AJ Burns, Tom L. Roberts, Clay Posey, Paul Benjamin Lowry, and Bryan Fuller (2022). "Going beyond deterrence: A middle-range theory of motives and controls for insider computer abuse," ***Information Systems Research (ISR)*** (accepted 28-Mar-2022)

If you have any questions, would like a copy of the final version of the article, or would like copies of other articles we've published, please contact any of us directly, as follows:

- **Dr. AJ Burns**
  - Stephenson Department of Entrepreneurship and Information Systems
  - Louisiana State University
  - Email: ajburns@lsu.edu
  - Website: https://www.lsu.edu/business/about/profile-viewer.php?un=ajburns
- **Prof. Tom L. Roberts**
  - Professor of Computer Science
  - Department: Computer Science
  - University of Texas at Tyler
  - Email: troberts2@uttyler.edu
  - Website: http://www.uttyler.edu/directory/cs/troberts.php
- **Dr. Clay Posey**
  - Associate Professor of Information Systems
  - Marriott School of Business, Brigham Young University
  - Email: clay.posey@byu.edu
  - Website: https://marriott.byu.edu/directory/details?id=77459
- ***Prof. Paul Benjamin Lowry,** Eminent Scholar and Suzanne Parker Thornhill Chair Professor
  - Business Information Technology, Pamplin College of Business
  - Virginia Tech
  - Email: Paul.Lowry.PhD@gmail.com
  - Website: https://sites.google.com/site/professorlowrypaulbenjamin/home
  - System to request Paul's articles: https://seanacademic.qualtrics.com/SE/?SID=SV_7WCaP0V7FA0GWWx
- **Prof. Bryan Fuller**
  - Humana/McCallister Endowed Professorship of Management and Marketing
  - Louisiana Tech University
  - Email: bfuller@latech.edu
  - Website: https://business.latech.edu/personnel-directory/single-entry/name/bryan-fuller/

*corresponding author

Going Beyond Deterrence: A Middle-Range Theory of Motives and Controls for Insider Computer Abuse

Abstract. Despite widespread agreement among practitioners and academicians that organizational insiders are a significant threat to organizational information systems security, insider computer abuse (ICA)—unauthorized and deliberate misuse of organizational information resources by organizational insiders—remains a serious issue. Recent studies have shown that most employees are willing to share confidential or regulated information under certain circumstances and nearly a third to half of major security breaches are tied to insiders. These trends indicate that organizational security efforts, which generally focus on deterrence and sanctions, have yet to effectively address ICA. Therefore, leading security researchers and practitioners have called for a more nuanced understanding of insiders in respect to deterrence efforts. We answer these calls by proposing a middle-range theory of ICA that focuses on understanding the inherent tensions between insider motivations and organizational controls. Our careful review distinguishes two categories of personal motives for ICA: (1) *instrumental* (i.e., financial benefits) (2) and *expressive* (i.e., psychological contract violations) motives. Our novel theory of ICA also includes the influence of two classes of controls for ICA: (1) *intrinsic* (i.e., self-control) and (2) *extrinsic* (i.e., organizational deterrence) controls. We developed and empirically examined a research model based on our middle-range theory that explains a substantial portion of the variance in ICA (R^2 = 0.462). Specifically, our results indicate that both instrumental and expressive motives were positively related to ICA. Moreover, intrinsic self-control exerted significant direct and moderating influences in our research model, whereas extrinsic organizational deterrence failed to exhibit a direct effect on ICA and significantly moderated instrumental motives' relationship with ICA only. Not only do our results show that self-control exerted a stronger effect on the model than deterrence did ($f^2_{\text{self-control}}$ = 0.195; $f^2_{\text{org.det.}}$ = 0.048) but they also help us identify the limits of deterrence in ICA research.

Keywords: Security; organizational security; information security; insider computer abuse (ICA); self-control theory; deterrence theory (DT); instrumental motives; expressive motives

1. Introduction

Organizations expend considerable resources to shield their sensitive information and associated systems from security threats from both external and internal sources (D'Arcy and Hovav 2007; Lowry et al. 2017a). Internally, organizations are susceptible to acts committed by *organizational insiders* (i.e., individuals with legitimate access to information within the organization, including employees, contractors, board members, and suppliers). (Posey et al. 2013), who are responsible for 25%–50% of all reported security breaches (Ponemon 2018; PWC 2015). Such incidents can be costlier and more damaging than those caused by outsiders,[1] with recent reports identifying privilege abuse as the most common insider tactic.[2]

Recent security events exemplify the seriousness of the risks posed by insiders committing insider computer abuse (ICA). For example, nation-state hackers recently sought to compromise Tesla's network by offering an employee a large sum of money to install malware on the corporate network.[3] Moreover, a former GE employee recently pleaded guilty to illicitly downloading thousands of files containing trade secrets to launch a competing company.[4]

It is critical to note that we are not interested in mere employee carelessness or lack of policy compliance; our focus is on harmful insider behavior relating to organizational information assets that is unauthorized and deliberate (Straub 1990). Moreover, this behavior involves different motives and factors than employee errors and other forms of incidental noncompliance. Drawing on Straub's early work (e.g., Straub 1990), the literature identifies such behavior as ICA (Posey et al. 2011; Willison and Lowry 2018; Willison et al. 2018a; Willison et al. 2018b). Given the importance of preventing ICA, researchers have long endeavored to better understand it by conducting theoretical and empirical studies (e.g., D'Arcy et al. 2009; Lee et al. 2004; Lowry et al. 2015; Lowry et al. 2013b; Straub 1990; Straub and Nance 1990) (Harrington 1996; Willison et al. 2018a; Willison et al. 2018b). Many researchers have employed research models based, at least in part, on *deterrence theory* (DT) (e.g., Nagin 1998) as a means to thwart ICA

[1] https://insights.sei.cmu.edu/insider-threat/2018/01/2017-us-state-of-cybercrime-highlights.html
[2] https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf
[3] https://www.wired.com/story/tesla-ransomware-insider-hack-attempt/
[4] https://www.fbi.gov/news/stories/two-guilty-in-theft-of-trade-secrets-from-ge-072920

(D'Arcy and Herath 2011; Willison et al. 2018a).

Despite their relatively widespread acceptance, a critical shortcoming of traditional deterrence-based studies is their singular focus on sanction perceptions. DT largely ignores other important motives and controls that may also influence individuals' ICA (D'Arcy and Herath 2011; Hu et al. 2011). As noted by Gottfredson (2011, p. 132):

> Deterrence theory makes very little room for individual differences in responsiveness to sanctions, preferring instead to focus on aspects of sanctions that make them more or less effective.

Hence, security researchers are increasingly advocating for a broader consideration of insiders' motives to engage in ICA, because traditional deterrence fails to address these crucial motivational precursors (Crossler et al. 2013; Willison et al. 2018a; Willison and Warkentin 2013; Willison et al. 2018b). In response, we propose a middle-range theory to explain how ICA occurs and how it can be thwarted. To accomplish this goal, we begin our study with a thorough literature review to better understand extant ICA research. Our analyses highlight the need for an expanded view of ICA that addresses the natural tensions between insider motives and organizational controls. Drawing on criminological theory, we assert that these tensions pose two classic questions about ICA (Hirschi 2017): (1) *Why do some insiders commit ICA?* and (2) *Why do some insiders choose not to commit ICA?*.

The first mechanisms in our ICA theory involve two distinct classes of motives: instrumental and expressive motives, which were proposed by Willison and Warkentin (2013) for addressing ICA but have yet to be used in empirical research on ICA. Consequently, the balanced consideration of these two factors is foundational to our theorizing. First, when ICA is committed as a means to achieve another objective, it is said to be fueled by *instrumental motive*s (Willison and Warkentin 2013).[5] By contrast, e*xpressive* motives are described as fueling ICA aimed at expressing individuals' emotions such that the ICA is performed for its own purposes as an end in itself (Willison and Warkentin 2013).[6] Thus, the key in

[5] An example of an *instrumental motive* is when someone steals property or information to sell it for cash (Ambrose et al. 2002). Notably, instrumental motives can lead to various forms of ICA. For example, insiders acting out of instrumental motives might abuse their IT privileges for the chance to receive financial benefits, such as greater bonuses or higher commissions.

[6] An example of an *expressive motive* is when someone steals property or information to destroy it to express dissatisfaction with something in the

distinguishing between instrumental and expressive motives lies in understanding the motivation behind the behavior, not the resulting ICA behaviors themselves.

Beyond the instrumental and expressive motives for committing ICA, the second mechanisms in our theory are intrinsic and extrinsic controls, which inhibit ICA motivations. As noted earlier, organizational deterrence is a form of extrinsic control that relies on individuals' perceptions of the certainty, severity, and celerity (i.e., speed) of extrinsic sanctions to counteract any perceived benefits of engaging in undesirable behavior (Nagin 1998; Yu 1994). Despite the clear contributions of research using the organizational deterrence foundation, intrinsic controls comprise an important complementary area of investigation for organizational security research (Crossler et al. 2013; Lowry et al. 2017a). A particularly promising intrinsic control for consideration is *self-control* (Hu et al. 2015; Hu et al. 2011; Li et al. 2018), which has been defined as "the ability to forgo immediate or near-term pleasures that have some negative consequences" or simply "the ability to act in favor of longer-term interests" (Gottfredson 2017, p. 3). Importantly, extant research indicates that differences in self-control help explain insiders' reactions to stimuli and their subsequent decision-making processes regarding ICA (Hu et al. 2015; Hu et al. 2011; Li et al. 2018).

Given the compelling need to improve our understanding of the causes of ICA if we are to better thwart this behavior, we propose the *motive-control theory of ICA* (MoCo theory). MoCo theory addresses key shortcomings in deterrence theory by not only acknowledging a broader set of motives and controls than considered in DT, but also the complex interplay among these different motives and controls. In short, MoCo theory offers a better, more complete, explanation of the key tensions that insiders experience when faced with the possibility of committing ICA than provided by prior theoretical frameworks. This middle-range theory distinguishes between the influences of expressive and instrumental motives on ICA and explains how intrinsic (i.e., self-control) and extrinsic (i.e., organizational deterrence) controls moderate these relationships. As an initial test of the hypotheses inherent in MoCo theory and the utility of this new

workplace (Ambrose et al. 2002). Again, expressive motives can result in various harmful behaviors, such as intentionally bending or breaking computer-related rules or policies. These can include but are not limited to revenge against a coworker, getting back at a boss for a mediocre performance evaluation, and so forth.

theory, we used an online field study of 532 full-time professionals and found that both instrumental (i.e., financial benefits) and expressive (i.e., psychological contract violations; PCVs) motives drive ICA. Also, intrinsic control (i.e., self-control) exhibited both direct and moderating effects in our model, whereas the extrinsic control of organizational deterrence failed to exert a direct relationship with ICA and significantly moderated the relationship between our instrumental motive and ICA only. These findings support the view that research in our field needs to go beyond deterrence foundations when examining ICA and demonstrates that MoCo theory represents an important advancement for both research and practice.

2. Proposal of a Middle-Range Theory of Insider Computer Abuse

Employees can exhibit many undesirable behaviors in the workplace. For example, previous organizational research identifies problematic behaviors such as sabotage (Wang et al. 2011), antisocial behavior (Robinson and O'Leary-Kelly 1998), counterproductive work behavior (Dalal 2005), organizational misbehavior (Vardi 2001), and organizational deviance (Bennett and Robinson 2000). In security research, phenomena such as cyberloafing (Khansa et al. 2017), phishing victimization (Jensen et al. 2017), system misuse intentions (D'Arcy et al. 2009), unethical IT use (Chatterjee et al. 2015), and cyber harassment (Lowry et al. 2017b; Lowry et al. 2016b) have been investigated.

To better understand security-related phenomena, researchers have, for example, drawn on *compliance theory* (Chen et al. 2012), *rational choice theory* (RCT) (D'Arcy and Lowry 2019; Willison and Lowry 2018), *protection motivation theory* (PMT) (Boss et al. 2015; Burns et al. 2017; Johnston et al. 2015; Menard et al. 2018; Posey et al. 2015), *fairness theory* (Lowry et al. 2015), *self-control theory* (Hu et al. 2015), and *DT* (D'Arcy et al. 2014; D'Arcy et al. 2009; Straub 1990). However, not all undesirable workplace behaviors have the same causes and explanations, especially those related to security (e.g., Boss et al. 2015; D'Arcy et al. 2009; Willison and Lowry 2018). We focus on unauthorized and deliberate ICA[7]

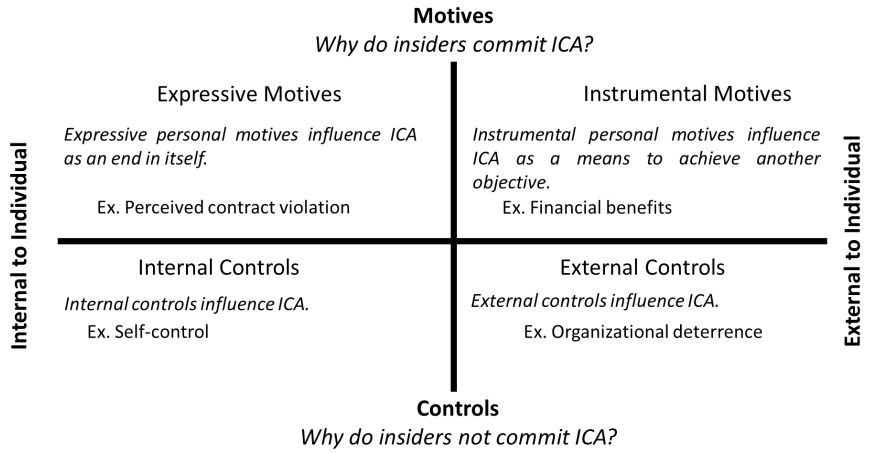
[7] Other researchers have further constrained insiders' computer abuse to also be malicious or harmful (Willison and Lowry 2018; Willison and Warkentin 2013). However, *malice* is defined as a "desire to cause pain, injury, or distress to another" (Merriam-Webster n.d.), which implies motive. Because we were interested in examining motives separately, we removed this constraint from our definition of ICA. Further, harm represents a consequence of behavior that is often unknown at the time of action. Likewise, the same ICA can inflict varying levels of harm depending on the circumstances. Thus, we adapted our formal definition of ICA from Staub's (1990) original definition of deliberate and unauthorized ICA.

because it is potentially the most destructive form of insider behavior, and as its motivations differ from unintentional or innocuous behaviors, it requires theorizing beyond mere compliance or deterrence (Lowry et al. 2017a; Willison et al. 2018a; Willison and Warkentin 2013).

Attempts to use organizational deterrence and its sanctions to thwart ICA are particularly challenging and have resulted in conflicting explanations and outcomes, thus repeatedly leading to conclusions that deterrence alone is insufficient or even detrimental (D'Arcy and Herath 2011; Hu et al. 2011; Lowry et al. 2015; Willison et al. 2018a; Willison and Warkentin 2013). Crucially, security researchers have overlooked what criminologists have long concluded: that deterrence is a form of control (Meier and Johnson 1977) and ICA decisions are influenced by *subjective assessments* (Willison et al. 2018a). Thus, other forms of control and personal motivations should also be considered (Willison et al. 2018a; Willison and Warkentin 2013). Despite explicit calls for this more expansive view (Willison et al. 2018a; Willison and Warkentin 2013), relatively little ICA research has incorporated insiders' personal motivations (e.g., instrumental and expressive motives) and intrinsic controls (e.g., self-control) with extrinsic controls (i.e., organizational sanctions) to gain a more encompassing understanding of ICA in actual organizational contexts. Even less attention has been given to the extent to which these motives and controls might outperform the more traditional extrinsic concepts of disincentives in decreasing ICA. Figure 1 exhibits our proposed framework of ICA motives and controls along with prototypical examples of key constructs.

Our framework reflects the philosophy that researchers must move beyond merely applying theories from reference disciplines to explain the tensions and contingencies involved in ICA. These theories often lack the unique contextual considerations to effectively address the well-known ICA problem. We contend that this research gap requires theories that leverage Merton's (1968) theory of the middle range. Such middle-range theorization has shown great promise in IS research (Hassan and Lowry 2015; Hassan et al. 2019; Park et al. 2017; Tiwana 2009, 2015). This paradigm also aligns with the growing IS research movement to embrace contextualization and focus on enhanced theoretical and practical contributions (Avgerou 2001; Breward et al. 2017; Davison and Martinsons 2016; Hong et al. 2014). Thus, these middle-range theories should not be confused with broader grand theories (e.g., Leidner and Tona 2021) or the

Figure 1. Framework of ICA Motives and Controls

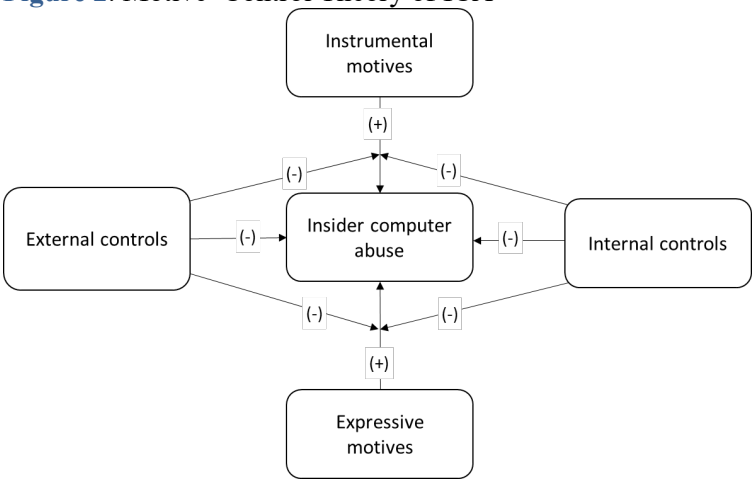


mid-range theories criticized by Grover and Lyytinen (2015). Essentially, rather than trying to develop a theory that is highly generalizable to various behaviors in many contexts (e.g., TPB, DT, RCT, PMT), we focus on one context (i.e., organizational security concerns) and one behavior set (i.e., ICA) and tighten the boundary conditions and assumptions surrounding them. This approach allows a clear research discourse through which we can look deeply at specific situational contingencies that give rise to ICA in organizations, allowing for a deeper theoretical understanding of our phenomena. IS and security researchers are increasingly advocating this kind of highly contextualized theorizing because this approach is crucial for bridging theory with actual meaningful recommendations that can improve practice.

Thus, our aim is not simply theoretical, but also pragmatic. Following Gregor (2006) we are interested in building theory as "statements of relationships among constructs that can be tested" (p. 613). Our novel theory of ICA provides a model that will translate directly to practice and improve organizational information security. Like all middle-range theories, we are bound by the limits of the "range" of the theory—that is, "the conceptual and contextual assumptions under which the model was developed" (Rivard 2021, p. 317). For example, our theory is developed within the organizational context and assumes that organizational insiders have access and opportunity for ICA. However, given the ubiquity of today's organizational IS, most insiders fall within the boundary of our research. Importantly, 8% of all data breaches stem from such insider attacks, and they are among the costliest for organizations, an average of

$4.61 Million per incident.[8] Although ICA is a broad-range topic within organizational IS security, we are not proposing a "grand theory" for understanding all forms of computer abuse. In the following sections, we describe MoCo theory of ICA and link the conceptual elements of the theory to the specific hypotheses in our proposed research model. Figure 2 exhibits the causal logic implied in our framework of ICA motives and controls. Our empirical research then operationalizes and tests these basic elements of the theory.

Figure 2. Motive–Control Theory of ICA



2.1. Instrumental and Expressive Motivations Facilitate Insider Computer Abuse

There are reasons why insiders may want to commit ICA despite their organizations not wanting them to do so. Theoretically, these reasons are categorized as instrumental and expressive motivations that facilitate or encourage ICA. In our context, we explain instrumental motivations in terms of career-related financial benefits and expressive motivations in terms of PCVs.

Briefly, the original conceptualizations of instrumental and expressive behavioral motives can be traced to Parson and Bales' (1955) use of the terms to explain different parenting behaviors. However, scholars today use the distinction between instrumental and expressive motives to gain insight into the origins of various behaviors, including supervisors' fair treatment of subordinates (Qin et al. 2018), citizens' support of political candidates (Brennan and Hamlin 1998), gang activities on social media (Storrod and Densley 2017), and criminal acts (Feshbach 1964). Notably, instrumental and expressive motives have been

[8] Per the IBM Cost of a Data Breach Report 2021.

highlighted as a fruitful area of research to better understand ICA behaviors (Willison and Warkentin 2013).

2.1.1. Financial Benefits as a Primary Instrumental Motivation for Insider Computer Abuse

Instrumental motives can be thought of as extrinsic motives because they drive behavior that serves as a means to some extrinsic end or outcome (Leonard et al. 1999). People who display certain behavior for instrumental reasons do so because they are interested in that behavior's future outcomes; that is, the behavior has value only because it is thought to be instrumental in obtaining some future benefit. For illustration, people may vote in an election because they are interested in the election's consequences (Brennan and Hamlin 1998), commit arson to "hide evidence at a crime scene" (Wachi et al. 2007, p. 30), or treat a subordinate fairly because the subordinate will work harder and exhibit more prosocial behavior, ultimately benefitting the supervisor (Qin et al. 2018).

Perhaps the most prototypical example of an instrumental motive is attaining a financial benefit (Barbuto 2005). Individuals who are motivated by financial benefits will choose to act in ways that they believe will result in monetary gain that can be useful for achieving some other goal (e.g., paying bills, supporting their family, or attaining higher social status). This expectation-driven motivation is similar to that predicted by other theoretical frameworks (e.g., Vroom 1964). Related to an expectancy-driven motivation, the perception of monetary benefits can also increase the valence (i.e., preference) of goal-driven outcomes (Locke 1981).

However, instrumental motives can be potentially harmful when insiders perceive opportunities to gain financial benefits in ways that are at odds with organizational interests (Ambrose et al. 2002; Robinson and Bennett 1997). Examples of this in the realm of ICA range widely from illegal behavior, such as an employee stealing credit card numbers or intellectual property to sell to a third party (Willison and Warkentin 2013) or stealing personal information for the purposes of identity theft, to intentional organizational policy violations aimed at increasing sales or attaining a higher bonus. As noted, the opportunities for financial benefits from ICA in contemporary organizations are numerous. Thus,

> **H1.** Insiders' perceptions of financial benefits of committing ICA (an *instrumental motive*) are positively related to their ICA.

2.1.2. PCV as a Primary Expressive Motivation for Internal Computer Abuse

In contrast to instrumental motives, *expressive motives* drive behavior that is an end in and of itself rather than behavior that is a means to the objective. The benefit is *intrinsic* to the behavior itself, or the behavior is the direct expression of the individual's goal (Youngs et al. 2016). For example, a citizen may vote in an election or support a political candidate because that behavior fulfills a civic responsibility or because it is an opportunity for self-expression (Brennan and Hamlin 1998). Another example would be when a supervisor treats his/her subordinates fairly because that behavior communicates the supervisor's values, such as cooperation and benevolence (Qin et al. 2018). However, in situations where people feel they have been harmed, they are often motivated to exhibit aggressive or harmful behaviors that serve to "vent, release, or express one's feelings of outrage, anger, or frustration" (Robinson and Bennett 1997, p. 16). Thus, the behavior is an emotionally driven retaliation against the party "who has caused harm to the actor" (Ambrose et al. 2002, p. 952).

A prototypical example of a negative expressive motivator is a PCV. A *psychological contract* is "made up of the employees' beliefs about the reciprocal obligations between them and their organization" (Morrison and Robinson 1997, p. 226). Thus, a PCV occurs when employees perceive that their organization has failed to uphold its explicit and/or implicit obligations to them (Morrison and Robinson 1997; Pavlou and Gefen 2005; Zhao et al. 2007). This type of violation is an emotional experience that involves "feelings of betrayal and deeper psychological distress [whereby] … the victim experiences anger, resentment, a sense of injustice and wrongful harm" (Rousseau 1989, p. 129).

PCVs have been linked to negative employee perceptions and behaviors, such as reduced trust toward employers, lower job satisfaction, reduced organizational commitment, and lower levels of citizenship behaviors (Morrison and Robinson 1997; Restubog et al. 2006; Zhao et al. 2007). Not surprisingly, as PCVs elicits anger and even outrage (Morrison and Robinson 1997), it has been identified as an expressive motive for counterproductive workplace behaviors (Bordia et al. 2008) as well as interpersonal and organizational deviance (Chiu and Peng 2008). Thus, through its relationship with organizational deviance, PCV threatens "the well-being of an organization, its members, or both" (Robinson and Bennett 1995, p. 556). This is

because employees who feel "let down" by their organization may express their dissatisfaction via behavior that works against the organization's interests. For example, in the IS literature, PCV has been linked to resistance to the implementation of organizational systems (Lin et al. 2018).

As an example, related directly to ICA, a disgruntled systems administrator was convicted of sending malicious code to his employer that led to over $1 million in damage and a three-year sentence in federal prison.[9] According to the U.S. Department of Justice, the perpetrator was terminated shortly before he severely damaged the system by abusing his remote access to the plant where he had worked for many years. This is a clear example of an expressive motive because the individual had virtually nothing to gain by committing ICA. In fact, the potential repercussions for the employee were more significant than the damage inflicted on the system. Yet this incident exemplifies the type of damage insiders can inflict on systems through ICA when they feel the company has violated its psychological contract.

Likewise, in extant IS research, PCVs have been linked not only to feelings of violation but also to user resistance and deviance (Lin et al. 2018), and the similar phenomenon of perceptions of unfair treatment have been shown to relate to ICA (Lowry et al. 2015; Posey et al. 2011). Conversely, employee perceptions of their organizations' contract fulfillment have been linked to individuals' information security policy compliance (Han et al. 2017). As PCVs tend to evoke negative emotions, PCV will likely be positively related to ICA because the behavior is an expression of insiders' discontent and anger. Thus,

H2. Insiders' perceptions of PCV (an *expressive motive*) are positively related to their ICA.

2.2. Extrinsic and Intrinsic Controls Inhibit Insiders from Committing ICA

We have shown how instrumental and expressive motivations can lead insiders to commit ICA, but it is also vital to consider the countervailing tensions that push against such considerations. Namely, theorization that includes multiple mechanisms for why individuals commit ICA alongside factors that inhibit such activity is required for a more encompassing view of this important organizational phenomenon. As such, our middle-range theory of ICA also includes both intrinsic (i.e., self-control) and extrinsic organizational

[9] https://www.justice.gov/usao-mdla/pr/former-systems-administrator-sentenced-prison-hacking-industrial-facility-computer

controls (i.e., deterrence via sanctions).

2.2.1. Self-Control as a Primary Intrinsic Control that Inhibits Insider Computer Abuse

Apart from instrumental and expressive motives, researchers have noted various factors that can guide security-relevant behavior (Gottfredson 2017; Gottfredson and Hirschi 1990; Nagin and Paternoster 1993). These factors include stress and moral disengagement (D'Arcy et al. 2014), threat and coping appraisals (Johnston et al. 2016), and neutralization techniques (Siponen and Vance 2010). Security education, training, and awareness (SETA) programs have also been linked directly or indirectly to these important employee actions (D'Arcy et al. 2009).

Interestingly, although criminologists have identified individual differences like self-control as a key construct in explaining individuals' criminal behaviors and other non-criminal problematic behaviors (Gottfredson 2017; Gottfredson and Hirschi 1990), relatively little research has investigated the influence of insiders' self-control on their willingness to engage in undesirable behaviors like ICA (Hu et al. 2015; Li et al. 2018). In fact, our review of information security publications in the senior AIS scholars' basket that mention self-control or deterrence theory (see Appendix A) identified only a few studies that actually measured individuals' self-control (i.e., Hu et al. 2015; Li et al. 2021; Lowry et al. 2017b; Lowry et al. 2019; Luo et al. 2020; Moody et al. 2018). Given the potential influence of self-control as a key individual difference in IS security research and lack of due attention, we explain its foundations and integrate it into MoCo theory. In doing so, we expand on prior research to elevate self-control as a central construct that has a direct influence on ICA as well as a powerful diminishing effect on both instrumental and expressive motives for ICA.

Self-control theory is a criminological theory that posits that people with low self-control are more likely than those with high self-control to commit a crime when presented with the opportunity (Gottfredson and Hirschi 1990). Self-control theory has been used to explain various criminal behaviors, such as fraud (Holtfreter et al. 2008), dating violence (Schreck et al. 2008), theft (Schreck 1999), and cyber harassment (Lowry et al. 2019; Turanovic and Pratt 2014). The causal mechanism involved in self-control in predicting problematic behavior is *self-regulation*, or the ability to control one's emotions and behaviors in seeking

immediate gratification (Gottfredson and Hirschi 1990; Murray and Kochanska 2002).

Self-control theory explains that people with low self-control are more emotionally driven and have more difficulty regulating their impulses toward gratification than those with high self-control. *Low self-control* is an absence of the capacity to self-regulate, thereby fostering deviant attitudes, beliefs, and intentions that lead to actual deviant behavior (Murray and Kochanska 2002). Seeking immediate gratification can take several deviant forms, "whether the gratification consists of pure hedonism, revenge, or the wielding of power" (Bossler and Holt 2010, p. 228). Nonetheless, this combination of low self-control and seeking immediate gratification are crucial in the decision to commit a crime (Tibbetts and Gibson 2002), in violating widely held norms of conduct (Hu et al. 2011), and in repeatedly performing deviant acts (Turanovic and Pratt 2014). Conversely, individuals with higher self-control can better control their emotions and inclinations toward self-gratification and are more rational and less reactionary, making them less inclined to commit ICA.

Moreover, research shows that as a key individual characteristic, self-control exists on a continuum within individuals (Tangney et al. 2004). Lower self-control relates to greater impulsivity (Jones and Lynam 2009; Nagin and Pogarsky 2001), criminality, and deviance (Gottfredson and Hirschi 1990), and higher self-control relates to increased behavioral deliberation (Hu et al. 2015). For example, compared with their counterparts with higher self-control, individuals with lower self-control often react quickly because they give less consideration to their behaviors before acting to derive near-term benefits at the expense of longer-term payoffs (Hu et al. 2015). This shorter decision-making time horizon makes individuals more susceptible to perceived immediate benefits that can harm them or their organizations in the longer term (Hu et al. 2011).

Time is thus a key consideration with self-control. The need for self-control can be explained through the principle of time discounting, whereby individuals perceive greater value in more immediately available *benefits* compared with future longer-term *consequences* of behavior (Ariely and Wertenbroch 2002). Lower self-control reflects a tendency to act with a "here and now" (i.e., immediate) mindset, while higher self-control is oriented more toward longer-term goals (Nagin and Pogarsky 2001). Thus, lower self-control

leads individuals to react quickly with limited thought given to a decision's full implications (Hu et al. 2015), again pointing to issues with self-regulation around immediate gratification. Hence,

H3. Insiders' self-control is negatively related to ICA.

A key aspect of middle-range theories is they often consider contingency effects to explain what is happening in a particular context (Hassan and Lowry 2015; Hassan et al. 2019; Park et al. 2017; Tiwana 2009, 2015). This improved explanatory power is due to the possible inclusion of associations that extend beyond simple linear relationships to more fully explain interesting phenomena, such as ICA (Willison et al. 2018a; Willison and Warkentin 2013). A natural contingency that must be considered for theoretical completeness is the attenuating effect of self-control on the relationship between motives and ICA.

Self-control often influences how individuals calculate the benefits of potential behaviors but may not necessarily motivate individuals to exhibit any specific set of behaviors (Gottfredson 2017). For example, higher self-control enables an insider facing a personal affront in the workplace to better resist the urge to retaliate, whereas lower self-control exacerbates the urge (Lian et al. 2014). Individuals with higher self-control who experience vengeful cognition engage in less subsequent organizational deviance than their counterparts with lower self-control (Bordia et al. 2008). Additionally, research shows that self-control moderates the relationship between perceived benefits of personal internet use in the workplace and employees' compliance with internet use policies at work (Li et al. 2018). Therefore, to better understand how ICA occurs in organizations, it is imperative to examine how self-control influences the relationships between individual motives and behaviors in addition to possible direct relationships between self-control and the behaviors of interest. Thus,

H4a. Insiders' self-control attenuates the relationship between financial benefits and ICA.

H4b. Insiders' self-control attenuates the relationship between PCV and ICA.

2.2.2. Deterrence Perceptions as a Primary Extrinsic Control Inhibiting Insider Computer Abuse

Whereas self-control can be seen as a primary intrinsic control that inhibits ICA, we turn to DT and its tenets to build our primary extrinsic control that inhibits ICA, thereby completing MoCo theory. DT, which originated in the criminology literature, explains that individuals weigh the expected benefits from their

behaviors against potential consequences of them (Bentham 1988; Gottfredson and Hirschi 1990; Gottfredson 2011). From this foundation, organizations (or societies) need only to foster expectations of negative consequences (i.e., sanctions) that outweigh potential benefits to deter individuals' undesirable behaviors. Traditional deterrence relies on perceptions of the certainty, severity, and celerity of sanctions to counteract any perceived benefits from engaging in undesirable behavior (Nagin 1998; Yu 1994). Based on utilitarianism (Bentham 1988), the goal of these deterrents (via sanctions) is to make undesirable behavior an irrational choice.

In criminology, the influence of deterrents (e.g., sanctions) is said to be twofold: (1) They can "prevent the person being punished from committing another crime" and (2) they can "prevent others who are contemplating crime from committing the act" (Piquero et al. 2011, p. 336). These two deterrent effects are called *specific deterrence* and *general deterrence*, respectively (Piquero et al. 2011). Whether general or specific, to be successful, a deterrent requires that an action's perceived costs (i.e., the deterrent) outweigh its perceived benefits. However, benefits and costs ultimately are not uniformly perceived: "Rewards and costs can come from ourselves, from those around us (friends, parents, teachers, employers, etc.), or from the act itself" (Andrews and Bonta 2010, p 187).

Since early seminal research on effective security (Straub 1990; Straub and Nance 1990), DT has become one of the most influential theories in the organizational security literature (D'Arcy and Herath 2011). Appendix A identifies more than 60 articles that explicitly mention both "deterrence theory" and "information security" in the AIS senior scholars' basket of eight IS journals (e.g., Chen et al. 2012; D'Arcy et al. 2014; D'Arcy et al. 2009; Guo et al. 2011; Herath and Rao 2009; Johnston et al. 2016; Johnston et al. 2015; Lowry et al. 2015; Moody et al. 2018; Willison et al. 2018a; Willison et al. 2018b). Thus, DT and its concepts are not new to the field, and we briefly mention several notable examples in the extant research.

Several organizational security studies have leveraged DT's components to explain various security phenomena. For example, Chen et al. (2012) examined the role of organizational punishment severity and certainty on employees' compliance intentions. In the healthcare context, Foth (2016) examined the effects of punishment severity and detection certainty on healthcare workers' intention to comply with data

protection regulations. D'Arcy et al. (2014) included the role of perceived sanctions in their study on individuals' violation intentions. Similarly, Johnston et al. (2015) and Siponen and Vance (2010) examined the roles of formal and informal sanctions in information security compliance intentions. Interestingly, Sojer et al. (2014) found that punishment severity indirectly influenced software developers' intention to reuse internet accessible code. Given the strong theoretical and empirical support for sanctions as a primary component of organizational deterrence efforts, we extend this work to our ICA context. Thus,

H5. Insiders' perceptions of organizational sanctions are positively related to their perceptions of organizational deterrence.

H6. Insiders' perceptions of organizational deterrence are negatively related to their ICA.

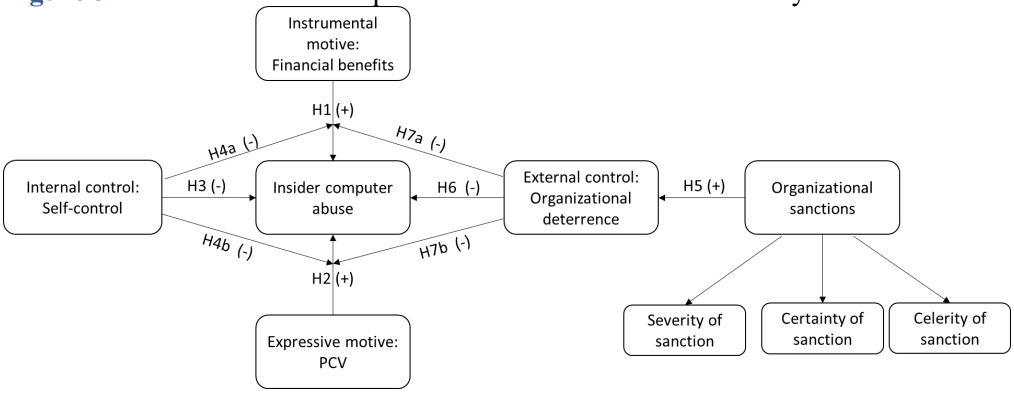
Like the contingency effects proposed for our intrinsic control mechanism, deterrence perceptions also likely attenuate the extent to which instrumental and expressive motivations foster ICA. Specifically, the presence of deterrents, primarily through sanctions, should reduce the attractiveness of deviant actions to individuals. Although instrumental and expressive motives can drive engagement in ICA, insiders' perceptions of organizational deterrence will limit the influence of their motives on their behavior owing to the greater chance that they will face sanctions if caught. This form of behavioral control has been illustrated in previous research that found sanctions moderate the relationship between organizational injustice and intentions to commit ICA (Willison et al. 2018b). Thus,

H7a. Insiders' perceptions of organizational deterrence attenuate the relationship between perceived financial benefits and ICA.

H7b. Insiders' perceptions of organizational deterrence attenuate the relationship between PCV and ICA.

Summarizing this section, Figure 3 depicts our research model used to test MoCo theory.

Figure 3. Research Model to Operationalize and Test MoCo Theory



3. Methodology

To test our hypotheses, we hired a marketing research firm to collect anonymized data from insiders working in various industries in the US. Collecting such data online is a widely accepted practice in organizational security research (e.g., Lowry et al. 2013a; Lowry et al. 2016b; Posey et al. 2013; Vance et al. 2013), especially as long as key actions are taken to increase data quality (Lowry et al. 2016a; Lowry et al. 2016b). Our actions to increase data quality included (1) hiring marketing professionals who pre-screened and qualified our participants as legitimate full-time employees with knowledge of deterrence efforts and ICA at their firms and (2) introducing attention traps and removing data that exhibited anomalies and/or hurried responses. According to the survey provider, 696 individuals initially received our survey and 532 agreed to provide responses. After excluding incomplete responses and screening for non-conscientious responses (e.g., straight-ticket responding), our final sample comprised 361 respondents. This figure equates to a usable-to-collected response rate of 67.9%, which meets or exceeds the rate of other similar research (e.g., D'Arcy et al. 2014).

When conducted with careful controls, online panels are especially appropriate for collecting sensitive information from insiders because they provide anonymous, off-site access to the survey. Increasing anonymity, in turn, yields responses that are more candid and less susceptible to method bias (Podsakoff et al. 2003). The average age of surveyed insiders was 45.4 years, with an average organizational tenure of10.8 years. Additionally, the sample was 49.0% female, with 66.5% of respondents holding at least a bachelor's degree. Finally, 35.2% of respondents indicated that they have a managerial role in their organization, and13.6% reported working in their organization's IT department. Our sample includes insiders working in a variety of job roles across numerous industries including education, finance and insurance, healthcare, professional services, governmental, and retail, among others. Appendix D provides the full industry breakdown of our sample, and Table 1 summarizes our sample characteristics.

3.1. Study Measures

As is standard practice, we leveraged previously developed measures whenever possible to operationalize the constructs in our research model. To assess individual differences associated with self-control, we

Table 1. Sample Characteristics

Characteristic	Statistic
Female	49.0%
Age	45.4 (average)
Organizational tenure	10.8 (average)
Education level	66.5% (at least a bachelor's degree)
Managerial role	35.2%
IT role	13.6%
Organizational size	
Very Large (10,000+ computers)	23.0%
Large (1,000–10,000 computers)	24.4%
Medium (100–1,000 computers)	25.5%
Small (1–100 computers)	27.1%

measured trait-like self-control using four items from Tangney et al. (2004). An example of an item measuring self-control is "I often act without thinking through all the alternatives" (reverse-worded item). We measured PCV using six items from Robinson and Morrison (2000), such as "My employer has broken many of its promises to me even though I have upheld my side of the deal." We measured insiders' perceptions of financial benefits through ICA with three items adapted from Posey et al. (2015), such as "I could be rewarded financially for choosing to abuse my organization's computer systems."

Insiders' perceptions of organizational sanctions were measured with 10 items reflecting the certainty, severity, and celerity of organizational sanctions for ICA inspired by previous research (D'Arcy and Herath 2011; D'Arcy et al. 2009; Guo et al. 2011; Siponen and Vance 2010). Based on the treatment of these sanction-related perceptions in prior studies (e.g., Bulgurcu et al. 2010; D'Arcy and Herath 2011; Guo et al. 2011; Johnston et al. 2016; Siponen and Vance 2010; Xu et al. 2016), we considered organizational sanctions a higher-order factor comprising certainty, severity, and celerity. For example, Siponen and Vance (2010) and Guo et al. (2011) measured sanctions as a reflective construct comprising perceptions of both sanction certainty and severity. As DT primarily discusses these perceptions separately, we chose to maintain these distinct but related sub-constructs as part of a higher-order factor rather than collapse them into a single reflective construct. As methodologists (i.e., Hair et al. 2017) have explained, higher-order specifications such as these are appropriate when a common factor explains correlations among the lower-order factors.

Items used to measure the deterrence constructs were based on prior studies on organizational

deterrence (D'Arcy and Herath 2011; D'Arcy et al. 2009; Siponen and Vance 2010). An example of an item on certainty of sanction is "My organization will discipline those whom it believes are guilty of information security violations on its computer system." An item measuring celerity of sanction is "My organization would immediately punish employees who commit information security violations on the computer system," and an item measuring severity of sanction is "It is likely that the punishment given by my organization to employees who commit information security violations on the computer system would be severe." We measured individuals' perceptions of organizational deterrence from ICA with three items based on D'Arcy and Herath (2011), such as "My organization deters its employees from committing information security violations." Finally, we used 12 items from Posey et al. (2011) to measure ICA, such as "I have purposely abused our organization's computer systems." The full set of items is included in Appendix B.

4. Analysis and Results

The research model was analyzed in a two-step procedure as recommended by methodologists (Gerbing and Anderson 1988). We used the partial least squares structural equation modeling (PLS-SEM) platform SmartPLS 3.2.8 (Ringle et al. 2015). PLS is appropriate for studies that examine complex relationships (Fornell and Bookstein 1982) that are exploratory or models in development that are not yet fully established in the literature (Henseler et al. 2014; Lowry and Gaskin 2014), thereby placing a premium on predictive validity (Hair et al. 2017).

4.1. Construct Validity

In the first step, we examined the construct validity of the measures to be included in the structural model. First, we assessed the presence of collinearity by examining the predictor constructs' variance inflation factors (VIFs) in the model. As the VIF values ranged from 0.289 to 1.974, none were above the conservative 3.3 level (Petter et al. 2007). Second, each construct's composite reliabilities were within the recommendations of prior research (Nunnally 1978). Additionally, each average extracted variance (AVE) was well above the recommended 0.50 level. Third, each pair of constructs met the Fornell-Larcker criterion, as indicated by a ratio of the square root of AVE to correlations (Fornell and Larcker 1981).

Fourth, the heterotrait–monotrait ratio between all constructs, except for the subdimensions of the higher-order sanctions construct, was below the recommended 0.90 value, averaging between 0.16 and 0.35 for each construct (Henseler et al. 2015). Finally, the standardized root mean square residual (SRMR) and root mean square residual covariance (RMS_{theta}) fit statistics indicated that the model has good fit (SRMR = 0.061; RMS_{theta} = 0.119) (Henseler et al. 2014; Hu and Bentler 1999). Table 2 shows the measurement model statistics. The full correlation table is in Appendix C.

Table 2. Measurement Model Statistics

Latent Constructs	ICA	PCV	FR	SC	OD	OS	CR	HTMT
Insider computer abuse (ICA)	**0.91**						0.98	0.24
Psychological contract violation (PCV)	0.37	**0.91**					0.96	0.18
Financial benefits (FB)	0.40	0.24	**0.93**				0.95	0.16
Self-control (SC)	−0.41	−0.35	−0.19	**0.72**			0.87	0.20
Organizational deterrence (OD)	−0.26	−0.28	−0.15	0.17	**0.84**		0.91	0.35
Organizational sanctions (OS)	−0.15	−0.15	−0.07	0.10	0.79	**0.86**	0.97	0.33

Square root of AVEs is in bold; CR: Composite Reliability; HTMT: Avg. Heterotrait–Monotrait ratio

For the higher-order organizational sanctions construct, we assessed the hierarchical component model as recommended by leading methodologists (Hair et al. 2017; Wetzels et al. 2009). Hair et al. (2017) specified two requirements of hierarchical component models: (1) the number of indicators should be similar across lower-order constructs and (2) the reflective measurement model criteria (e.g., AVEs, composite reliability) should be met at each level of the model—with the important exception that discriminant validity between the higher- and lower-order constructs, as well as between the lower-order constructs in reflective hierarchical component models, need not be established (Hair et al. 2017).

We met the first criterion with three to four indicators among the three sub-constructs. The AVEs of lower-order components were above the 0.50 threshold and composite reliabilities were above the 0.70 cutoff point (Hair et al. 2017), indicating strong internal (convergent) reliability and validity. The cross-loadings' pattern supports the higher-order factor with the highest items' loadings on the associated lower-order construct and relatively lower cross-loadings on each other lower-order construct (average factor loading = 0.910; average cross loading = 0.764). Table 3 depicts the cross-loadings.

We note that our decision to model sanctions as a higher-order reflective construct is supported by prior research. For example, because of their positive interrelationships, many previous studies collapsed

Table 3. Organizational Sanction Statistics

Item/Label	Celerity	Certainty	Severity
AVE	0.735	0.873	0.880
CR	0.917	0.954	0.956
Celerity1	**0.856**	0.634	0.689
Celerity2	**0.871**	0.800	0.801
Celerity3	**0.815**	0.575	0.595
Celerity4	**0.885**	0.740	0.745
Certainty1	0.729	**0.915**	0.834
Certainty2	0.767	**0.943**	0.851
Certainty3	0.771	**0.944**	0.864
Severity1	0.726	0.793	**0.917**
Severity2	0.794	0.853	**0.950**
Severity3	0.814	0.909	**0.947**

AVE: Average Variance Extracted; CR: Composite Reliability

deterrence dimensions into a single construct (e.g., Bulgurcu et al. 2010; Guo et al. 2011; Johnston et al. 2016; Siponen and Vance 2010; Xu et al. 2016). Specifically, Guo et al. (2011) measured perceived sanctions as a single reflective measure with separate items for severity, celerity, and certainty loading onto the same construct (loadings ranged from 0.77 to 0.93). Additionally, previous researchers found relatively high correlations and cross-loadings among deterrence-related constructs when including them separately in a research model. For instance, Siponen and Vance (2010) found that formal and informal sanctions were highly correlated ($r = 0.76$) and shared cross-loadings with a range of 0.61–0.75.

4.2. Structural Model

We assessed the hypothesized relationships in the research model via SmartPLS 3.0 with 5,000 bootstrapped subsamples. To establish robustness, we included several controls in the assessment: age, gender, organizational tenure, and whether the insider had an IT/IS or a managerial position. Since some insiders might consider engaging in some forms of ICA a moral issue (D'Arcy et al. 2009; Myyry et al. 2009), we included a control for moral identity (Aquino and Reed 2002). As noted, moral identity can be regarded as a "self-regulatory mechanism that motivates moral action" (Aquino and Reed 2002, p. 1423). Finally, ICA actively works against the organization's interests, thereby contradicting any SETA initiatives the organization employs. We also included a control for SETA awareness (D'Arcy et al. 2009). Both Table 4 and Figure 4 display the results of our structural assessment.

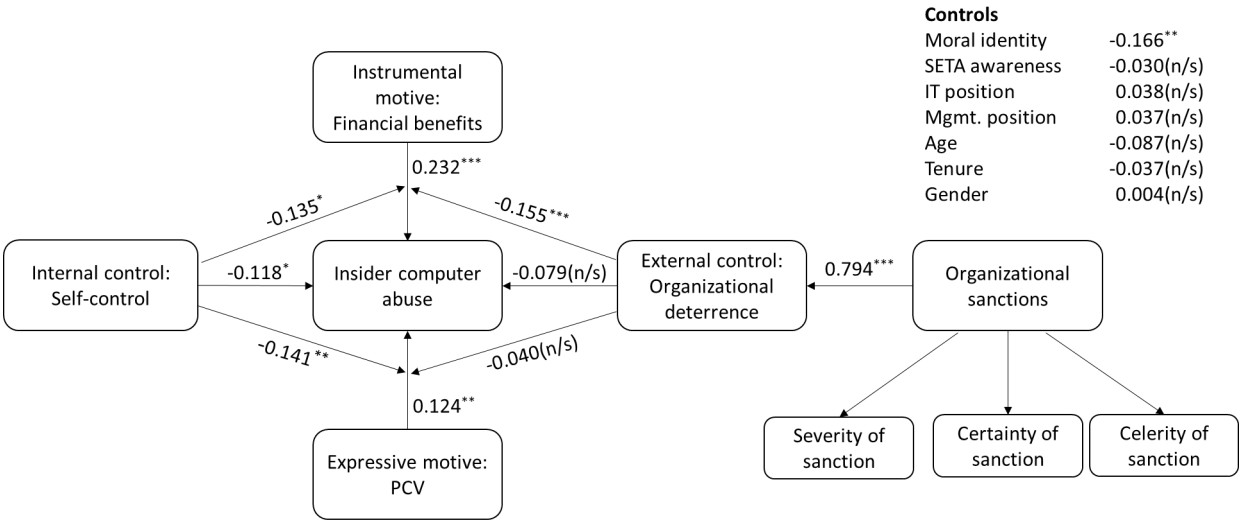
Our second-order perceived sanctions construct explained 62.7% of the variance in deterrence

Table 4. Structural Model Testing Results

Relationship	β (sig.)	*t*-stat.	Bias-corrected CI[t]
H1. Financial benefits → ICA	0.232***	4.972	[0.143, 0.329]
H2. PCV → ICA	0.124**	2.642	[0.028, 0.211]
H3. Self-control → ICA	−0.118*	2.450	[−0.193, −0.013]
H4a. Self-control X Financial benefits → ICA	−0.135*	2.485	[−0.251, −0.029]
H4b. Self-control X PCV → ICA	−0.141**	2.702	[−0.244, −0.053]
H5. Organizational sanctions → Organizational. Deterrence	0.794***	31.780	[0.735, 0.834]
H6. Organizational deterrence → ICA	−0.079(n/s)	1.778	[−0.177, 0.005]
H7a. Organizational deterrence X Financial benefits → ICA	−0.155***	3.626	[−0.235, −0.070]
H7b. Organizational deterrence X PCV → ICA	−0.040(n/s)	1.011	[−0.110, 0.038]
Controls	**B**	***t*-stat.**	**Bias-corrected CI**
Moral identity	−0.166**	3.105	[−0.269, −0.060]
SETA awareness	−0.030(n/s)	0.483	[−0.106, 0.083]
IT position	0.038(n/s)	0.916	[−0.042, 0.113]
Management position	0.037(n/s)	0.875	[−0.047, 0.113]
Age	−0.087(n/s)	1.740	[−0.175, 0.015]
Tenure	−0.037(n/s)	0.985	[−0.115, 0.036]
Gender	−0.004(n/s)	0.123	[−0.085, 0.074]

*p = 0.05; **p = 0.01; ***p = 0.001; n/s = not significant; [t]bias-corrected confidence intervals: 2.5%–97.5%; interaction terms standardized prior to calculation[10]; calculated using 5,000 subsamples

Figure 4. Visual Depiction of Structural Model Results



*p = 0.05; **p = 0.01; ***p = 0.001; n/s = not significant; interaction terms standardized prior to calculation; Calculated using 5,000 subsamples

perceptions. The model also explained 46.2% of insiders' self-reported ICA. All hypotheses except for H6 and H7b were supported. The relationship between our instrumental motive (i.e., financial benefits) and

[10] As recommended by methodologists (Hair et al. 2017; Henseler and Chin 2010), we used the two-stage approach to develop the interaction terms. Appendix E provides additional discussion and support for the moderation analyses.

ICA was attenuated by our extrinsic inhibiting control (i.e., organizational deterrence) ($\beta = -0.155$***), but the relationship between our expressive motive (i.e., PCV) and ICA was not ($\beta = -0.040$). However, our intrinsic inhibiting control of self-control was found to moderate, significantly and negatively, the relationship between both instrumental ($\beta = -0.135$*) and expressive ($\beta = -0.141$**) motives and ICA.

In addition to the model's hypothesized relationships, we examined the effect sizes of our two inhibiting controls. Thus, we re-ran the model twice: once with self-control, PCV, and financial benefits (excluding organizational deterrence) and once with organizational deterrence, PCV, and financial benefits (excluding self-control). Then we compared the results to the full model. Next, we calculated the two models' effect size (f^2), such that $f^2 = (R^2_{included} - R^2_{excluded})/(1-R^2_{included})$ (Hair et al. 2017). The effect of adding intrinsic self-control to the model was 0.195, a medium-size effect, while the effect of adding extrinsic deterrence to the model was 0.048, a small effect. Owing to the small effect size of deterrence, we also examined our analyses' statistical power to ensure ample power to detect organizational deterrence's influence in a model including self-control. Our analysis supports our ability to detect a significant influence from organizational deterrence, should one exist (i.e., $f^2 = 0.048$; $\alpha = 0.05$; power = 0.948) (Cohen 1988; Soper 2019).

We also examined organizational sanctions' influence on insiders' perceptions of organizational deterrence. Again, DT postulates that perceptions of organizational sanctions drive perceptions of deterrence. Our results indicate that sanctions as a higher-order construct accounted for a significant portion of insiders' perceptions of organizational deterrence, explaining 62.7% of its variance. However, organizational deterrence was not significantly related to ICA when self-control was included in the model, and deterrence exhibited a smaller effect than self-control in the model ($f^2_{self\text{-}control} = 0.195$; $f^2_{org.det.} = 0.048$).

Finally, we included various controls, both demographic (i.e., gender, age, organizational tenure, and position) and substantive (i.e., SETA perceptions and moral identity). Of these controls, only moral identity was significantly related to ICA. As noted, moral identity is a mechanism of self-regulation (Aquino and Reed 2002). Thus, it is not surprising that moral identity was negatively related to ICA. However, moral identity and self-control are far from interchangeable and shared only 9% of their variance ($r = 0.30$).

4.3. Post-hoc Analyses of Interaction Effects

To examine the hypothesized interaction effects, we plotted the simple slopes in Figures 5–8. As shown in Figures 5 and 6, insiders with relatively high self-control exhibited lower levels of ICA than their counterparts with low self-control when perceptions of financial benefits and contract violations were relatively high. There was little difference in ICA levels between individuals with low and high self-control when financial benefits and PCV were relatively low. Insiders who perceived relatively high organizational deterrence also exhibited lower levels of ICA when perceptions of financial benefits were relatively high compared with those who perceived lower organizational deterrence (see Figure 7). However, as indicated by the nonsignificant interaction effect, differences in perceptions of organizational deterrence did not appear to influence the overall positive relationship between PCV and ICA (see Figure 8).

Figure 5. Interaction of Self-Control and Financial Benefits on ICA

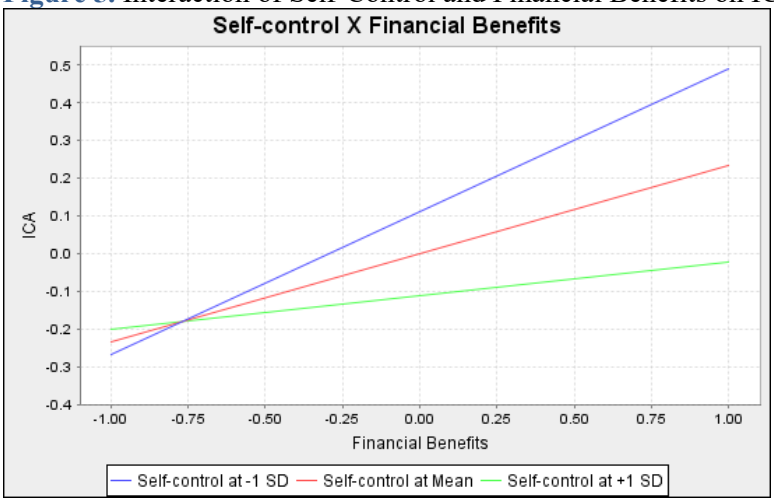


Figure 6. Interaction of Self-Control and Psychological Contract Violation on ICA

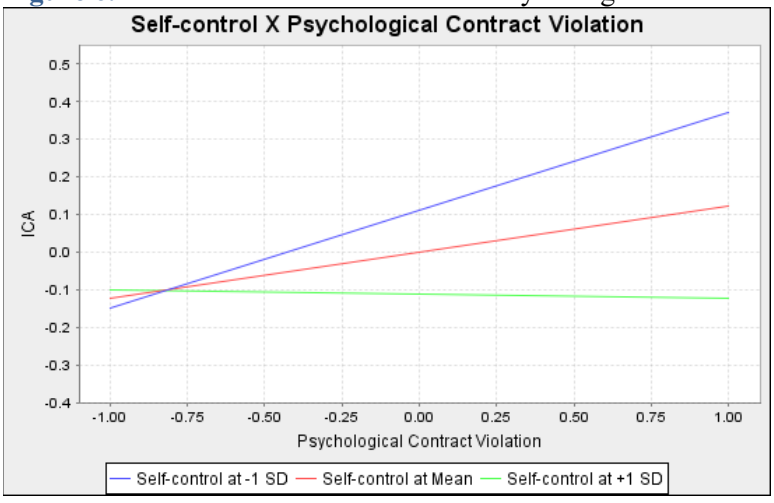


Figure 7. Interaction of Organizational Deterrence and Financial Benefits on ICA

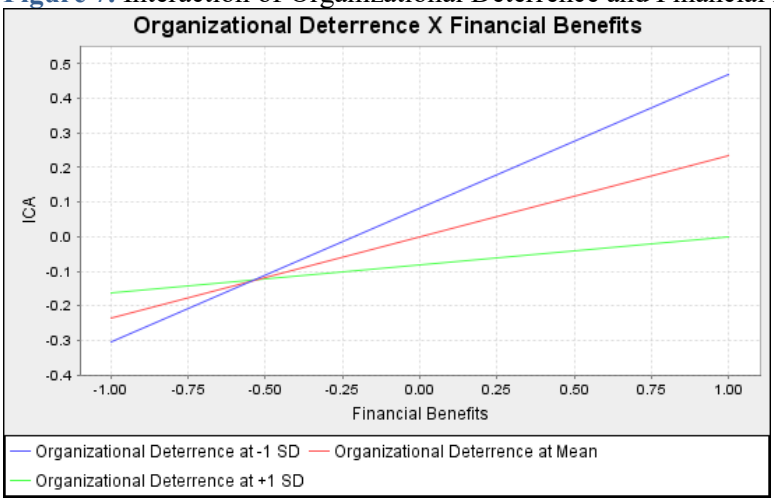
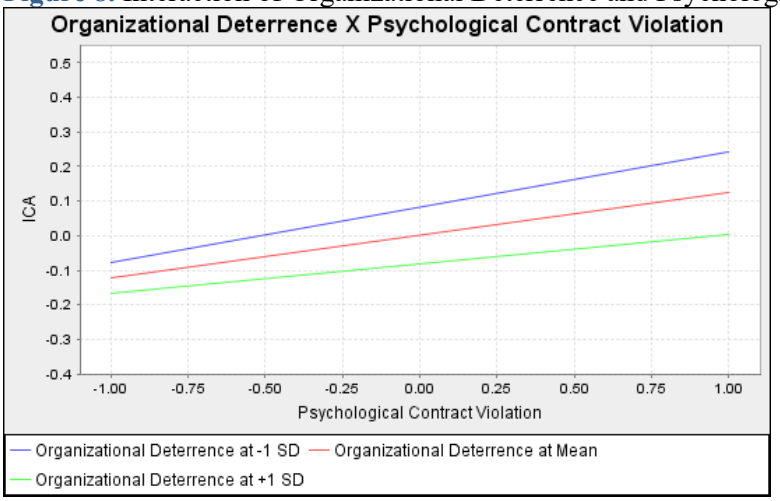


Figure 8. Interaction of Organizational Deterrence and Psychological Contract Violation on ICA



4.4. Common Method Variance

To ensure that our data did not suffer from harmful common method variance (CMV), we performed two analyses recommended by Schwarz et al. (2017): an unmeasured latent variable (UMLV) analysis (Liang et al. 2007) and a measured latent marker variable (MLMV) analysis (Chin et al. 2013). According to our UMLV assessment, the AVE by our substantive items was 77.8% and the AVE by the method's unmeasured latent variable (i.e., method-based variance) was only 0.4%. Additionally, our MLMV assessment found little evidence of harmful CMV, with an average difference, in terms of beta weights, between the baseline CMV model and the MLMV model of 0.004. Therefore, our sample did not suffer from harmful CMV (Podsakoff et al. 2003; Schwarz et al. 2017). The full results from both CMV analyses are included in Appendix F.

5. Discussion and Contributions

As our MoCo theory proposes and our results confirm, tensions exist between insiders' motives and controls to commit ICA. This finding helps answer calls to challenge the extant organizational security focus in DT (e.g., Crossler et al. 2013; Lowry et al. 2017a; Willison et al. 2018a; Willison and Warkentin 2013; Willison et al. 2018b) via more expansive approaches to information security theorizing (Dey et al. 2021; Moody et al. 2018). Interestingly, despite much of the discipline's theoretical and rhetorical framing around DT (e.g., D'Arcy et al. 2009; Johnston and Warkentin 2010; Johnston et al. 2015; Straub 1990), we find that, compared to intrinsic controls, organizational deterrence serves a much more limited role in thwarting ICA. Specifically, we find that organizational deterrence attenuated only one set of motives—instrumental motives.

This discovery represents a significant departure from the traditional view of IS security in DT-based research, which overlooks motivations. For example, D'Arcy et al. (2009) conducted a DT-based study of employees' misuse of organizational IS resources that did not consider any motivations to perform the behavior itself—only external controls aimed at deterring it (i.e., organizational security-related sanctions, policies, programs, and monitoring). Siponen and Vance (2010) included DT-based sanctions in their study of security policy violations, but rather than study insiders' motives they investigated the role of neutralization (e.g., rationalization) strategies on the deterring effect of sanctions. Moody et al. (2018) found that organizational deterrents (i.e., punishments) did not explain policy violations and subsequently removed them from their proposed *unified model of information security policy compliance* (UMISPC). However, they did not examine the moderating effects of such punishments on instrumental motives. Finally, Dey et al. (2021) developed a microeconomic model to examine organizational policy circumvention. They focused on two classes of deterrents that they describe as "countermeasures" and "anti-circumvention measures." Thus, like many other DT-focused studies, their research looks at external controls only, not internal controls or employees' triggering motives.

By contrast, our research includes two major forms of employee motives and demonstrates that internal controls show broader applicability to ICA with direct and moderating effects. Namely, insiders' self-

control reduced ICA in three ways: it negatively influenced ICA directly and it weakened the influence of both instrumental and expressive motives. Thus, our initial test of MoCo theory suggests that self-control was the single most important factor for inhibiting ICA. In addition, effect size calculations indicate that the ability of extrinsic controls (i.e., organizational deterrence) to curb negative insider behavior ($f^2 = 0.048$) is overshadowed by employees' self-regulatory abilities (i.e., self-control) ($f^2 = 0.195$). However, we do not wish to imply that organizational deterrence does not serve a role in thwarting ICA. Although deterrence did not significantly attenuate the relationship between expressive motives and ICA, it did diminish the relationship between instrumental motives and ICA. It is thus likely that employees who view ICA as a means to attain some other goal (e.g., financial gain) can be dissuaded to some degree through sanctions that drive deterrence perceptions. Unfortunately, deterrence appears to do little to halt ICA if an insider's actions represent the end goal (e.g., to vent frustration).

We believe this finding reflects a fundamental difference between instrumental and expressive motives. Instrumental motives, which relate to extrinsic tangible outcomes (Barbuto 2005), are externally focused and influenced by extrinsic controls (e.g., organizational deterrence). Alternatively, expressive motives are intrinsic in nature and reflect a desire to express oneself (Robinson and Bennett 1997). Therefore, extrinsic inhibiting controls, such as organizational deterrence, are unlikely to be effective at limiting the effects of expressive motivators, like PCV on ICA. This insight is crucial for organizational leaders as they seek to minimize ICA, and it indicates that insiders' instrumental and expressive intentions are derived from distinct motives and must be managed differently. As criminologists have opined (e.g., Gottfredson 2017; Gottfredson and Hirschi 1990) and has been theorized by ICA scholars (Willison and Lowry 2018; Willison et al. 2018a), one possibility is that although the general idea of sanctions and overall deterrence is rational, many decisions are governed by bounded rationality, and pure rationality alone rarely explains why people act. Thus, it is rare for research to fully explain how to prevent negative behaviors like ICA through rational sanctions. This especially seems to be the case when considering ICA behavior with expressive motives.

5.1. Implications

Our MoCo theory of ICA provides unique and refreshing insight into a phenomenon that was introduced to

our discipline more than three decades ago. This insight is possible because our theory pits two major types of motives that positively relate to ICA against two major types of controls that serve to attenuate the influence of those motives. Although recent researchers have called for broader, more comprehensive approaches (e.g., Dey et al. 2021), we are not aware of research that examines ICA in this way. Consequently, our theory complements existing research and has major implications for future IS security research.

The first major implication of our study is that IS security researchers should simultaneously account for the distinctions and interdependencies among insiders' motives and controls, as explained by MoCo theory, rather than studying these factors independently. Our results indicate that controls must be calibrated against the motives being managed for the controls to be efficacious. Without considering these factors together, researchers will miss the true theoretical linkages among motives and controls—and ultimately behaviors. Thus, a major contribution of our study is that it demonstrates that controls attenuate the influence of motives. Put another way, our research indicates that while controls can influence behavior directly, they also function as regulation mechanisms for motives. However, when studied in isolation, such controls may appear to serve a motivational rather than a regulatory role.

To further underscore this matter, we found that self-control negatively influences ICA directly and simultaneously moderates the influence of instrumental (e.g., financial benefits) and expressive (e.g., PCV) motives for ICA. Conversely, deterrence only diminishes the influence of perceived financial benefits on ICA. Thus, in the context of ICA, organizational deterrents (e.g., sanctions) themselves do not create new motives for ICA, but rather they weaken some already existing motives (e.g., financial benefits). As a counter example, when an insider is not motivated to commit ICA, the insider likely does not consider the threat of sanction for actions they have no intention to commit. We believe this helps explain why prior researchers found very weak evidence for the influence of deterrents on positive behaviors (e.g., compliance intentions) (D'Arcy and Herath 2011). When an insider has compelling motives to comply with policy, the existence of a sanction for not complying likely has a limited influence on their compliance intention. This may appear to be a subtle distinction, but it has powerful implications for researchers and practitioners and

may help explain the disparate findings of prior DT research (cf. D'Arcy and Herath 2011).

The second major implication of our research derives from its contribution as a middle-range, theoretical framework for organizational and behavioral ICA research. Recently, Moody et al. (2018) and Dey et al. (2021) explain the need for more expansive theories in IS security. As Moody et al. (2018) note, "many of competing theories in IS [security] are often tested in isolation rather than in comparison with each other" (p. 286). We largely agree with these sentiments but add that middle range theories, such as MoCo theory, are often better viewed as complementary rather than competitive. To this end, and to illustrate the breadth and depth of our implications, we next explain the implications of MoCo theory in comparison to these other recent works (i.e., Dey et al. 2021; Moody et al. 2018).

The implications of our MoCo theory are distinct, yet complement those of Moody et al. (2018) in several important ways. For instance, we provide a middle-range theory for ICA, while their study explains policy compliance by way of two distinct dependent variables: (1) intention to share a computer password and (2) reactance, which they define as "denying the possible [IS security] problem" (Moody et al. 2018, p. 305). Thus, our theory has novel implications for deliberate ICA that their study does not address, especially because these phenomena are only tangentially related. For example, to the extent that they studied positive motivations to violate policy (i.e., share a password), they studied it in the form of *habit* and *role values.* Upon inspection, these are wholly unrelated to ICA. Habit reflects the fact that compliance is something an insider "does without thinking," and role values indicate that the compliant or noncompliant behavior is "compatible with his/her work" (Moody et al. 2018, p. A3-A4). The motives in the UMISPC are incompatible with ICA, which is deliberate, nonhabitual behavior. Also, as abusive behavior, ICA works against an organization's interests and is incompatible with formal work roles. Moody et al. (2018) studied only the direct effect of deterrence (i.e., punishments) on intentions. When they found no significant direct relationship, they subsequently dropped deterrence from the UMISPC. As our results show, despite a nonsignificant direct relationship, deterrence may moderate insiders' instrumental motives for security-related behaviors. This clarification further exemplifies the complementary nature of our works.

Our also work uniquely complements Dey et al.'s (2021) recent findings that shed light on an important

security-related tensions—those of organizational security *education* and *enforcement*. However, the tension between education and enforcement is distinct from the tension between motives and controls. In fact, one of the contextual factors at play in the study by Dey et al. (2021) is organizational budgetary constraints, as they note:

> Our work also sheds light on an organization's planning and budgeting for IT security. As discussed earlier, most organizations operate within a fixed budget allocated to anticircumvention measures. A major shortcoming of a fixed budget is that investing more in one countermeasure can come only at the expense of cutting the other, which introduces an artificial substitutability where none exists (Dey et al. 2021, p. 14).

Thus, one of the contributions of their microeconomic model is to help organizations with budget allocation across organizational countermeasures (or controls). In contrast, the MoCo theory of ICA sheds light on a distinct set of tensions: *instrumental* and *expressive motives* versus *internal* and *external controls*. Rather than being focused on states of circumvention across an organization, we are focused on the *behavior of individuals,* making these two works complementary. The microeconomic model of Dey et al. (2021) says nothing about any individual's circumvention behavior, but rather generalizes to the level of circumvention prevalence across a firm (described as "states"). Conversely, our work does not describe or explain the state of ICA across a firm (i.e., a firm-level conceptual perspective), but rather explains ICA decisions of individual insiders.

Finally, the third major implication of our research is practitioners can now call upon a much broader array of human resource management (HRM) practices to reduce ICA than indicated in prior research. Drawing on the rich history of research on the foundations of PCV, our study suggests HRM practices that foster interpersonal relationships between supervisors and subordinates, increase congruency in perceived employer-employee obligations and values, and reduce sensitivity to perceived psychological contract breaches should effectively reduce PCVs, thereby reducing occurrences of ICA (Morrison and Robinson 1997). For example, using realistic job previews, providing more truthful and accurate pre-hire information (e.g., accurate recruiting videos and recruiter information sharing), and ensuring greater levels of interaction between the candidate and organization agents should result in a greater degree of congruence between candidate and employer schemata of the employment relationship (i.e., obligations, promises) (Morrison

and Robinson 1997; Robinson and Morrison 2000). Greater congruence between schemata decreases the likelihood of breaches occurring, thereby lessening the possibility of PCV. Further, because the first year of employment is when employees tend to realize that their pre-hire schemata of shared obligations are inaccurate, organizations can utilize intense formalized socialization processes that not only validate company values/beliefs proffered pre-hire but also transfer pre-hire promises to organization agents to operationalize (Robinson and Morrison 2000; Sutton and Griffin 2004).

In addition, it is important to acknowledge psychological contracts can evolve over time. Accordingly, HRM practices can also be used to reduce the likelihood that changes in psychological contracts will lead to perceived contract violations (Morrison and Robinson 1997), thereby reducing the potential for ICA These practices include hiring people with low levels of equity sensitivity and negative affect (Kunze and Gower 2012; Morrison and Robinson 1997), training leaders in procedural/interactional justice (Tekleab et al. 2005), placement for supervisor–subordinate fit (Tekleab et al. 2005), and providing opportunities for participation in decision-making (Rousseau 2004).

More important are the practical implications for using HRM practices to reduce ICA by increasing an organization's stock of self-control capital. A clear takeaway from our research is that self-control is vital in moderating the influence of both instrumental and expressive motives to commit ICA. While organizational leadership cannot always prevent such insider motives from forming across their workforce, it is essential to maintain personnel with adequate self-control to diminish the impact of such harmful motives should they arise. This is especially true for insiders in positions with increased opportunity to commit ICA. As such, perhaps the most obvious way to reduce ICA is to use trait measures of self-control as a screening tool in the selection process. Additionally, insiders' self-control levels can be used to help determine whether an employee is a good fit for a job where there is substantial potential for ICA. In short, companies that wish to reduce the occurrence of ICA have a wide variety of HRM practices at their disposal to solve the problem beyond methods discussed in deterrence-related models.

5.2. Limitations and Future Research

Inherent limitations exist in self-reported security research, although using online panels to collect data is

accepted widely in security research (Boss et al. 2009; Burns et al. 2018; Johnston and Warkentin 2010; Lowry et al. 2016a; Lowry et al. 2016b; Posey et al. 2013). To minimize limitations in self-reporting, this study provided off-site surveys to insiders, thereby increasing their sense of anonymity, encouraging candid responses (Kays et al. 2012), and reducing response bias (Podsakoff et al. 2003). We also performed a formal test for CMV and found little evidence to indicate that harmful CMV biased our results. Although this is an important first step, ICA can take many individual forms, and future research should shed light on potential differences among individual ICA behaviors.

Our results present several other opportunities for future research. First, researchers should examine a broader set of factors that create instrumental and expressive motives to commit ICA. Such future studies will not only uncover new ground for ICA research but further refine our emergent theory. Additionally, future research should examine how such instrumental and expressive motives develop over time. For example, our study indicates that insiders sometimes believe they could benefit financially for abusing their organizations' systems, and this perception can influence their ICA; however, future research is needed to uncover the specific situations or positions that create these opportunistic incentives.

Second, we found that PCV influences ICA directly. As an expressive motivator, perceived contract violations can lead to acts of organizational sabotage, such as ICA. However, further research is needed to examine exactly how these perceptions emerge within insiders causally, particularly for situations in which contract violations lead to ICA. For example, future research can examine whether insiders' positions within the organization play a role in their ICA as a reaction to PCV. This could be a fruitful avenue for future investigations because some positions may provide more opportunities to commit ICA than others. Understanding this causally will likely require the collection of longitudinal data. Further, the potential for the HRM practices to reduce ICA by diminishing PCV suggests a need for research aimed at better understanding expressive motives for ICA to determine how to reduce ICA's occurrence. Such research should also explore contextual boundary conditions (e.g., turbulent versus stable work environment) for when these HRM practices are and are not effective in reducing PCV and ICA.

Third, less than two-thirds of the variance in organizational deterrence was explained by insiders'

perceptions of organizational sanctions. Given DT's prominence in driving organizational security programs and security research, future studies might examine what factors other than the certainty, severity, and celerity of sanctions influence insiders' perceptions of organizational deterrence. However, given the limited influence of deterrence in our research model, future studies based solely on DT are ill-advised, as suggested in extant literature (cf. Willison et al. 2018a; Willison and Warkentin 2013).

Finally, given the direct and moderating influence of self-control on insiders' ICA, further research is needed to better understand the role of self-control in regulating security-related behavior. In the workplace, this is especially important for insiders entrusted with access to valuable organizational information assets because their self-control plays a key role in reducing ICA intentions. Although we used a broad and relatively stable trait measure of self-control in our study, self-control has also been conceptualized as a finite resource that can be depleted by overwork or other demanding situations (Gino et al. 2011; Hagger et al. 2010), and scholars have shown that self-control resources can fluctuate during the workday (Johnson et al. 2018). Future research should thus examine the role other conceptualizations of self-control play in ICA, such as state self-control, self-control effort, and self-control motivation (cf. Wehrt et al. 2020). It is also possible that there are situations in which ICA requires high levels of self-control to commit, such as with sophisticated multistage attacks (e.g., a situation in which an insider must perform detailed reconnaissance and wait patiently to strike at the opportune time). Future research should also examine whether there are specific contextual factors that lead to a positive relationship between self-control and ICA.

6. Conclusion

We extended the deterrence perspective in a new middle-range theory of ICA termed the Motive-Control Theory of ICA, or MoCo theory for short, that emphasizes both instrumental (e.g., financial benefits) and expressive (e.g., PCV) motives for ICA as well as intrinsic and extrinsic inhibiting controls—insiders' self-control and perceptions of organizational deterrence, respectively—on ICA. Our results indicate that motives driven by insiders' perceptions of financial benefits and PCV are strongly related to their ICA. Insiders' self-control significantly moderates the relationship between certain instrumental and expressive

motives. Finally, we found that deterrence moderates the relationship between financial benefits and ICA only, thereby failing to exhibit a significant direct relationship with ICA or a significant moderating relationship on the path between expressive motives and ICA.

Our study thus demonstrates that both instrumental and expressive motivations engender ICA within organizations and that intrinsic inhibiting controls, such as self-control, exhibit significant direct and moderating influences in the model. Conversely, and despite their continued utilization in the field, deterrence perceptions attenuated the influence of outward-focused motives for ICA only, leaving the influence of inward, expressive motives for ICA unaltered. Our study offers a greater theoretical and empirical understanding of the relationship between self-control and instrumental and expressive motivators while providing insights for when deterrence perceptions do and do not help minimize ICA.

References

Ambrose ML, Seabright MA, Schminke M (2002) Sabotage in the workplace: The role of organizational injustice. *Organizational Behavior and Human Decision Processes* 89(1):947-965.

Andrews DA, Bonta J (2010) *The psychology of criminal conduct*, (Matthew Bender & Company, New Providence, NJ).

Aquino K, Reed A, II (2002) The self-importance of moral identity. *Journal of Personality and Social Psychology* 83(6):1423-1440.

Ariely D, Wertenbroch K (2002) Procrastination, deadlines, and performance: Self-control by precommitment. *Psychological Science* 13(3):219-224.

Avgerou C (2001) The significance of context in information systems and organizational change. *Information Systems Journal* 11(1):43-63.

Barbuto JE (2005) Motivation and transactional, charismatic, and transformational leadership: A test of antecedents. *Journal of Leadership & Organizational Studies* 11(4):26-40.

Bennett RJ, Robinson SL (2000) Development of a measure of workplace deviance. *Journal of Applied Psychology* 85(3):349-360.

Bentham J (1988) *An Introduction to the Principles of Morals and Legislation*, (Prometheus Books, New York, NY).

Bordia P, Restubog SLD, Tang RL (2008) When employees strike back: investigating mediating mechanisms between psychological contract breach and workplace deviance. *Journal of Applied Psychology* 93(5):1104-1117.

Boss SR, Galletta DF, Lowry PB, Moody GD, Polak P (2015) What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly* 39(4):837-864.

Boss SR, Kirsch LJ, Angermeier I, Shingler RA, Boss RW (2009) If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. *European Journal of Information Systems* 18(2):151-164.

Bossler AM, Holt TJ (2010) The effect of self-control on victimization in the cyberworld. *Journal of Criminal Justice* 38(3):227-236.

Brennan G, Hamlin A (1998) Expressive voting and electoral equilibrium. *Public Choice* 95(1):149-175.

Breward M, Hassanein K, Head M (2017) Understanding consumers' attitudes toward controversial

information technologies: A contextualization approach. *Information Systems Research* 28(4):760-774.
Bulgurcu B, Cavusoglu H, Benbasat I (2010) Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly* 34(4):523-548.
Burns AJ, Posey C, Roberts TL, Lowry PB (2017) Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. *Computers in Human Behavior* 68(March):190-209.
Burns AJ, Roberts TL, Posey C, Bennett RJ, Courtney JF (2018) Intentions to comply versus intentions to protect: A VIE theory approach to understanding the influence of insiders' awareness of organizational SETA efforts. *Decision Sciences* 49(6):1187-1228.
Chatterjee S, Sarker S, Valacich JS (2015) The behavioral roots of information systems security: Exploring key factors related to unethical IT use. *Journal of Management Information Systems* 31(4):49-87.
Chen Y, Ramamurthy K, Wen K-W (2012) Organizations' information security policy compliance: Stick or carrot approach? *Journal of Management Information Systems* 29(3):157-188.
Chin WW, Thatcher JB, Wright RT, Steel D (2013) Controlling for common method variance in PLS analysis: the measured latent marker variable approach. H Abdi, WW Chin, E Vinzi, R V., T G., L, eds. *New Perspectives in Partial Least Squares and Related Methods* (Springer) 231-239.
Chiu S-F, Peng J-C (2008) The relationship between psychological contract breach and employee deviance: The moderating role of hostile attributional style. *Journal of Vocational Behavior* 73(3):426-433.
Cohen J (1988) *Statistical Power Analysis for the Behavioral Sciences (2nd Edition)*, (Lawrence Erlbaum Associates, Hillsdale, NJ).
Crossler RE, Johnston AC, Lowry PB, Hu Q, Warkentin M, Baskerville R (2013) Future directions for behavioral information security research. *Computers & Security* 32(February):90-101.
D'Arcy J, Herath T (2011) A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *European Journal of Information Systems* 20(6):643-658.
D'Arcy J, Herath T, Shoss M (2014) Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of Management Information Systems* 31(2):285-318.
D'Arcy J, Hovav A (2007) Deterring internal information systems misuse. *Communications of the ACM* 50(10):113-117.
D'Arcy J, Hovav A, Galletta D (2009) User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research* 20(1):79-98.
D'Arcy J, Lowry PB (2019) Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal* 29(1):43-69.
Dalal RS (2005) A meta-analysis of the relationship between organizational citizenship behavior and counterproductive work behavior. *Journal of Applied Psychology* 90(6):1241-1255.
Davison RM, Martinsons MG (2016) Context is king! Considering particularism in research design and reporting. *Journal of Information Technology* 31(3):241-249.
Dey D, Ghoshal A, Lahiri A (2021) Circumventing circumvention: An economic analysis of the role of education and enforcement. *Management Science* 0(0): doi: 10.1287/mnsc.2021.4027.
Feshbach S (1964) The function of aggression and the regulation of aggressive drive. *Psychological Review* 71(4):257-272.
Fornell C, Bookstein FL (1982) Two structural equation models: LISREL and PLS applied to consumer exit-voice theory. *Journal of Marketing Research* 19(4):440-452.
Fornell C, Larcker DF (1981) Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research* 18(1):39-50.
Foth M (2016) Factors influencing the intention to comply with data protection regulations in hospitals: based on gender differences in behaviour and deterrence. *European Journal of Information Systems* 25(2):91-109.
Gerbing DW, Anderson JC (1988) An updated paradigm for scale development incorporating unidimensionality and its assessment. *Journal of Marketing Research* 25(2):186-192.
Gino F, Schweitzer ME, Mead NL, Ariely D (2011) Unable to resist temptation: How self-control depletion promotes unethical behavior. *Organizational Behavior and Human Decision Processes* 115(2):191-

203.
Gottfredson M (2017) Self-Control Theory and Crime. *Oxford Research Encyclopedia of Criminology*.
Gottfredson M, Hirschi T (1990) *A General Theory of Crime*, (Stanford University Press, Stanford, California).
Gottfredson MR (2011) Sanctions, situations, and agency in control theories of crime. *European Journal of Criminology* 8(2):128-143.
Gregor S (2006) The nature of theory in information systems. *MIS Quarterly* 30(3):611-642.
Grover V, Lyytinen K (2015) New state of play in information systems research: The push to the edges. *MIS Quarterly* 39(2):271-296.
Guo KH, Yuan Y, Archer NP, Connelly CE (2011) Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems* 28(2):203-236.
Hagger MS, Wood C, Stiff C, Chatzisarantis NLD (2010) Ego depletion and the strength model of self-control: A meta-analysis. *Psychological Bulletin* 136(4):495-525.
Hair JF, Hult GTM, Ringle CM, Sarstedt M (2017) *A Primer on Partial Least Squares Structural Equations Modeling (PLS-SEM), 2nd Edition*, (Sage, Thousand Oaks, CA).
Han J, Kim YJ, Kim H (2017) An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective. *Computers & Security* 66(May):52-65.
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.
Hassan NR, Lowry PB (2015) Seeking middle-range theories in information systems research. *International Conference on Information Systems (ICIS 2015)* (AIS, Fort Worth, TX), December 13–18.
Hassan NR, Mathiassen L, Lowry PB (2019) The process of information systems theorizing as a discursive practice. *Journal of Information Technology* 34(3):198-220.
Henseler J, Chin WW (2010) A Comparison of Approaches for the Analysis of Interaction Effects Between Latent Variables Using Partial Least Squares Path Modeling. *Structural Equation Modeling: A Multidisciplinary Journal* 17(1):82-109.
Henseler J, Dijkstra TK, Sarstedt M, Ringle CM, Diamantopoulos A, Straub DW, Ketchen DJ, Hair JF, Hult GTM, Calantone RJ (2014) Common beliefs and reality about PLS: Comments on Rönkkö and Evermann (2013). *Organizational Research Methods* 17(2):182-209.
Henseler J, Ringle CM, Sarstedt M (2015) A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science* 43(1):115-135.
Herath T, Rao HR (2009) Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems* 18(2):106-125.
Hirschi T (2017) *Causes of Delinquency*, (Routledge, New York, NY).
Holtfreter K, Reisig MD, Pratt TC (2008) Low self-control, routine activities, and fraud victimization. *Criminology* 46(1):189-220.
Hong W, Chan FKY, Thong JYL, Chasalow LC, Dhillon G (2014) A framework and guidelines for context-specific theorizing in information systems research. *Information Systems Research* 25(1):111-136.
Hu L, Bentler PM (1999) Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling: A Multidisciplinary Journal* 6(1):1-55.
Hu Q, West R, Smarandescu L (2015) The role of self-control in information security violations: Insights from a cognitive neuroscience perspective. *Journal of Management Information Systems* 31(4):6-48.
Hu Q, Xu Z, Dinev T, Ling H (2011) Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM* 54(6):54-60.
Jensen ML, Dinger M, Wright RT, Thatcher JB (2017) Training to mitigate phishing attacks using mindfulness techniques. *Journal of Management Information Systems* 34(2):597-626.
Johnson RE, Lin S-H, Lee HW (2018) Self-control as the fuel for effective self-regulation at work: Antecedents, consequences, and boundary conditions of employee self-control. *Advances in motivation science* (Elsevier) 87-128.
Johnston AC, Warkentin M (2010) Fear appeals and information security behaviors: An empirical study.

MIS Quarterly 34(3):549-566.
Johnston AC, Warkentin M, McBride M, Carter L (2016) Dispositional and situational factors: influences on information security policy violations. *European Journal of Information Systems* 25(3):231-251.
Johnston AC, Warkentin M, Siponen M (2015) An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly* 39(1):113-134.
Jones S, Lynam DR (2009) In the eye of the impulsive beholder: The interaction between impulsivity and perceived informal social control on offending. *Criminal Justice and Behavior* 36(3):307-321.
Kays K, Gathercoal K, Buhrow W (2012) Does survey format influence self-disclosure on sensitive question items? *Computers in Human Behavior* 28(1):251-256.
Khansa L, Kuem J, Siponen M, Kim SS (2017) To cyberloaf or not to cyberloaf: The impact of the announcement of formal organizational controls. *Journal of Management Information Systems* 34(1):141-176.
Kunze M, Gower K (2012) The influence of subordinate affect and self-monitoring on multiple dimensions of leader-member exchange. *International Journal of Management and Marketing Research* 5(3):83-100.
Lee SM, Lee SG, Yoo S (2004) An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management* 41(6):707-718.
Leidner D, Tona O (2021) The CARE Theory of Dignity Amid Personal Data Digitalization. *MIS Quarterly* 45(1b):343-370.
Leonard NH, Beauvais LL, Scholl RW (1999) Work motivation: The incorporation of self-concept-based processes. *Human Relations* 52(8):969-998.
Li H, Luo X, Zhang J, Sarathy R (2018) Self-control, organizational context, and rational choice in Internet abuses at work. *Information & Management* 55(3):358-367.
Li H, Luo XR, Chen Y (2021) Understanding information security policy violation from a situational action perspective. *Journal of the Association for Information Systems* 22(3):5.
Lian H, Brown DJ, Ferris DL, Liang LH, Keeping LM, Morrison R (2014) Abusive supervision and retaliation: A self-control framework. *Academy of Management Journal* 57(1):116-139.
Liang H, Saraf N, Hu Q, Xue Y (2007) Assimilation of enterprise systems: The effect of institutional pressures and the mediating role of top management. *MIS Quarterly* 31(1):59-87.
Lin T-C, Huang S-L, Chiang S-C (2018) User resistance to the implementation of information systems: A psychological contract breach perspective. *Journal of the Association for Information Systems* 19(4):306-332.
Locke EA (1981) Goal setting and task performance: 1969-1980. *Psychological Bulletin* 90(1):125-152.
Lowry P, Moody G, Galletta D, Vance A (2013a) The drivers in the use of online whistle-blowing reporting systems. *Journal of Management Information Systems* 30(1):153-189.
Lowry PB, D'Arcy J, Hammer B, Moody GD (2016a) "Cargo Cult" science in traditional organization and information systems survey research: A case for using nontraditional methods of data collection, including Mechanical Turk and online panels. *Journal of Strategic Information Systems* 25(3):232-240.
Lowry PB, Dinev T, Willison R (2017a) Why security and privacy research lies at the centre of the information systems (IS) artefact: Proposing a bold research agenda. *European Journal of Information Systems* 26(6):546-563.
Lowry PB, Gaskin J (2014) Partial least squares (PLS) structural equation modeling (SEM) for building and testing behavioral causal theory: When to choose it and how to use it. *IEEE Transactions on Professional Communication* 57(2):123-146.
Lowry PB, Moody GD, Chatterjee S (2017b) Using IT design to prevent cyberbullying. *Journal of Management Information Systems* 34(3):863-901.
Lowry PB, Posey C, Bennett RJ, Roberts TL (2015) Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: An empirical study of the influence of counterfactual reasoning and organisational trust. *Information Systems Journal* 25(3):193-273.
Lowry PB, Posey C, Roberts TL, Bennett RJ (2013b) Is your banker leaking your personal information?

The roles of ethics and individual-level cultural characteristics in predicting organizational computer abuse. *Journal of Business Ethics* 121(3):385-401.
Lowry PB, Zhang J, Moody GD, Chatterjee S, Wang C, Wu T (2019) An integrative theory addressing cyberharassment in the light of technology-based opportunism. *Journal of Management Information Systems* 36(4):1142-1178.
Lowry PB, Zhang J, Wang C, Siponen M (2016b) Why do adults engage in cyberbullying on social media? An integration of online disinhibition and deindividuation effects with the social structure and social learning model. *Information Systems Research* 27(4):962-986.
Luo XR, Li H, Hu Q, Xu H (2020) Why individual employees commit malicious computer abuse: A routine activity theory perspective. *Journal of the Association for Information Systems* 21(6):1552-1593.
Meier RF, Johnson WT (1977) Deterrence as Social Control: The Legal and Extralegal Production of Conformity. *American Sociological Review* 42(2):292-304.
Menard P, Warkentin M, Lowry PB (2018) The impact of collectivism and psychological ownership on protection motivation: A cross-cultural examination. *Computers & Security* 75(June):147-166.
Merriam-Webster (n.d.) Malice. (https://www.merriam-webster.com/dictionary/malice; accessed March 11, 2021).
Merton RK (1968) *Social Theory and Social Structure*, (Free Press, New York, NY).
Moody GD, Siponen M, Pahnila S (2018) Toward a unified model of information security policy compliance. *MIS Quarterly* 42(1):285-311.
Morrison EW, Robinson SL (1997) When employees feel betrayed: A model of how psychological contract violation develops. *Academy of Management Review* 22(1):226-256.
Murray KT, Kochanska G (2002) Effortful control: Factor structure and relation to externalizing and internalizing behaviors. *Journal of Abnormal Child Psychology* 30(5):503-514.
Myyry L, Siponen M, Pahnila S, Vartiainen T, Vance A (2009) What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems* 18(2):126-139.
Nagin DS (1998) Deterrence and incapacitation. M Tonry, ed. *The Handbook of Crime and Punishment* (Oxford University Press, New York, NY) 345-368.
Nagin DS, Paternoster R (1993) Enduring individual differences and rational choice theories of crime. *Law and Society Review* 27(3):467-496.
Nagin DS, Pogarsky G (2001) Integrating celerity, impulsivity, and extralegal sanction threats into a model of general deterrence: Theory and evidence. *Criminology* 39(4):865-892.
Nunnally J (1978) *Psychometric Theory*, (McGraw-Hill, New York).
Park Y, El Sawy OA, Fiss P (2017) The role of business intelligence and communication technologies in organizational agility: A configurational approach. *Journal of the Association for Information Systems* 18(9):648-686.
Parsons T, Bales RF (1955) *Family, Socialization and Interaction Process*, (Free Press, Glencoe, Il).
Pavlou PA, Gefen D (2005) Psychological contract violation in online marketplaces: Antecedents, consequences, and moderating role. *Information Systems Research* 16(4):372-399.
Petter S, Straub DW, Rai A (2007) Specifying formative constructs in information systems research. *MIS Quarterly* 31(4):623-656.
Piquero AR, Paternoster R, Pogarsky G, Loughran T (2011) Elaborating the individual difference component in deterrence theory. *Annual Review of Law and Social Science* 7(1):335-360.
Podsakoff PM, MacKenzie SB, Lee JY, Podsakoff NP (2003) Common method biases in behavioral research: a critical review of the literature and recommended remedies. *Journal of Applied Psychology* 88(5):879-903.
Ponemon (2018) 2018 Cost of a Data Breach Study: Global Overview. (https://www.ibm.com/security/data-breach; accessed April 18, 2019).
Posey C, Bennett RJ, Roberts TL (2011) Understanding the mindset of the abusive insider: An examination of insiders' causal reasoning following internal security changes. *Computers & Security* 30(6):486-497.
Posey C, Roberts TL, Lowry PB (2015) The impact of organizational commitment on insiders' motivation

to protect organizational information assets. *Journal of Management Information Systems* 32(4):179-214.
Posey C, Roberts TL, Lowry PB, Bennett RJ, Courtney JF (2013) Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. *MIS Quarterly* 37(4):1189-1210.
PWC (2015) Managing cyber risks in an interconnected world: Key findings from The Global State of Information Security. Available at https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf (www.pwc.com/gsiss2015; accessed September 2014).
Qin X, Huang M, Johnson RE, Hu Q, Ju D (2018) The short-lived benefits of abusive supervisory behavior for actors: An investigation of recovery and work engagement. *Academy of Management Journal* 61(5):1951-1975.
Restubog SLD, Bordia P, Tang RL (2006) Effects of psychological contract breach on performance of IT employees: The mediating role of affective commitment. *Journal of Occupational and Organizational Psychology* 79(2):299-306.
Ringle CM, Wende S, Becker J-M (2015) SmartPLS3. Bönningstedt: SmartPLS. Retrieved from http://www.smartpls.com. accessed
Rivard S (2021) Theory building is neither an art nor a science. It is a craft. *Journal of Information Technology* 36(3):316-328.
Robinson SL, Bennett RJ (1995) A typology of deviant workplace behaviors: A multidimensional scaling study. *Academy of Management Journal* 38(2):555-572.
Robinson SL, Bennett RJ (1997) Workplace deviance: Its definition, its manifestations, and its causes. RJ Lewicki, RJ Bies, BH Sheppard, eds. *Research on Negotiations in Organizations (Vol. 6)* (Elsevier, Amsterdam) 3-27.
Robinson SL, Morrison EW (2000) The development of psychological contract breach and violation: a longitudinal study. *Journal of Organizational Behavior* 21(5):525-546.
Robinson SL, O'Leary-Kelly AM (1998) Monkey see, monkey do: The influence of work groups on the antisocial behavior of employees. *Academy of Management Journal* 41(6):658-672.
Rousseau DM (1989) Psychological and implied contracts in organizations. *Employee responsibilities and rights journal* 2(2):121-139.
Rousseau DM (2004) Psychological contracts in the workplace: Understanding the ties that motivate. *Academy of Management Perspectives* 18(1):120-127.
Schreck CJ (1999) Criminal victimization and low self-control: An extension and test of a general theory of crime. *Justice Quarterly* 16(3):633-654.
Schreck CJ, Stewart EA, Osgood DW (2008) A reappraisal of the overlap of violent offenders and victims. *Criminology* 46(4):871-906.
Schwarz A, Rizzuto T, Carraher-Wolverton C, Roldán JL, Barrera-Barrera R (2017) Examining the impact and detection of the urban legend of common method bias. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems* 48(1):93-119.
Siponen M, Vance A (2010) Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly* 34(3):487-502.
Sojer M, Alexy O, Kleinknecht S, Henkel J (2014) Understanding the drivers of unethical programming behavior: The inappropriate reuse of internet-accessible code. *Journal of Management Information Systems* 31(3):287-325.
Soper D (2019) Post-hoc Statistical Power Calculator for Hierarchical Multiple Regression [Software].
Storrod ML, Densley JA (2017) 'Going viral' and 'Going country': the expressive and instrumental activities of street gangs on social media. *Journal of Youth Studies* 20(6):677-696.
Straub DW (1990) Effective IS security. *Information Systems Research* 1(3):255-276.
Straub DW, Nance W (1990) Discovering and disciplining computer abuse in organizations: A field study. *MIS Quarterly* 14(1):45-60.
Sutton G, Griffin MA (2004) Integrating expectations, experiences, and psychological contract violations:

A longitudinal study of new professionals. *Journal of Occupational and Organizational Psychology* 77(4):493-514.
Tangney JP, Baumeister RF, Boone AL (2004) High self-control predicts good adjustment, less pathology, better grades, and interpersonal success. *Journal of Personality* 72(2):271-324.
Tekleab AG, Takeuchi R, Taylor MS (2005) Extending the chain of relationships among organizational justice, social exchange, and employee reactions: The role of contract violations. *Academy of Management journal* 48(1):146-157.
Tibbetts SG, Gibson CL (2002) Individual propensities and rational decision-making: Recent findings and promising approaches. AR Piquero, SG Tibbetts, eds. *Rational Choice and Criminal Behavior Recent Research and Future Challenges* (Routledge, New York, NY) 3-24.
Tiwana A (2009) Governance-knowledge fit in systems development projects. *Information Systems Research* 20(2):180-197.
Tiwana A (2015) Evolutionary competition in platform ecosystems. *Information Systems Research* 26(2):266-281.
Turanovic JJ, Pratt TC (2014) "Can't stop, won't stop": Self-control, risky lifestyles, and repeat victimization. *Journal of Quantitative Criminology* 30(1):29-56.
Vance A, Lowry PB, Eggett D (2013) Using accountability to reduce access policy violations in information systems. *Journal of Management Information Systems* 29(4):263-289.
Vardi Y (2001) The effects of organizational and ethical climates on misconduct at work. *Journal of Business Ethics* 29(4):325-337.
Vroom V (1964) *Work and Motivation*, (Wiley, Oxford, England).
Wachi T, Watanabe K, Yokota K, Suzuki M, Hoshino M, Sato A, Fujita G (2007) Offender and crime characteristics of female serial arsonists in Japan. *Journal of Investigative Psychology and Offender Profiling* 4(1):29-52.
Wang M, Liao H, Zhan Y, Shi J (2011) Daily customer mistreatment and employee sabotage against customers: Examining emotion and resource perspectives. *Academy of Management Journal* 54(2):312-334.
Wehrt W, Casper A, Sonnentag S (2020) Beyond depletion: Daily self-control motivation as an explanation of self-control failure at work. *Journal of Organizational Behavior* 41(9):931-947.
Wetzels M, Odekerken-Schroder G, Van Oppen C (2009) Using PLS path modeling for assessing hierarchical construct models: Guidelines and empirical illustration. *MIS Quarterly* 33(1):177-196.
Willison R, Lowry PB (2018) Disentangling the motivations for organizational insider computer abuse through the rational choice and life course perspectives. *The DATA BASE for Advances in Information Systems* 49(April):81-102.
Willison R, Lowry PB, Paternoster R (2018a) A tale of two deterrents: Considering the role of absolute and restrictive deterrence in inspiring new directions in behavioral and organizational security. *Journal of the Association for Information Systems* 19(12):1187-1216.
Willison R, Warkentin M (2013) Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly* 37(1):1-20.
Willison R, Warkentin M, Johnston AC (2018b) Examining employee computer abuse intentions: Insights from justice, deterrence and neutralization perspectives. *Information Systems Journal* 28(2):266-293.
Xu B, Xu Z, Li D (2016) Internet aggression in online communities: a contemporary deterrence perspective. *Information Systems Journal* 26(6):641-667.
Youngs D, Ioannou M, Eagles J (2016) Expressive and instrumental offending: Reconciling the paradox of specialisation and versatility. *International Journal of Offender Therapy and Comparative Criminology* 60(4):397-422.
Yu J (1994) Punishment celerity and severity: Testing a specific deterrence model on drunk driving recidivism. *Journal of Criminal Justice* 22(4):355-366.
Zhao H, Wayne SJ, Glibkowski BC, Bravo J (2007) The impact of psychological contract breach on work-related outcomes: A meta-analysis. *Personnel Psychology* 60(3):647-680.

Appendix A. Studies in "The Senior Scholars' Basket Journals" Mentioning Deterrence Theory or Self-control[1,2]

Table A.1. Studies mentioning "information security" and "deterrence theory" or "self-control"

#	Citation	Article title	Journal	Mention self-control?	Mention deterrence theory?	Measure self-control?	Measure deterrence?	DV
1	Anderson et al. (2017)	Information security control theory: Achieving a sustainable reconciliation between sharing and protecting the privacy of information	*JMIS*		X	No	No	n/a
2	Aurigemma and Mattson (2019)	Generally speaking, context matters: Making the case for a change from universal to particular ISP research	*JAIS*		X	No	Yes: Sanction probability; Sanction severity	Behavioral intent
3	Boss et al. (2009)	If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security	*EJIS*		X	No	No	Precautions taken
4	Boss et al. (2015)	What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors	*MISQ*		X	No	No	Protection motivation/Anti-malware use
5	Bulgurcu et al. (2010)	Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness	*MISQ*		X	No	Yes: Sanctions	Intention to comply
6	Chatterjee et al. (2015b)	The behavioral roots of information systems security: Exploring key factors related to unethical IT use	*JMIS*	X		No	No	Intention toward unethical IT use
7	Chatterjee et al. (2015a)	Strategic relevance of organizational virtues enabled by information technology in organizational innovation	*JMIS*	X		No	No	Organizational Innovativeness
8	Chen et al. (2012)	Organizations' information security policy compliance: Stick or carrot approach?	*JMIS*		X*	No	Yes: severity of punishment; certainty of enforcement	Compliance Intention
9	Cram et al. (2016)	Information systems control: A review and framework for emerging information systems processes	*JAIS*	X	X	No	No	n/a

#	Citation	Article title	Journal	Mention self-control?	Mention deterrence theory?	Measure self-control?	Measure deterrence?	DV
10	Cram et al. (2017)	Organizational information security policies: A review and research framework	*EJIS*	X	X	No	No	n/a
11	Cram et al. (2019)	Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance	*MISQ*		X	No	No	Meta-analysis
12	D'Arcy and Herath (2011)	A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings	*EJIS*	X	X*	No	No	n/a
13	D'Arcy and Lowry (2019)	Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study	*ISJ*		X	No	No	Compliance behavior
14	D'Arcy et al. (2014)	Understanding employee responses to stressful information security requirements: A coping perspective	*JMIS*		X	No	Yes: Perceived sanctions	Violation intention
15	D'Arcy et al. (2009)	User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach	*ISR*		X*	No	Yes: Certainty & Severity of Sanctions (vignette)	IS misuse intention
16	Dawson et al. (2010)	Information asymmetry in information systems consulting: Toward a theory of relationship constraints	*JMIS*	X		No	No	Constraint mechanism
17	Dhillon et al. (2020)	The mediating role of psychological empowerment in information security compliance intentions	*JAIS*		X	No	No	ISP compliance intention
18	Donalds and Barclay (2021)	Beyond technical measures: A value-focused thinking appraisal of strategic drivers in improving information security policy compliance	*EJIS*		X	No	No	n/a
19	Feng et al. (2019)	How paternalistic leadership influences IT security policy compliance: The mediating role of	*JAIS*		X	No	No	ISP compliance behavior

#	Citation	Article title	Journal	Mention self-control?	Mention deterrence theory?	Measure self-control?	Measure deterrence?	DV
		the social bond						
20	Foth (2016)	Factors influencing the intention to comply with data protection regulations in hospitals: Based on gender differences in behaviour and deterrence	*EJIS*		X*	No	Yes: Punishment severity; detection certainty	Intention to comply with data protections regulations
21	Guo et al. (2011)	Understanding nonmalicious security violations in the workplace: A composite behavior model	*JMIS*		X	No	Yes: Perceived sanctions	Nonmalicious security violation intention
22	Harrington (1996)	The effect of codes of ethics and personal denial of responsibility on ICA judgments and intentions	*MISQ*	X	X	No	No	ICA intention
23	Hensel and Kacprzak (2021)	Curbing cyberloafing: Studying general and specific deterrence effects with field evidence	*EJIS*		X*	No	Yes: Punishment	Cyberloafing
24	Herath and Rao (2009)	Protection motivation and deterrence: A framework for security policy compliance in organisations	*EJIS*		X*	No	Yes: Punishment severity; detection certainty	Security policy compliance intention
25	Hsu et al. (2015)	The role of extra-role behaviors and social controls in information security policy effectiveness	*ISR*		X	No	No	Extra-role and In-role behaviors
26	Hu et al. (2015)	The role of self-control in information security violations: Insights from a cognitive neuroscience perspective	*JMIS*	X*		Yes, high/low	No	Decision choices using EEG
27	Hua and Bapna (2013)	The economic impact of cyber terrorism	*JSIS*		X	No	No	Security investments
28	Hui et al. (2017)	Cybercrime deterrence and international legislation: Evidence from distributed denial of service attacks	*MISQ*		X	No	No	DDOS attacks
29	Johnston et al. (2015)	An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric	*MISQ*		X	No	Yes	Compliance intention

#	Citation	Article title	Journal	Mention self-control?	Mention deterrence theory?	Measure self-control?	Measure deterrence?	DV
30	Johnston et al. (2016)	Dispositional and situational factors: Influences on information security policy violations	*EJIS*		X	No	Yes: sanction severity & certainty (single measure)	Vignette: Intention to violate IS security policies
31	Karjalainen and Siponen (2011)	Toward a new meta-theory for designing information systems (IS) security training approaches	*JAIS*		X	No	No	n/a
32	Khansa et al. (2017)	To cyberloaf or not to cyberloaf: The impact of the announcement of formal organizational controls	*JMIS*	X	X	No	No	Cyberloafing intention
33	Kwak et al. (2019)	Measuring and controlling social desirability bias: Applications in information systems research	*JAIS*	X		No	No	Digital piracy intention
34	Lee et al. (2018)	Design and validation of the bright internet	*JAIS*		X	No	No	n/a
35	Lee et al. (2009)	Understanding post-adoption usage of mobile data services: The role of supplier-side variables	*JAIS*	X		No	No	Service usage change
36	Li et al. (2014)	Exploring the effects of organizational justice, personal ethics and sanction on internet use policy compliance	*ISJ*	X	X	No	Yes: sanction certainty; sanction severity	Internet use policy compliance intention
37	Li et al. (2021b)	The roles of IT strategy and security investments in reducing organizational security breaches	*JMIS*		X	No	No	Security breaches
38	Li et al. (2021a)	Understanding information security policy violations form a situational action perspective	*JAIS*	X		Yes	Yes: sanction certainty; sanction severity	Violation intention
39	Liang et al. (2019)	What users do besides problem-focused coping when facing It security threats: An emotion-focused coping perspective	*MISQ*	X		No	No	Problem focused coping behavior
40	Liang and Xue (2010)	Understanding security behaviors in personal computer usage: A threat avoidance perspective	*JAIS*		X	No	No	Avoidance behavior
41	Lowry and	Proposing the control-reactance	*ISJ*	X		No	No	Intent to comply

#	Citation	Article title	Journal	Mention self-control?	Mention deterrence theory?	Measure self-control?	Measure deterrence?	DV
	Moody (2015)	compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies						
42	Lowry et al. (2017a)	Why security and privacy research lies at the centre of the information systems (IS) artefact: Proposing a bold research agenda	*EJIS*		X*	No	No	n/a
43	Lowry et al. (2015)	Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: An empirical study of the influence of counterfactual reasoning and organisational trust	*ISJ*		X*	No	Yes	Reactive ICA
44	Lowry et al. (2016)	Why do adults engage in cyberbullying on social media? An integration of online disinhibition and deindividuation effects with the social structure and social learning model	*ISR*	X	X	No	No	Cyberbullying frequency
45	Lowry et al. (2019)	An integrative theory addressing cyberharassment in light of technology-based opportunism	*JMIS*	X*	X	Yes	No	Cyberharassment
46	Lowry et al. (2017b)	Using IT design to prevent cyberbullying	*JMIS*	X		Yes	No	Cyberbullying
47	Luo et al. (2020)	Why individual employees commit malicious computer abuse: A routine activity theory perspective	*JAIS*	X*	X	Yes	Yes	Computer crime
48	Moody et al. (2018)	Toward a unified model of information security policy compliance	*MISQ*	X	X*	Yes	Yes	Compliance intention
49	Murungi et al. (2019)	Control and emotions: Understanding the dynamics of controllee behaviors in a health care information systems project	*ISJ*	X		No	No	n/a (case analysis)

#	Citation	Article title	Journal	Mention self-control?	Mention deterrence theory?	Measure self-control?	Measure deterrence?	DV
50	Myyry et al. (2009)	What levels of moral reasoning and values explain adherence to information security rules? An empirical study	*EJIS*		X	No	No	Compliance
51	Ormond et al. (2019)	Integrating cognition with an affective lens to better understand information security policy compliance	*JAIS*	X	X	No	No	ISP compliance
52	Posey et al. (2015)	The impact of organizational commitment on insiders' motivation to protect organizational information assets	*JMIS*		X	No	No	Protection motivated behaviors
53	Hensel and Kacprzak (2021)	Curbing cyberloafing: studying general and specific deterrence effects with field evidence	*EJIS*		X	No	Yes	Cyberloafing
54	Puhakainen and Siponen (2010)	Improving employees' compliance through information systems security training: an action research study	*MISQ*		X	No	No	n/a (action research study)
55	Ransbotham and Mitra (2009)	Choice and chance: A conceptual model of paths to information security compromise	*ISR*	X		No	No	Security compromise
56	Salo et al. (2019)	Technostress and social networking services: Explaining user's concentration, sleep, identity, and social relation problems	*ISJ*	X		No	No	n/a (qualitative interviews)
57	Siponen and Baskerville (2018)	Intervention effect rates as a path to research relevance: Information systems security example	*JAIS*		X	No	No	n/a
58	Siponen and Vance (2010)	Neutralization: new insights into the problem of employee information systems security policy violations	*MISQ*		X*	No	Yes: formal sanctions; informal sanctions	Intention to violate IS Security policy
59	Siponen and Vance (2014)	Guidelines for improving the contextual relevance of field surveys: The case of information security policy violations	*EJIS*		X	No	No	Issues & opinions
60	Sojer et al.	Understanding the drivers of	*JMIS*		X	No	Yes:	Intention to reuse

#	Citation	Article title	Journal	Mention self-control?	Mention deterrence theory?	Measure self-control?	Measure deterrence?	DV
	(2014)	unethical programming behavior: The inappropriate reuse of internet-accessible code					punishment severity and certainty	Internet accessible code
61	Srivastava et al. (2015)	Technostress creators and job outcomes: Theorising the moderating influence of personality traits	*ISJ*	X		No	No	Job burnout/engagement
62	Straub and Welke (1998)	Coping with systems risk: Security planning models for management decision making	*MISQ*		X	No	No	n/a
63	Straub (1989)	Validating instruments in MIS research	*MISQ*		X	No	No	n/a
64	Straub (1990)	Effective IS security: An empirical study	*ISR*		X*	No	Yes: (measured as security staff salaries, etc.)	ICA
65	Trinkle et al. (2021)	High-risk deviant decisions: Does neutralization still play a role?	*JAIS*		X	No	Yes: sanction certainty; sanction severity	Intention to violate policy
66	Tsohou et al. (2015)	Managing the introduction of information security awareness programmes in organisations	*EJIS*		X	No	No	n/a
67	Turel and Qahri-Saremi (2016)	Problematic use of social networking sites: Antecedents and consequence from a dual-system theory perspective	*JMIS*	X		No	No	Academic performance
68	Turel et al. (2021)	Examining the neural basis of information security policy violations: A noninvasive brain simulation approach	*MISQ*	X	X	No	No	Nonmalicious ISP violations
69	Vance et al. (2015)	Increasing accountability through user-interface design artifacts: A new approach to addressing the problem of access-policy violations	*MISQ*		X	No	No	Intention to violate access policy
70	Wall et al. (2016)	Organizational violations of externally governed privacy and security rules: Explaining and predicting selective violations under	*JAIS*		X*	No	Yes	Likelihood of rule violation

#	Citation	Article title	Journal	Mention self-control?	Mention deterrence theory?	Measure self-control?	Measure deterrence?	DV
		conditions of strain and excess						
71	Wang et al. (2015)	Insider threats in a financial institution: Analysis of attack-proneness of information systems applications.	*MISQ*		X	No	No	Risk of unauthorized access
72	Wang et al. (2011)	Same coin, different sides: Differential impact of social learning on two facets of music piracy	*JMIS*		X	No	No	Unauthorized obtaining and sharing
73	Warkentin and Willison (2009)	Behavioral and policy issues in information systems security: The insider threat	*EJIS*		X	No	No	n/a (editorial)
74	Wiener et al. (2015)	The effective promotion of informal control in information systems offshoring projects	*EJIS*	X*		No	No	Project performance
75	Willison and Warkentin (2013)	Beyond deterrence: An expanded view of employee ICA	*MISQ*		X	No	No	n/a (editorial)
76	Willison et al. (2018a)	A tale of two deterrents: Considering the role of absolute and restrictive deterrence to inspire new directions in behavioral and organizational security research	*JAIS*	X	X*	No	No	n/a
77	Willison et al. (2018b)	Examining employee ICA intentions: Insights from justice, deterrence and neutralization perspectives	*ISJ*	X	X*	No	Yes: Sanction Severity, Sanction Certainty (vignette)	Behavioral Intention to Commit Employee ICA
78	Xiao et al. (2013)	Inter-firm IT governance in power-imbalanced buyer–supplier dyads: exploring how it works and why it lasts	*EJIS*	X		No	No	n/a
79	Xu et al. (2016)	Internet aggression in online communities: A contemporary deterrence perspective	*ISJ*		X	No	Yes (formal sanction)	Internet aggression intention
80	Yazdanmehr et al. (2020)	Peers matter: The moderating role of social influence on information security policy compliance	*ISJ*	X	X	No	No	ISP compliance

#	Citation	Article title	Journal	Mention self-control?	Mention deterrence theory?	Measure self-control?	Measure deterrence?	DV
81	Yoo et al. (2020)	Is cybersecurity a team sport? A multilevel examination of workgroup information security effectiveness	*MISQ*		X	No	No	Workgroup information security effectiveness

[1]Articles included were in the Senior Scholars' Basket of Journals (https://aisnet.org/general/custom.asp?page=SeniorScholarBasket): *European Journal of Information Systems* (*EJIS*); *Information Systems Journal* (*ISJ*); *Information Systems Research* (*ISR*); *Journal of the Association for Information Systems* (*JAIS*); *Journal of Information Technology* (*JIT*); *Journal of Management Information Systems* (*JMIS*); *Journal of Strategic Information Systems* (*JSIS*); *Management Information Systems Quarterly* (*MISQ*).
[2]Note: ISJ, ISR, JAIS, JIT, JMIS, MIS Quarterly were searched using EBSCO Business Source Complete; JSIS was not available on business source complete and was searched in the Science Direct Database; EJIS articles were not fully indexed in Business Source Complete and was searched directly from its publisher, Taylor and Francis.
* Denotes the term appears in the article abstract.

Online Appendix B. Measurement Items Included in Study

Table B.1. Constructs in Study

Construct	Item	Measurement Item	Mean	SD
Insider ICA (ICA) Posey et al. (2011)	ICA1	I have damaged computer property belonging to my employer (e.g., hardware, software, data files, etc.).	1.52	1.164
	ICA2	I have deliberately bent or broken a computer-related rule or policy.	1.81	1.356
	ICA3	I have adjusted data in the computer system to make my activity appear more in line with organizational computer guidelines, policies, and/or rules.	1.60	1.243
	ICA4	I have gone against management decisions regarding what management deems as appropriate computer system use.	1.89	1.434
	ICA5	I have sabotaged portions of the computer system.	1.48	1.195
	ICA6	I have intentionally made errors in the computer system.	1.50	1.184
	ICA7	I have covered up mistakes in the computer system.	1.60	1.224
	ICA8	I have taken computer-system resources without proper approval (e.g., hardware, software, data files).	1.59	1.242
	ICA9	I have misused my computer-system access privilege(s).	1.79	1.331
	ICA10	I have accessed files or viewed data in the computer system without being given authorization to do so.	1.74	1.304
	ICA11	I have intentionally abused the computer systems at work.	1.61	1.256
	ICA12	I have purposely abused our organization's computer systems.	1.60	1.259
Psychological contract violation (PCV) Robinson and Morrison (2000)	PCV1	I have not received everything promised to me in exchange for my contributions	2.44	1.262
	PCV2	My employer has broken many of its promises to me even though I've upheld my side of the deal	2.34	1.257
	PCV3	I feel a great deal of anger toward my organization	2.02	1.174
	PCV4	I feel betrayed by my organization	2.18	1.230
	PCV5	I feel that my organization has violated the contract between us	2.16	1.171
	PCV6	I feel extremely frustrated by how I have been treated by my organization	2.39	1.262
Financial benefits (FB) Posey et al. (2015)	FR1	I could be rewarded financially for choosing to abuse my organization's computer systems.	2.50	1.747
	FR2	I believe others would be willing to reward me financially for intentionally abusing my organization's information systems.	2.60	1.790
	FR3	The opportunity for employees to receive financial gain for abusing our organization's computer systems is considerable.	2.81	1.766

Self-control (SC) (reverse-worded) Tangney et al. (2004)	SC1	I have a hard time breaking bad habits.	5.51	1.126
	SC2	I say inappropriate things.	5.87	1.084
	SC3	I do certain things that are bad for me, if they are fun.	5.61	1.077
	SC4	Pleasure and fun sometimes keep me from getting work done.	5.79	1.133
	SC5	Sometimes I can't stop myself from doing something, even if I know it is wrong.	5.96	1.016
	SC6	I often act without thinking through all the alternatives.	6.07	0.995
Org. Deterrence (OD) Based on D'Arcy and Herath (2011) and Guo et al. (2011)	OD1	My organization deters its employees from committing information-security violations	5.22	1.428
	OD2	In general, employees are deterred from committing information-security violations by my organization	5.32	1.383
	OD3	My organization discourages its employees from engaging in information-security violations	5.41	1.468
Certainty of Sanction (Cert) Based on D'Arcy et al. (2009)	Cert1	If I were caught committing an information-security violation on the computer system, the probability that my organization would punish me would be high.	5.27	1.505
	Cert2	My organization will discipline those who it believes is guilty of information-security violations on its computer system.	5.29	1.416
	Cert3	Employees caught committing an information-security violation on the computer system will be punished by my organization.	5.35	1.413
Severity of Sanction (Severe) Based on D'Arcy et al. (2009)	Sever1	It is likely that the punishment given by my organization to employees who commit information-security violations on the computer system would be severe.	5.02	1.545
	Sever2	Organizational sanctions for employee violations of information security on the computer system would be severe.	5.06	1.514
	Sever3	My organization would take strict action against employees who are punished for committing information-security violations on the computer system.	5.19	1.461
Celerity of Sanction (Celer) Based on D'Arcy and Herath (2011)	Celer1	My organization's response (i.e., issue of punishment) to information-security violations on the computer system by employees would be instantaneous.	4.50	1.511
	Celer2	My organization would immediately punish employees who commit information-security violations on the computer system.	5.10	1.510
	Celer3	Very little time would elapse between detection of information-security violations on the computer system by employees and my organization's disciplinary response to them.	4.61	1.562
	Celer4	My organization's response (i.e., punishment) process to employee violations of information security on the computer system would be very timely.	4.94	1.450

Table B.2. Controls in Study

Construct	Item	Measurement Item	Mean/ Proportion	SD
Moral Identity (MI) (Aquino and Reed 2002)		Listed are some characteristics that may describe a person: caring, compassionate, fair, friendly, generous, hardworking, helpful, honest, and kind. The person with these characteristics could be you or it could be someone else. For a moment, visualize in your mind the kind of person who has these characteristics. Imagine how that person would think, feel, and act. When you have a clear image of what this person would be like, please respond to the following comments		
	MI1	It would make me feel good to be a person who has these characteristics.	4.42	.826
	MI2	Being someone who has these characteristics is an important part of who I am.	4.18	.829
	MI3	I strongly desire to have these characteristics.	4.13	.883
Security Education Training and Awareness (SETA) (D'Arcy et al. 2009)	SETA1	My organization makes certain its employees are fully aware of what specific information security risks/threats it experiences or might experience.	4.88	1.658
	SETA2	My organization trains its employees on how to perform their job duties in a secure manner.	4.82	1.666
	SETA3	My organization educates and explains to its employees why specific information security risks/threats exist.	4.81	1.685
	SETA4	My organization makes certain its employees are involved with information security education, training, and awareness programs.	4.71	1.711
Age		What is your age (in years)?	45.42	12.034
Tenure		How long (in years) have you been employed within this organization?	2.60	1.790
IT/IS Position		Is your occupation / job title considered to be an Information Technology (IT) or an Information Systems (IS) position?	13.6% (yes)	
Management		Is your occupation / job title considered to be a managerial position?	35.2% (yes)	
Gender		What is your gender?	49.0% (female)	

Online Appendix C. Full Correlation Matrix

Table C.1. Correlation Matrix

Variable	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
ICA (1)	1																		
Age (2)	-.239	1																	
Celerity of sanction (3)	-.095	.116	1																
Certainty of sanction (4)	-.190	.088	.809	1															
Fin. benefits X Org. Deterrence (5)	-.166	-.004	-.009	.033	1														
Fin. benefits X Self-control (6)	-.408	.155	-.043	.021	.167	1													
Financial benefits (7)	.396	-.134	-.037	-.101	.190	-.162	1												
Gender (8)	-.104	-.044	.051	.046	-.041	.027	-.111	1											
IT role (9)	.107	-.023	.098	.084	.018	-.003	.143	-.033	1										
Management (10)	.082	.066	-.079	-.091	.046	-.036	.065	-.177	.081	1									
Org Deterrence (11)	-.264	.152	.694	.793	-.081	.050	-.152	.075	.036	-.131	1								
PCV (12)	.372	-.168	-.126	-.166	-.076	-.186	.241	-.123	.057	-.033	-.278	1							
PCV X Org. Deterrence (13)	-.077	-.091	.016	-.003	.106	-.001	-.073	.038	.000	-.009	-.031	-.075	1						
PCV X Self-control (14)	-.366	.056	-.131	-.093	0	.509	-.186	-.005	-.060	-.118	-.002	-.164	.059	1					
Moral Identity (15)	-.363	.122	.230	.331	.106	.060	-.261	.205	-.093	-.051	.380	-.202	-.007	-.018	1				
SETA frequency (16)	-.103	.087	.562	.551	-.070	-.044	.017	.076	.083	-.101	.612	-.233	-.029	-.122	.142	1			
Org Sanctions (17)	-.150	.116	.930	.954	-.004	-.021	-.071	.044	.101	-.092	.792	-.146	-.004	-.121	.300	.594	1		
Severity of sanction (18)	-.145	.125	.831	.909	-.035	-.036	-.064	.029	.106	-.093	.768	-.124	-.026	-.118	.296	.577	.962	1	
Org Tenure (19)	-.136	.461	.068	.060	-.021	.073	-.082	-.017	-.008	.158	.135	-.056	-.084	-.028	.067	.095	.064	.055	1
Self-control (20)	-.409	.170	.078	.111	.060	.287	-.194	.119	-.063	-.016	.167	-.346	-.002	.379	.298	.085	.097	.087	.112

Online Appendix D. Industries in Sample

Table D.1 Industries Represented in Sample

Industry	Percentage
Construction	2.49%
Educational services	15.24%
Finance and insurance	5.54%
Health care and social assistance	13.57%
Information (e.g., publishing, broadcasting, telecommunications)	2.77%
Leisure and hospitality	1.66%
Manufacturing - durable goods (e.g., structural metals, computers, furniture)	5.54%
Manufacturing - nondurable goods (e.g., food, tobacco, textiles, paper)	3.60%
Military	1.11%
Professional and technical services (e.g., legal services, accounting)	7.48%
Public administration / government	8.03%
Trade - Retail	6.09%
Trade - Wholesale	1.39%
Transportation and warehousing	3.60%
Utilities	1.39%
Other	18.84%
Total	100.00%

Online Appendix E. Structural Model Comparisons: Main Effects, Two-stage Moderators, and Orthogonalized Moderators

As explained in Hair et al. (2017), Henseler and Chin (2010) performed an extensive simulation study and found evidence that the two-stage approach to calculating moderators is preferred when the objective of the research is to determine the statistical significance of the moderation. In PLS when the moderator is included in the model in the recommended way, the main effects become simple effects in the moderation model (e.g., the relationship between Y_1 and Y_2 when the moderator variable is equal to zero [which is its mean because it requires standardization]) (Hair et al. 2017). Simple effects are often like main effects, but there can be differences that are important for how they are interpreted. Since we hypothesize the main effects as well as the moderation effects, we included a main effects model in the appendix to verify the compatibility between the "simple effects" in the moderation model and the main effects in the model without the moderators. Running these models separately is recommended by Hair et al. (2017) to aid in the interpretation of the main effects.

An alternative approach to creating interaction terms in PLS is the orthogonalizing approach. With this approach, the main effects and simple effects in the moderation model are almost identical (Hair et al. 2017). Thus, hypotheses tests for main and moderating effects can be assessed in the same model. However, orthogonalizing approach is less robust for establishing statistical significance of moderators (Hair et al. 2017).

To account for these differences, we ran our model three times: (1) a main effects model (excluding moderators), (2) a two-stage moderator approach, and (3) an orthogonalized moderator approach. As shown in Table D.1, the three models provide identical results in terms of significance of our theoretical constructs including the moderators. This supports our inclusion of the two-step moderator approach results in the manuscript.

Table E.1 Structural Model Comparisons

Relationship	**Main Effects β (sig.)**	**Two-Stage Moderators β (sig.)**	**Orthogonalized Moderators β (sig.)**
H1. Financial benefits → ICA	0.232***	0.232***	0.232***
H2. PCV → ICA	0.175***	0.124**	0.136**
H3. Self-control → ICA	-0.227***	-0.118*	-0.209***
H4a. Self-control X Financial benefits → ICA	n/a	-0.135*	-0.067*
H4b. Self-control X PCV → ICA	n/a	-0.141**	-0.119**
H5. Organizational sanctions → Organizational. deterrence	0.793***	0.794***	0.793***
H6. Organizational deterrence → ICA	-0.076 (n/s)	-0.079(n/s)	-0.061(n/s)
H7a. Organizational deterrence X Financial benefits → ICA	n/a	-0.155***	-0.066***
H7b. Organizational deterrence X PCV → ICA	n/a	-0.040(n/s)	-0.019(n/s)
Controls	**β (sig.)**	**β (sig.)**	**β (sig.)**
Moral identity	-0.159**	-0.166**	-0.176***
SETA awareness	0.033 (n/s)	-0.030(n/s)	-0.035(n/s)
IT position	0.030(n/s)	0.038(n/s)	0.031(n/s)
Management position	0.065 (n/s)	0.037(n/s)	0.048(n/s)
Age	-0.103*	-0.087(n/s)	-0.086(n/s)
Tenure	-0.025 (n/s)	-0.037(n/s)	-0.033(n/s)
Gender	0.013 (n/s)	-0.004(n/s)	0.002(n/s)

*p = 0.05; **p = 0.01; ***p = 0.001; n/s = not significant; n/a = not applicable; calculated using 5,000 subsamples

Online Appendix F. CMV Analyses

To assess for common method variance (CMV) we performed two separate assessments recommended by (Schwarz et al. 2017): an unmeasured latent variable (UMLV) approach and a marker variable technique (i.e., a measured latent marker variable (MLMV) approach). First, following the recommendations of Liang et al. (2007), we assessed CMV using a UMLV approach. In the UMLV approach, we examined the path loadings and subsequent variance explained by each substantive variable and a new method construct made up of all the substantive items. As shown in Table B.1 below, the substantive constructs provided substantial explanation of their items (average variance explained of 0.78) and the method construct provided very little explanation of the items (average variance explained of 0.004). Additionally, there were no qualitative differences in the model including the method construct (i.e., no significance changes among substantive relationships). These results indicate that method bias is not an issue for this data (Podsakoff et al. 2003; Vance et al. 2008).

Table F.1. CMV Analysis

Construct	Indicator	R1*	$R1^2$	R2	$R2^2$
Insider ICA (ICA)	ICA1	0.908	0.824	0.011	0.000
	ICA2	0.921	0.848	-0.078	0.006
	ICA3	0.829	0.687	0.090	0.008
	ICA4	0.890	0.792	-0.062	0.004
	ICA5	0.935	0.874	-0.020	0.000
	ICA6	0.909	0.826	0.026	0.001
	ICA7	0.877	0.769	0.044	0.002
	ICA8	0.855	0.731	0.085	0.007
	ICA9	0.970	0.941	-0.117	0.014
	ICA10	0.827	0.684	0.051	0.003
	ICA11	0.957	0.916	-0.026	0.001
	ICA12	0.959	0.920	-0.019	0.000
Psychological contract violation (PCV)	PCV1	0.909	0.826	-0.073	0.005
	PCV2	0.943	0.889	-0.048	0.002
	PCV3	0.804	0.646	0.120	0.014
	PCV4	0.923	0.852	-0.014	0.000
	PCV5	0.909	0.826	0.031	0.001
	PCV6	0.929	0.863	-0.015	0.000
Financial benefits (FB)	FR1	0.911	0.830	0.055	0.003
	FR2	0.944	0.891	-0.019	0.000
	FR3	0.925	0.856	-0.038	0.001
Self-control (SC)	SC1	0.764	0.584	0.100	0.010
	SC2	0.623	0.388	-0.090	0.008
	SC3	0.759	0.576	0.088	0.008
	SC4	0.785	0.616	0.001	0.000
	SC5	0.772	0.596	-0.012	0.000
	SC6	0.634	0.402	-0.092	0.008
Organizational deterrence (OD)	OD1	0.933	0.870	0.029	0.001
	OD2	0.913	0.834	0.008	0.000
	OD3	0.857	0.734	-0.039	0.002

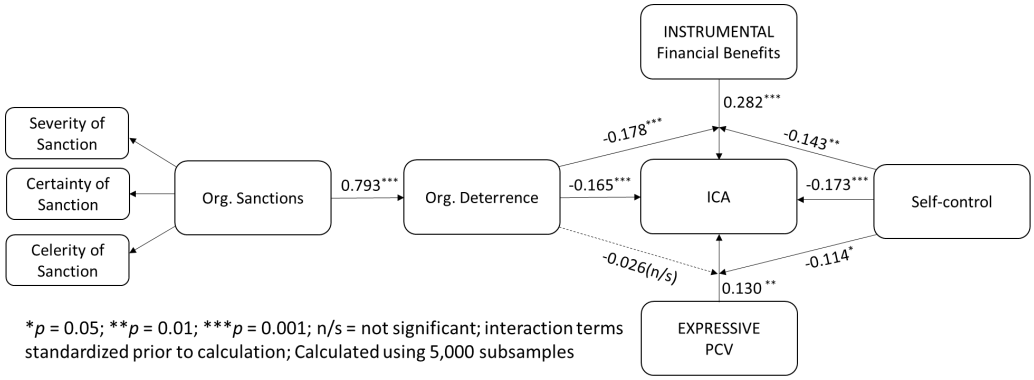
Construct	Indicator	R1*	$R1^2$	R2	$R2^2$
Certainty of Sanction (Cert)	Cert1	0.923	0.852	0.013	0.000
	Cert2	0.938	0.880	-0.011	0.000
	Cert3	0.943	0.889	-0.002	0.000
Severity of Sanction (Severe)	Severe1	0.951	0.904	0.066	0.004
	Severe2	0.948	0.899	-0.004	0.000
	Severe3	0.916	0.839	-0.059	0.003
Celerity of Sanction (Celer)	Celer1	0.894	0.799	0.078	0.006
	Celer2	0.803	0.645	-0.137	0.019
	Celer3	0.867	0.752	0.098	0.010
	Celer4	0.870	0.757	-0.029	0.001
Average		0.878	0.778	0.000	0.004

*R1 = Substantive factor loading; R2 = Method factor loading

As noted, alternative approach to the UMLV is a MLMV approach (Chin et al. 2013; Schwarz et al. 2017). While Schwarz et al. (2017) suggest a marker variable technique such as that explained by Richardson et al. (2009) and Williams et al. (2010), this techniques are applicable only for covariance-based SEM (CB-SEM). Thus, we adopted Chin et al.'s (2013) MLMV approach for partial least squares SEM (PLS-SEM) that can both detect and correct for CMV. Our marker variable measures attitude toward the color blue with a four-item scale (i.e., "I prefer blue to other colors"). As explained by Chin et al. (2013), we performed a construct-level analysis of CMV.

To perform the analysis, we created six identical CMV constructs of our MLMV and included new paths from the marker variable to each substantive variable in our model. As noted, "each CMV control uses the same entire set of MLMV items," then the CMV constructs are "modeled as impacting each model construct" (Chin et al. 2013, p. 233). Figure B.1. exhibits the baseline model for our CMV analyses and Figure B.2. exhibits the MLMV model. Chin et al. (2013) note that the model including MLMV should account for more than 70% of CMV within the data and, therefore, produce substantive relationships with little CMV bias. Therefore, to assess whether CMV has biased our results, we compared the results of the baseline CMV model and MLMV model. Table B.1. includes the results of our baseline CMV model and MLMV model. As shown the average difference in terms of beta weights between the two models was 0.004 and there were no changes in significance. These results suggest that our data does not suffer from harmful CMV.

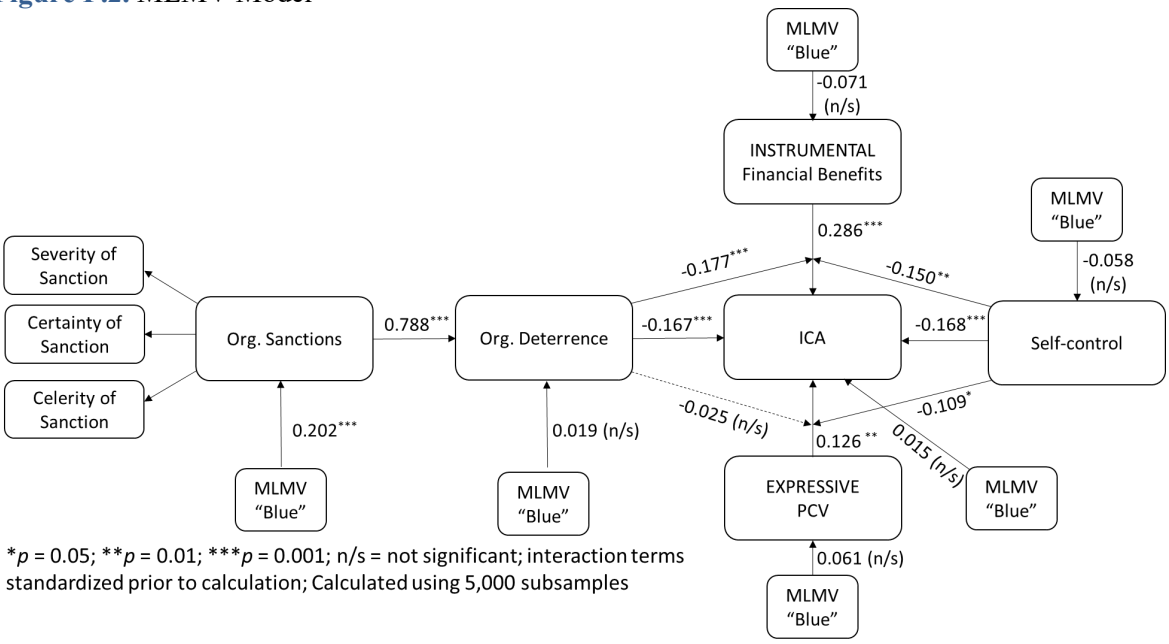
Figure F.1. Baseline CMV Model



*p = 0.05; **p = 0.01; ***p = 0.001; n/s = not significant; interaction terms standardized prior to calculation; Calculated using 5,000 subsamples

Note: The CMV analyses do not include the controls from figure 2 in the manuscript. This accounts for the differences in the results between Figures F.1. and Figure 2.

Figure F.2. MLMV Model



*p = 0.05; **p = 0.01; ***p = 0.001; n/s = not significant; interaction terms standardized prior to calculation; Calculated using 5,000 subsamples

Table F.2. MLMV CMV Method Results

Relationship	**Baseline β (sig.)**	**MLMV β (sig.)**	**Difference**	**Δ Sig.**
H1. Financial benefits → ICA	0.282***	0.286***	0.004	n/a
H2. PCV → ICA	0.130**	0.126**	0.004	n/a
H3. Self-control → ICA	-0.173***	-0.168***	0.005	n/a
H4a. Self-control X Financial benefits → ICA	-0.143**	-0.150**	0.007	n/a
H4b. Self-control X PCV → ICA	-0.114*	-0.109*	0.005	n/a
H5. Organizational sanctions → Organizational. deterrence	0.793***	0.788***	0.005	n/a
H6. Organizational deterrence → ICA	-0.165***	-0.167***	0.002	n/a
H7a. Organizational deterrence X Financial benefits → ICA	-0.178***	-0.177***	0.001	n/a
H7b. Organizational deterrence X PCV → ICA	-0.026(ns)	-0.025(n/s)	0.001	n/a
MLMV	**Baseline β (sig.)**	**MLMV β (sig.)**	**Difference**	**Δ Sig.**
MLMV → Org. Sanction	n/a	0.202	n/a	n/a
MLMV → Org. Deterrence	n/a	0.019	n/a	n/a
MLMV → Financial Benefits	n/a	0.071	n/a	n/a
MLMV → PCV	n/a	0.061	n/a	n/a
MLMV → Self-control	n/a	-0.058	n/a	n/a
MLMV → ICA	n/a	0.015	n/a	n/a

*p = 0.05; **p = 0.01; ***p = 0.001; n/s = not significant; interaction terms standardized prior to calculation; calculated using 5,000 subsamples.

References for Online Appendices

Anderson C, Baskerville RL, Kaul M (2017) Information security control theory: Achieving a sustainable reconciliation between sharing and protecting the privacy of information. *Journal of Management Information Systems* 34(4):1082-1112.

Aquino K, Reed A, II (2002) The self-importance of moral identity. *Journal of Personality and Social Psychology* 83(6):1423-1440.

Aurigemma S, Mattson T (2019) Generally speaking, context matters: Making the case for a change from universal to particular ISP research. *Journal of the Association for Information Systems* 20(12):7.

Boss SR, Galletta DF, Lowry PB, Moody GD, Polak P (2015) What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly* 39(4):837-864.

Boss SR, Kirsch LJ, Angermeier I, Shingler RA, Boss RW (2009) If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. *European Journal of Information Systems* 18(2):151-164.

Bulgurcu B, Cavusoglu H, Benbasat I (2010) Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly* 34(4):523-548.

Chatterjee S, Moody G, Lowry PB, Chakraborty S, Hardin A (2015a) Strategic relevance of organizational virtues enabled by information technology in organizational innovation. *Journal of Management Information Systems* 32(3):158-196.

Chatterjee S, Sarker S, Valacich JS (2015b) The behavioral roots of information systems security: Exploring key factors related to unethical IT use. *Journal of Management Information Systems* 31(4):49-87.

Chen Y, Ramamurthy K, Wen K-W (2012) Organizations' information security policy compliance: Stick or carrot approach? *Journal of Management Information Systems* 29(3):157-188.

Chin WW, Thatcher JB, Wright RT, Steel D (2013) Controlling for common method variance in PLS analysis: the measured latent marker variable approach. H Abdi, WW Chin, E Vinzi, R V., T G., L, eds. *New Perspectives in Partial Least Squares and Related Methods* (Springer) 231-239.

Cram WA, Brohman K, Gallupe RB (2016) Information systems control: A review and framework for emerging information systems processes. *Journal of the Association for Information Systems* 17(4):216.

Cram WA, D'arcy J, Proudfoot JG (2019) Seeing the forest and the trees: a meta-analysis of the antecedents to information security policy compliance. *MIS Quarterly* 43(2):525-554.

Cram WA, Proudfoot JG, D'Arcy J (2017) Organizational information security policies: A review and research framework. *European Journal of Information Systems* 26(6):605-641.

D'Arcy J, Herath T (2011) A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *European Journal of Information Systems* 20(6):643-658.

D'Arcy J, Herath T, Shoss M (2014) Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of Management Information Systems* 31(2):285-318.

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

D'Arcy J, Lowry PB (2019) Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal* 29(1):43-69.

Dawson GS, Watson RT, Boudreau M-C (2010) Information asymmetry in information systems consulting: Toward a theory of relationship constraints. *Journal of Management Information Systems* 27(3):143-178.

Dhillon G, Abdul Talib YY, Picoto WN (2020) The mediating role of psychological empowerment in information security compliance intentions. *Journal of the Association for Information Systems* 21(1):152-174.

Donalds C, Barclay C (2021) Beyond technical measures: A value-focused thinking appraisal of strategic drivers in improving information security policy compliance. *European Journal of Information*

*Systems*1-16.
Foth M (2016) Factors influencing the intention to comply with data protection regulations in hospitals: based on gender differences in behaviour and deterrence. *European Journal of Information Systems* 25(2):91-109.
Guo KH, Yuan Y, Archer NP, Connelly CE (2011) Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems* 28(2):203-236.
Hair JF, Hult GTM, Ringle CM, Sarstedt M (2017) *A Primer on Partial Least Squares Structural Equations Modeling (PLS-SEM), 2nd Edition*, (Sage, Thousand Oaks, CA).
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.
Hensel PG, Kacprzak A (2021) Curbing cyberloafing: Studying general and specific deterrence effects with field evidence. *European Journal of Information Systems* 30(2):219-235.
Henseler J, Chin WW (2010) A Comparison of Approaches for the Analysis of Interaction Effects Between Latent Variables Using Partial Least Squares Path Modeling. *Structural Equation Modeling: A Multidisciplinary Journal* 17(1):82-109.
Herath T, Rao HR (2009) Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems* 18(2):106-125.
Hsu JS-C, Shih S-P, Hung YW, Lowry PB (2015) The role of extra-role behaviors and social controls in information security policy effectiveness. *Information Systems Research* 26(2):282-300.
Hu Q, West R, Smarandescu L (2015) The role of self-control in information security violations: Insights from a cognitive neuroscience perspective. *Journal of Management Information Systems* 31(4):6-48.
Hua J, Bapna S (2013) The economic impact of cyber terrorism. *The Journal of Strategic Information Systems* 22(2):175-186.
Hui K-L, Kim SH, Wang Q-H (2017) Cybercrime deterrence and international legislation: evidence from distributed denial of service attacks. *MIS Quarterly* 41(2):497.
Johnston AC, Warkentin M, McBride M, Carter L (2016) Dispositional and situational factors: influences on information security policy violations. *European Journal of Information Systems* 25(3):231-251.
Johnston AC, Warkentin M, Siponen M (2015) An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly* 39(1):113-134.
Karjalainen M, Siponen M (2011) Toward a new meta-theory for designing information systems (IS) security training approaches. *Journal of the Association for Information Systems* 12(8):518-555.
Khansa L, Kuem J, Siponen M, Kim SS (2017) To cyberloaf or not to cyberloaf: The impact of the announcement of formal organizational controls. *Journal of Management Information Systems* 34(1):141-176.
Kwak D-H, Holtkamp P, Kim SS (2019) Measuring and controlling social desirability bias: Applications in information systems research. *Journal of the Association for Information Systems* 20(4):317-345.
Lee JK, Cho D, Lim GG (2018) Design and validation of the Bright Internet. *Journal of the Association for Information Systems* 19(2):63-85.
Lee S, Shin B, Lee HG (2009) Understanding post-adoption usage of mobile data services: The role of supplier-side variables. *Journal of the Association for Information Systems* 10(12):2.
Li H, Luo XR, Chen Y (2021a) Understanding information security policy violation from a situational action perspective. *Journal of the Association for Information Systems* 22(3):5.
Li H, Sarathy R, Zhang J, Luo X (2014) Exploring the effects of organizational justice, personal ethics and sanction on Internet use policy compliance. *Information Systems Journal* 24(6):479-502.
Li H, Yoo S, Kettinger WJ (2021b) The roles of IT strategies and security investments in reducing organizational security breaches. *Journal of Management Information Systems* 38(1):222-245.
Liang H, Saraf N, Hu Q, Xue Y (2007) Assimilation of enterprise systems: The effect of institutional pressures and the mediating role of top management. *MIS Quarterly* 31(1):59-87.
Liang H, Xue Y (2010) Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems* 11(7):394-413.

Liang H, Xue Y, Pinsonneault A, Wu Y (2019) What users do besides problem-focused coping when facing IT security threats: An emotion-focused coping perspective. *MIS Quarterly* 43(2):373-394.
Lowry PB, Dinev T, Willison R (2017a) Why security and privacy research lies at the centre of the information systems (IS) artefact: Proposing a bold research agenda. *European Journal of Information Systems* 26(6):546-563.
Lowry PB, Moody GD (2015) Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies. *Information Systems Journal* 25(5):433-463.
Lowry PB, Moody GD, Chatterjee S (2017b) Using IT design to prevent cyberbullying. *Journal of Management Information Systems* 34(3):863-901.
Lowry PB, Posey C, Bennett RJ, Roberts TL (2015) Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: An empirical study of the influence of counterfactual reasoning and organisational trust. *Information Systems Journal* 25(3):193-273.
Lowry PB, Zhang J, Moody GD, Chatterjee S, Wang C, Wu T (2019) An integrative theory addressing cyberharassment in the light of technology-based opportunism. *Journal of Management Information Systems* 36(4):1142-1178.
Lowry PB, Zhang J, Wang C, Siponen M (2016) Why do adults engage in cyberbullying on social media? An integration of online disinhibition and deindividuation effects with the social structure and social learning model. *Information Systems Research* 27(4):962-986.
Luo XR, Li H, Hu Q, Xu H (2020) Why individual employees commit malicious computer abuse: A routine activity theory perspective. *Journal of the Association for Information Systems* 21(6):1552-1593.
Moody GD, Siponen M, Pahnila S (2018) Toward a unified model of information security policy compliance. *MIS Quarterly* 42(1):285-311.
Murungi D, Wiener M, Marabelli M (2019) Control and emotions: Understanding the dynamics of controllee behaviours in a health care information systems project. *Information Systems Journal* 29(5):1058-1082.
Myyry L, Siponen M, Pahnila S, Vartiainen T, Vance A (2009) What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems* 18(2):126-139.
Ormond D, Warkentin M, Crossler RE (2019) Integrating cognition with an affective lens to better understand information security policy compliance. *Journal of the Association for Information Systems* 20(12):1794-1843.
Podsakoff PM, MacKenzie SB, Lee JY, Podsakoff NP (2003) Common method biases in behavioral research: a critical review of the literature and recommended remedies. *Journal of Applied Psychology* 88(5):879-903.
Posey C, Bennett RJ, Roberts TL (2011) Understanding the mindset of the abusive insider: An examination of insiders' causal reasoning following internal security changes. *Computers & Security* 30(6):486-497.
Posey C, Roberts TL, Lowry PB (2015) The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems* 32(4):179-214.
Puhakainen P, Siponen M (2010) Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly* 34(4):757-778.
Ransbotham S, Mitra S (2009) Choice and chance: A conceptual model of paths to information security compromise. *Information Systems Research* 20(1):121-139.
Richardson HA, Simmering MJ, Sturman MC (2009) A tale of three perspectives. *Organizational Research Methods* 12(4):762-800.
Robinson SL, Morrison EW (2000) The development of psychological contract breach and violation: a longitudinal study. *Journal of Organizational Behavior* 21(5):525-546.

Salo M, Pirkkalainen H, Koskelainen T (2019) Technostress and social networking services: Explaining users' concentration, sleep, identity, and social relation problems. *Information Systems Journal* 29(2):408-435.
Schwarz A, Rizzuto T, Carraher-Wolverton C, Roldán JL, Barrera-Barrera R (2017) Examining the impact and detection of the urban legend of common method bias. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems* 48(1):93-119.
Siponen M, Baskerville R (2018) Intervention Effect Rates as a Path to Research Relevance: Information Systems Security Example. *Journal of the Association for Information Systems* 19(4):247-265.
Siponen M, Vance A (2010) Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly* 34(3):487-502.
Siponen M, Vance A (2014) Guidelines for improving the contextual relevance of field surveys: The case of information security policy violations. *European Journal of Information Systems* 23(3):289-305.
Sojer M, Alexy O, Kleinknecht S, Henkel J (2014) Understanding the drivers of unethical programming behavior: The inappropriate reuse of internet-accessible code. *Journal of Management Information Systems* 31(3):287-325.
Srivastava SC, Chandra S, Shirish A (2015) Technostress creators and job outcomes: theorising the moderating influence of personality traits. *Information Systems Journal* 25(4):355-401.
Straub DW (1989) Validating instruments in MIS research. *MIS Quarterly* 13(2):147-169.
Straub DW (1990) Effective IS security. *Information Systems Research* 1(3):255-276.
Straub DW, Welke RJ (1998) Coping with systems risk: Security planning models for management decision making. *MIS Quarterly* 22(4):441-469.
Tangney JP, Baumeister RF, Boone AL (2004) High self-control predicts good adjustment, less pathology, better grades, and interpersonal success. *Journal of Personality* 72(2):271-324.
Trinkle BS, Warkentin M, Malimage K, Raddatz N (2021) High-risk deviant decisions: Does neutralization still play a role? *Journal of the Association for Information Systems* 22(3):797-826.
Tsohou A, Karyda M, Kokolakis S, Kiountouzis E (2015) Managing the introduction of information security awareness programmes in organisations. *European Journal of Information Systems* 24(1):38-58.
Turel O, He Q, Wen Y (2021) Examining the neural basis of information security policy violations: A non-invasive brain stimulation approach. *MIS Quarterly* 45(4):1715-1744.
Turel O, Qahri-Saremi H (2016) Problematic use of social networking sites: antecedents and consequence from a dual-system theory perspective. *Journal of Management Information Systems* 33(4):1087-1116.
Vance A, Elie-Dit-Cosaque C, Straub DW (2008) Examining trust in information technology artifacts: the effects of system quality and culture. *Journal of Management Information Systems* 24(4):73-100.
Vance A, Lowry PB, Eggett D (2015) Increasing accountability through user-interface design artifacts: A new approach to addressing the problem of access-policy violations. *MIS quarterly* 39(2):345-366.
Wall J, Lowry PB, Barlow JB (2016) Organizational violations of externally governed privacy and security rules: Explaining and predicting selective violations under conditions of strain and excess. *Journal of the Association for Information Systems* 17(1):39-76.
Wang J, Gupta M, Rao HR (2015) Insider threats in a financial institution: Analysis of attack-proneness of information systems applications. *MIS quarterly* 39(1).
Wang J, Yang Z, Bhattacharjee S (2011) Same coin, different sides: Differential impact of social learning on two facets of music piracy. *Journal of Management Information Systems* 28(3):343-384.
Warkentin M, Willison R (2009) Behavioral and policy issues in information systems security: The insider threat. *European Journal of Information Systems* 18(2):101-105.
Wiener M, Remus U, Heumann J, Mähring M (2015) The effective promotion of informal control in information systems offshoring projects. *European Journal of Information Systems* 24(6):569-587.
Williams LJ, Hartman N, Cavazotte F (2010) Method variance and marker variables: A review and comprehensive CFA marker technique. *Organizational Research Methods* 13(3):477-514.
Willison R, Lowry PB, Paternoster R (2018a) A tale of two deterrents: Considering the role of absolute

and restrictive deterrence in inspiring new directions in behavioral and organizational security. *Journal of the Association for Information Systems* 19(12):1187-1216.
Willison R, Warkentin M (2013) Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly* 37(1):1-20.
Willison R, Warkentin M, Johnston AC (2018b) Examining employee computer abuse intentions: Insights from justice, deterrence and neutralization perspectives. *Information Systems Journal* 28(2):266-293.
Xiao J, Xie K, Hu Q (2013) Inter-firm IT governance in power-imbalanced buyer–supplier dyads: exploring how it works and why it lasts. *European Journal of Information Systems* 22(5):512-528.
Xu B, Xu Z, Li D (2016) Internet aggression in online communities: a contemporary deterrence perspective. *Information Systems Journal* 26(6):641-667.
Yazdanmehr A, Wang J, Yang Z (2020) Peers matter: The moderating role of social influence on information security policy compliance. *Information Systems Journal* 30(5):791-844.
Yoo CW, Goo J, Rao HR (2020) Is cybersecurity a team sport? A multilevel examination of workgroup information security effectiveness. *MIS Quarterly* 44(2):907-931.