the IS deterrence literature reflect the various ways in which the sanction constructs have been measured and their treatment (e.g., separate constructs, combined indexes, inclusion of informal sanctions). Researchers need to consider these issues and recognize that in some cases direct comparisons of findings across IS deterrence studies are not appropriate. Progress in this area is contingent upon researchers striving for greater consistency in their measurement and treatment of sanction constructs when applying deterrence theory to the IS security domain.

To this end, IS researchers should expand their operational definitions of deterrence theory to be consistent with advances in the broader deterrence literature. First, in light of research indicating that shame has a strong influence in the deterrence process, this construct should be considered for inclusion in any individual-level IS deterrence model. We also recommend more inclusive multiplicative models that include interactions between formal and informal sanctions and shame, and their individual certainty and severity dimensions. The work of Cochran *et al* (2008) and Elis & Simpson (1995) in the deterrence literature can serve as exemplars in this regard.

From an operationalization perspective, future research is needed to assist scholars in measuring and applying sanctions in IS deterrence studies. One option is to design an empirical study that compares different ways to measure sanctions using the same population. The study could utilize a large sample with respondents randomly assigned to different groups, with each group subjected to different measurements for sanctions. For example, the different sanction 'treatments' could consist of objective *vs* perceptual measures, self-reference *vs* other-reference measures, and measures with fixed penalty values *vs* those that ask respondents to estimate their own values. This approach would control for differences in response rates, sample characteristics, organizational and country cultures, constructs in the model, anonymity of the survey, and statistical techniques. An alternative approach would be to design a single survey instrument with the various types of sanction measures included. However, this would presumably require a lengthy instrument, thus risking respondent fatigue and common method effects in the results.

We also recommend extensive pretesting and validation of sanction construct measures to ensure that conceptual overlap is not obscuring their individual influences. This is particularly important for contemporary deterrence frameworks that require informal sanction measures such as guilt, shame, and social disapproval.

Additional substantive issues

The discussion of additional substantive issues points to several research opportunities that can help advance deterrence theory in the IS security context. Certain methodological guidelines can also be offered. Namely, researchers should be wary of using generalized measures of deterrence constructs across a range of behaviors that may represent different phenomena in the minds of users. Doing so may result in models that lack adequate explanatory power. However, generalized measures are appropriate when the researcher is interested in assessing the impact of sanctions across similar behaviors. As a validation check, researchers can ask respondents to rate their outcome variables in terms of severity, benefits, etc. to determine whether the behaviors are perceived as closely related.

Along these lines, future research should apply deterrence theory across a variety of user behaviors that vary in terms of the above characteristics. Based on the evidence discussed earlier, it may be that positive and negative user behaviors such as security policy compliance and IS misuse are not exactly two sides of the same coin and thus have a different set of antecedents. Research should also investigate whether IS deterrence models require more nuanced arguments other than simply 'both perceived certainty and severity of formal and informal sanctions influence behavior' depending on the behavior in question. This again speaks to the need for more inclusive multiplicative models that incorporate interaction hypotheses.

We also recommend that IS deterrence studies incorporate the more comprehensive rational choice framework that accounts for both positive and negative consequences of behavior, especially since research indicates that perceived benefits have a strong influence on corporate offending decisions (Simpson *et al*, 2002). Assessing the impact of sanctions along with the competing influences of positive incentives provides a more complete understanding of the deterrence process.

Finally, related to an earlier point, future research should incorporate celerity of sanctions into IS deterrence frameworks to determine whether this seldom explored component of deterrence theory has explanatory power in the IS security context. For example, in line with our call for more inclusive deterrence models, future research can explore the interactive influences of the certainty, severity, and celerity dimensions of formal and informal sanctions and shame.

Conclusion

It has been over two decades since Straub (1990) published a seminal study that applied deterrence theory to IS security to assess the effectiveness of deterrent countermeasures in reducing incidents of computer abuse. Since then deterrence theory has informed a sizeable body of IS security research, particularly behavioral studies. Although this body of work has contributed significant theoretical insight and practical knowledge to the IS security field, it has also been plagued by inconsistent and sometimes contradictory findings. In this paper, we set out to make greater sense of the discrepant findings in the IS deterrence literature by drawing upon the more mature body of deterrence literature that spans multiple disciplines, with particular emphasis on the criminological deterrence research.

The impetus for this paper came from the seemingly divergent findings from our own set of studies. Upon reviewing the broader IS deterrence literature, we discovered similar equivocality throughout much of this work. As a first step in trying to explain the murky findings, we identified five potential moderators of the impact of sanctions on IS security-related behavioral outcomes. If these and potentially other moderating influences exist and are not accounted for in studies, the results will likely suffer from some degree of inaccuracy. Secondly, we indentified a series of methodological issues involving the measurement and treatment of deterrence constructs. The methodological issues presented here shed light on many of the discrepant findings across IS deterrence studies and can inform future research in this area. Finally, we identified substantive theoretical issues concerning IS deterrence studies that provide further insight into the mixed findings. One issue in particular is that extant IS deterrence investigations have focused largely on one side of the rational decision process, that is, the perceived costs with little regard for the competing influence of perceived benefits.

In closing, we believe that the equivocality of the IS deterrence literature warranted an in-depth review and analysis of this work. Gaining a better understanding of when and where deterrence works within IS settings is necessary for both theoretical purposes and practice. Absent such clarification, scientific knowledge about deterrence theory in the IS security realm will remain incomplete. Furthermore, accompanying policies and procedures will be guided more by faith than fact. We hope that the contents of this paper are a useful contribution and a step in the right direction along these lines.

About the authors

John D'Arcy is an assistant professor in the Department of Management at the University of Notre Dame. He received his Ph.D. from Temple University. His research areas include information assurance and security. His research has been published in journals such as *Information Systems Research*, *Communications of the ACM*, and *Decision Support Systems*.

Tejaswini Herath is an assistant professor in the Faculty of Business at Brock University. She received her Ph.D. from SUNY Buffalo. Her research interests include information security and privacy and economics of information security. Her research has been published in journals such as *Journal of Management Information Systems*, *European Journal of Information Systems*, and *Decision Support Systems*.

References

ANTIA KD, BERGEN ME, DUTTA S and FISHER RJ (2006) How does market enforcement deter gray market incidence? *Journal of Marketing* **70(1)**, 92 106.

BACHMAN R, PATERNOSTER R and WARD S (1992) The rationality of sexual offending: testing a deterrence/rational choice conception of sexual assault. *Law & Society Review* **26(2)**, 343 372.

BECCARIA C (1963) *On Crimes and Punishment*. Macmillan, New York.

BOUFFARD JA, EXUM ML and COLLINS PA (2010) Methodological artifacts in tests of rational choice theory. *Journal of Criminal Justice* **38(4)**, 400 409.

BULGURCU B, CAVUSOGLU H and BENBASAT I (2010) Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly* **34(3)**, 523 548.

CAO L (2004) *Major Criminological Theories: Concepts and Measurement*. Wadsworth, Belmont, California.

CHIDAMBARAM L and TUNG LL (2005) Is out of sight, out of mind? an empirical study of social loafing in technology-supported groups. *Information Systems Research* **16(2)**, 149 168.

COCHRAN JK, ALEKSA V and SANDERS BA (2008) Are persons low in self-control rational and deterrable? *Deviant Behavior* **29(5)**, 461 483.

CSO/CERT/DELOITTE (2010) Cybersecurity watch survey. [WWW document] http://www.cert.org/insider threat (accessed 1 May 2011).

D'ARCY J and HOVAV A (2009) Does one size fit all? examining the differential effects of IS security countermeasures. *Journal of Business Ethics* **89(1)**, 59 71.

D'Arcy J, Hovav A and Galletta DF (2009) User awareness of security countermeasures and its impact on information systems misuse: a deterrence perspective. *Information Systems Research* **20(1)**, 79 98.

Elis LA and Simpson S (1995) Informal sanction threats and corporate crime: additive versus multiplicative models. *Journal of Research in Crime and Delinquency* **32(4)**, 399 424.

Ernst and Young (2009) 12th annual global information security survey. [WWW document] http://www.ey.com (accessed 1 May 2011).

Gibbs JP (1975) *Crime, Punishment, and Deterrence*. Elsevier, New York.

Gopal RD and Sanders GL (1997) Preventative and deterrent controls for software piracy. *Journal of Management Information Systems* **13(4)**, 29 47.

Grasmick HG and Bryjak GJ (1980) The deterrent effect of perceived severity of punishment. *Social Forces* **59(2)**, 471 491.

Grasmick HG and Bursik R (1990) Conscience, significant others, and rational choice: extending the deterrence model. *Law and Society Review* **24(3)**, 837 861.

Grasmick HG, Tittle R, Bursik J and Arneklev B (1993) Testing the core implications of Gettfredson and Hirschi's general theory of crime. *Journal of Research in Crime and Delinquency* **30(1)**, 5 29.

Harrington SJ (1996) The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. *MIS Quarterly* **20(3)**, 257 278.

Herath T and Rao HR (2009a) Protection motivation and deterrence: a framework for security policy compliance in organizations. *European Journal of Information Systems* **18(2)**, 106 125.

Herath T and Rao HR (2009b) Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness. *Decision Support Systems* **47(2)**, 14 165.

Higgins G, Wilson A and Fell B (2005) An application of deterrence theory to software piracy. *Journal of Criminal Justice and Popular Culture* **12(3)**, 166 184.

Hollinger RC (1993) Crime by computer: correlates of software piracy and unauthorized account access. *Security Journal* **4(1)**, 2 12.

Jacobs BA (2010) Deterrence and deterrability. *Criminology* **48(2)**, 417 441.

Kankanhalli A, Teo H-H, Tan BCY and Wei K-K (2003) An integrative study of information systems security effectiveness. *International Journal of Information Management* **23(2)**, 139 154.

Klepper S and Nagin DS (1989) The deterrent effect of perceived certainty and severity of punishment revisited. *Criminology* **27(4)**, 721 746.

Kohlberg L (1969) Stage and sequence: the cognitive developmental approach to socialization. In *Handbook of Socialization Theory* (Goslin DA, Ed.), pp 347 380, Rand McNally, Chicago.

Kruegar NJ and Dickson PR (1994) How believing in ourselves increases risk taking: perceived self-efficacy and opportunity recognition. *Decision Sciences* **25(3)**, 385 400.

Lee SM, Lee S-G and Yoo S (2004) An integrative model of computer abuse based on social control and general deterrence theories. *Information and Management* **41(6)**, 707 718.

Li H, Zhang J and Sarathy R (2010) Understanding compliance within internet use policy from the perspective of rational choice theory. *Decision Support Systems* **48(4)**, 635 645.

Liao Q, Gurung A, Luo X and Li L (2009) Workplace management and employee misuse: does punishment matter? *Journal of Computer Information Systems* **50(2)**, 49 59.

Loch KD and Conger S (1996) Evaluating ethical decision making and computer use. *Communications of the ACM* **39(7)**, 74 83.

Mann RE, Smart RG, Stoduto G, Adlaf EM, Vingilis E, Beirness D, Lamble R and Ashbridge M (2003) The effects of drinking-driving laws: a test of the differential deterrence hypothesis. *Addiction* **98(11)**, 1531 1536.

Marakas GM, Johnson RD and Clay PF (2007) The evolving nature of the computer self-efficacy construct: an empirical investigation of measurement construction, validity, reliability and stability over time. *Journal of the Association for Information Systems* **8(1)**, 16 46.

McCloskey DW and Igbaria M (2003) Does 'out of sight' mean 'out of mind'? an empirical investigation of career advancement prospects of telecommuters. *Information Resources Management Journal* **16(2)**, 19 34.

Mendes SM and McDonald MD (2001) Putting severity of punishment back in the deterrence package. *Policy Studies Journal* **29(4)**, 588 610.

Mercuri RT (2003) Analyzing security costs. *Communications of the ACM* **46(6)**, 15 18.

Myyry L, Siponen M, Pahnila S, Vartiainen T and Vance A (2009) What levels of moral reasoning and values explain adherence to information security rules? an empirical study. *European Journal of Information Systems* **18(2)**, 1 14.

Nagin DS and Pogarsky G (2001) Integrating celerity, impulsivity, and extralegal sanction threats into a model of general deterrence: theory and evidence. *Criminology* **39(4)**, 865 891.

Pahnila S, Siponen M and Mahmood A (2007) Employees' behavior towards IS security policy compliance. In *Proceedings of the 40th Annual Hawaii International Conference on System Sciences*, Hawaii, USA.

Paternoster R (1987) The deterrence effect of perceived certainty and severity of punishment: a review of the evidence and issues. *Justice Quarterly* **4(2)**, 173 217.

Paternoster R (2010) How much do we really know about criminal deterrence? *The Journal of Criminal Law and Criminology* **100(3)**, 765 823.

Paternoster R and Iovanni L (1986) The deterrent effect of perceived severity: a reexamination. *Social Forces* **64**, 751 777.

Paternoster R and Simpson S (1993) A rational choice theory of corporate crime. In *Routine Activities and Rational Choice: Advances in Criminological Theory, Volume 5* (Clarke RV and Felson M, Eds), pp 37 58, Transaction Publishers, New Brunswick, NJ.

Paternoster R and Simpson S (1996) Sanction threats and appeals to morality: testing a rational choice model of corporate crime. *Law & Society Review* **30(3)**, 549 584.

Pinsonneault A and Heppel N (1998) Anonymity in group support systems research: a new conceptualization, measure, and contingency framework. *Journal of Management Information Systems* **14(3)**, 89 108.

Piquero A and Tibbetts S (1996) Specifying the direct and indirect effects of low self-control and situational factors in offenders decision making: toward a more comparative model of rational offending. *Justice Quarterly* **13(3)**, 481 510.

Pogarsky G and Piquero AR (2004) Studying the reach of deterrence: can deterrence theory help explain police misconduct? *Journal of Criminal Justice* **32(4)**, 371 386.

Pogarsky G, Piquero AR and Paternoster R (2004) Modeling change in perceptions about sanction threats: the neglected linkage in deterrence theory. *Journal of Quantitative Criminology* **20(4)**, 343 369.

Postmes T and Spears R (1998) Deindividuation and antinormative behavior: a meta-analysis. *Psychological Bulletin* **123(3)**, 238 259.

Pratt TC and Cullen FT (2000) The empirical status of Gottfredson and Hirschi's general theory of crime: a meta-analysis. *Criminology* **38**, 931 964.

Pratt TC, Cullen FT, Blevis KR, Daigle LE and Madensen TD (2006) The empirical status of deterrence theory: a meta-analysis. In *Taking Stock: The Status of Criminological Theory* (Cullen FT, Wright JP and Blevins KR, Eds), pp 37 76, Transaction Publishers, New Brunswick, NJ.

Predd J, Pfleeger SL, Hunker J and Bulford C (2008) Insiders behaving badly. *IEEE Security & Privacy* **6(4)**, 66 70.

PwC/CSO/CIO (2010) The global state of information security. [WWW document] http://www.pwc.com/en GX/gx/information-security-survey/pdf/pwcsurvey2010 cio reprint.pdf (accessed 1 May 2011).

Rebellon CJ, Piquero NL, Piquero AR and Tibbetts SG (2010) Anticipated shaming and criminal offending. *Journal of Criminal Justice* **38(5)**, 988 997.

Robey D and Boudreau MC (1996) Accounting for the contradictory organizational consequences of information technology: theoretical directions and methodological implications. *Information Systems Research* **10(2)**, 167 185.

Schoepfer A and Piquero AR (2006) Self-control, moral beliefs, and criminal activity. *Deviant Behavior* **27(1)**, 51 71.

Silberman M (1976) Toward a theory of criminal deterrence. *American Sociological Review* **41(3)**, 442 461.

Simpson S, Piquero N and Paternoster R (2002) Rationality and corporate offending decisions. In *Rational Choice and Criminal Behavior: Recent Research and Future Challenges* (Piquero AR and Tibbetts SG, Eds), pp 25 39, Routledge, New York.

Siponen M and Vance A (2010) Neutralization: new insights into the problem of employee information systems security policy violations. *MIS Quarterly* **34(3)**, 487 502.

Siponen M, Pahnila S and Mahmood A (2007) Employees' adherence to information security policies: an empirical study. In *International Federation* *for Information Processing, Volume 232, New Approaches for Security, Privacy and Trust in Complex Environments* (Venter H, Eloff M, Labuschagne L, Eloff J and Von Solms R Eds), pp 133 144, Springer, Boston, MA.

Siponen M, Willison R and Baskerville R (2008) Power and practice in information systems security research. In *Proceedings of the International Conference on Information Systems* , pp 14 17, Paris, France.

Skinner WF and Fream AM (1997) A social learning theory analysis of computer crime among college students. *Journal of Research in Crime and Delinquency* **34(4),** 495 518.

Smith NC, Simpson SS and Huang C-Y (2007) Why managers fail to do the right thing: an empirical study of unethical and illegal conduct. *Business Ethics Quarterly* **17(4),** 633 667.

Straub DW (1990) Effective IS security: an empirical study. *Information Systems Research* **1(3),** 255 276.

Theoharidou M, Kokolakis S, Karyda M and Kiountouzis E (2005) The insider threat to information systems and the effectiveness of ISO17799. *Computers & Security* **24(6),** 472 484.

Thornberry TP (1989) Reflections on the advantages and disadvantages of theoretical integration. In *Theoretical Integration in the Study of Deviance and Crime* (Messner SF, Krohn MD, and Liska AE, eds.), pp 51 60, State University of New York Press, Albany, NY.

Tittle CR (1980) *Sanctions and Social Deviance: The Question of Deterrence*. Praeger, New York.

Trevino LK, Weaver GR and Reynolds SJ (2006) Behavioral ethics in organizations: a review. *Journal of Management* **32(6),** 951 990.

United Nations (2005) Information economy report 2005. [WWW document] http://www.unctad.org/en/docs/sdteecb20051overview en .pdf (accessed 1 May 2011).

Warkentin M and Willison R (2009) Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems* **18(2),** 101 105.

Wiesenfeld B, Raghuram S and Garud R (1999) Communication patterns as determinants of organizational identification in a virtual organization. *Organization Science* **10(6),** 777 790.

Williams KR and Hawkins R (1986) Perceptual research on general deterrence: a critical review. *Law & Society Review* **20(4),** 545 572.

Workman M and Gathegi J (2007) Punishment and ethics deterrents: a study of insider security contravention. *Journal of the American Society for Information Science and Technology* **58(2),** 212 222.

Wright BRE, Caspi A, Moffitt TE and Paternoster R (2004) Does the perceived risk of punishment deter criminally prone individuals? rational choice, self-control, and crime. *Journal of Research in Crime and Delinquency* **41(2),** 180 213.

Zhang L, Smith WW and McDowell WC (2006) Examining digital piracy: self-control, punishment, and self-efficacy. *Information Resources Management Journal* **22(1),** 24 44.

Zimbardo PG (1969) The human choice: individuation, reason, and order versus deindividuation, impulse, and chaos. In *Nebraska Symposium on Motivation* (Arnold WJ and Levine D, Eds), pp 237 307, University of Nebraska Press, Lincoln, Nebraska.

Supplementary Information accompanies the paper on *European Journal of Information Systems* website (http://www.palgrave.com/ejis)