Journal of the Association for Information Systems (2020) **21**(6), 1552-1593
doi: 10.17705/1jais.000646

RESEARCH ARTICLE

ISSN 1536-9323

Why Individual Employees Commit Malicious Computer Abuse: A Routine Activity Theory Perspective

Xin (Robert) Luo[1], Han Li[2], Qing Hu[3], Heng Xu[4]

[1]The University of New Mexico, USA, xinluo@unm.edu
[2]The University of New Mexico, USA, hanli@unm.edu
[3]Brooklyn College, The City University of New York, USA, qing.hu@brooklyn.cuny.edu
[4]American University, USA, xu@american.edu

Abstract

Prior information security studies have largely focused on understanding employee security behavior from a policy compliance perspective. We contend that there is a pressing need to develop a comprehensive understanding of the circumstances that lead to employee commitment of deliberate and malicious acts against organizational digital assets. Drawing on routine activity theory (RAT), we seek to establish a comprehensive model of employee-committed malicious computer abuse (MCA) by investigating the motivations of the offenders, the suitability of the desired targets, and the effect of security guardianship in organizational settings. Specifically, we delineate the effects of the individual characteristics of self-control, hacking self-efficacy, and moral beliefs, as well as the organizational aspects of deterrence based on the routine activity framework of crime. We tested this research model using research participants holding a wide range of corporate positions and possessing varying degrees of computer skills. Our findings offer fresh insights on insider security threats, identify new directions for future research, and provide managers with prescriptive guidance for formulating effective security policies and management programs for preventing MCA in organizations.

Keywords: Routine Activity Theory, Information Security, Insider Threat, Malicious Computer Abuse, Security Management

Suprateek Sarker was the accepting senior editor. This research article was submitted on November 1, 2017 and underwent three revisions.

1 Introduction

Insider threats to organizational information security are becoming increasingly significant concerns for government agencies, as epitomized, for example, by the widely publicized Chelsea Manning (Savage & Huetteman, 2013) and Edward Snowden (Gellma, Blake, & Miller, 2013) incidents. Insider security threats are also prevalent and serious in organizations of all sizes and in all industries. According to a recent survey, 89% of respondents felt that their organizations were at risk from insider attacks, and 34% felt very or extremely vulnerable (Kellett, 2015). A CERT (2016) report suggests that although only 23% of electronic crime events were suspected or known to be caused by insiders, 45% of the respondents thought that damage by insider attacks was more severe than that from outsiders.

It is therefore no coincidence that many information systems (IS) scholars have studied information security from the perspectives of understanding and managing insider threats to organizations, especially regarding the information security behavior of employees who have routine access to organizational

data and information systems. IS researchers have studied information security threats of internal employees since the early 1990s (see a summary of the literature in Appendix A). One common insight from these prior studies is that internal employees represent one of the greatest threats to an organization's information security, as they are closest to the organizational data and information (Whitman & Mattord, 2005). As such, *human factors* are more likely to cause serious security breaches than technological vulnerabilities and are often deemed the weakest link in corporate information security defense. Most extant behavioral IS security studies have endeavored to employ theories from various disciplines (e.g., fear appeal, general deterrence theory, theory of planned behavior, rational choice theory, social learning theory, etc.) to understand and analyze cybersecurity issues related to insiders, such as employees' information security precaution-taking behavior, employees' compliance with or violation of policies, employees' security awareness programs, employees' motivations to perform computer abuse, and effects of organizational sanctions (see Appendix A).

While these studies have significantly enriched our understanding of employee security behavior in this context, our literature review shows that most of these studies have focused on employee security behaviors or deviant acts with *nonmalicious* intent (see Appendix A). Unintentional and nonmalicious violations of organizational information security policies and procedures by employees could dramatically weaken multilayered security defense systems and expose the vulnerabilities of security defense to both internal and external threats. But, in reality, it often requires deliberate actions by either internal or external actors with malicious intent to take advantage of these vulnerabilities and weaknesses in a way that causes security breaches and significant economic, social, and political damage to organizations. Thus, we argue that there is a significant need to advance this line of research in order to capture and assess the crucial factors that lead to employees committing computer-related abuse with malicious intent in organizations.

To differentiate this study from prior research that studies employee violations of information security policies (ISPs) which may or may not be malicious, we choose malicious computer abuse (MCA) by insiders as the focal phenomenon and dependent variable of this research. We define MCA as deliberate and malicious digital asset abuse that violates established organizational policies (Willison and Warkentin, 2013). More specifically, MCA refers to activities where computers and systems are used as tools by offenders to target, access, transfer, or alter restricted organizational data or information for fraudulent and perhaps unlawful purposes.

Because MCA committed by individuals either inside or outside an organization becomes cybercrime when federal and/or state laws are violated, as they often do, in searching for a strong theoretical foundation for our research, we naturally gravitated to criminology as a primary reference discipline for understanding this phenomenon. After a thorough review of commonly used criminological theories in the literature, a widely acclaimed and tested general crime theory, routine activity theory (RAT) (Cohen & Felson, 1979), emerged as a salient theoretical framework to contextualize and build a theory-based empirical model for understanding MCA committed by employee insiders. This is because those organizational insiders are often privileged information systems users, whose routine organizational activities converge in time and space with sensitive and valuable digital assets in their organization, and according to RAT, are afforded rich and unique situational opportunities for committing MCA.

RAT was developed by Cohen and Felson (1979) to explain the variation in national crime rates over time and in different geographic regions between 1947-1974, when significant economic and sociological trend shifts occurred in the United States following World War II. Cohen and Felson (1979) argue that structural changes in daily routines in society influence crime opportunities and, therefore, affect crime rates and crime trends at regional and national levels. The central proposition of RAT is that criminal acts result from the convergence in time and space of three key elements: motivated offenders, suitable targets, and the absence of capable guardians to prevent criminal acts (Cohen & Felson, 1979). Crime opportunities emerge when a motivated offender has the opportunity to interact with a suitable target in the absence of capable guardians, given a physical location conducive to such an interaction. RAT implicitly assumes that (1) there are three key elements of crime (offender motivation, suitable target, and absence of capable guardian) but identifies no specific factors that contribute to the formation of these elements; (2) there is a constant supply of motivated offenders with criminal inclination (Pratt, Holtfreter, & Reisig, 2010); (3) these offenders are rational decision makers who evaluate the suitability of a target and the absence of capable guardianship; and (4) when the three key elements of crime converge in time and space, a crime occurs.

In recent years, criminologists have attempted to adapt RAT from the physical world to the virtual world in order to explain the dramatic emergence of cybercrime (e.g., Leukfeldt & Yar, 2016; Yar, 2005). However, empirical support for the validity of RAT in cyberspace has been mixed. The wide variety of cybercrimes examined and the issues in the operationalization of RAT constructs in these studies may have contributed

to the mixed findings (Leukfeldt & Yar, 2016). Further, these RAT-based criminological studies almost exclusively focus on the victims or victimization (Leukfeldt & Yar, 2016; Wilcox & Cullen, 2018), trying to understand how the characteristics of individual internet users and their personal security measures affect their chances of being victimized. Diverging from these previous studies, we shift the attention to the protection of organizational digital assets and focus on motivated offenders, or insiders who commit malicious acts against their organizational data and systems.

Moreover, prior studies based on RAT have generally treated crime motivation (i.e., the motivated offender) as a given without explicitly identifying the motivational sources. As suggested in the literature summary in Appendix A, our study is the first that operationalizes and empirically tests the underlying dimensions of all three pillars of crime articulated in RAT in the context of MCA in organizational settings. This study is also among the first that extends and contextualizes the RAT framework by identifying antecedents and moderators for the core RAT constructs and relationships. Therefore, the major research questions that drive this study are:

1. *How and why are employees motivated to commit MCA at the workplace?*
2. *What and how are organizational and computer system factors conducive to MCA in an organization?*

By contextualizing RAT in organizational information security settings, integrating with other theories of crime, and validating the resulting comprehensive insider security behavioral model with data from a wide range of employee subjects, we hope to make a significant contribution to a comprehensive understanding of insider MCA and a significant improvement of information security management practices.

2 Theoretical Development

2.1 Malicious Computer Abuse and Routine Activity Theory

As a well-established criminological theory, RAT has attracted significant interest in criminology and has been subjected to numerous empirical studies. RAT's simple analytical framework allows for straightforward applications in a variety of criminal activities and its clear guidance allows for the development of policies and crime prevention initiatives (Leukfeldt & Yar, 2016). RAT has been used to examine various crimes, from burglary (Cohen & Felson, 1979) to automobile theft (Rice & Csmith, 2002). With the advent of digital computer and networking technologies, RAT has been further adapted to various digital contexts to explain cybercrimes, such as consumer fraud targeting online shoppers (Pratt et al., 2010), cyberstalking (Reyns, Henson, & Fisher, 2011), and identity theft (Reyns, 2013). Holsapple et al. (2008) applied the theory to provide an explanation of software piracy. Willison (2006) analyzed a case associated with the Barings Bank collapse, using RAT to understand the effect of organizational context on computer crimes committed by insiders. Wang et al. (2015) analyzed computer log files to understand the effect of target properties and guardianship on the risk of insider threats. However, no prior studies have operationalized all three key elements in RAT and empirically examined MCA by insiders with datasets that include both behavioral and physical characteristics of the criminal elements.

RAT emphasizes the importance of both motivation and situational opportunities for crimes to occur. Prior studies have used RAT as the conceptual foundation to develop contextualized versions of RAT, also called situational opportunity theories of crime (Wilcox & Cullen, 2018). Opportunities are highly crime specific, requiring the examination of the immediate crime context (Clarke, 2012). These different strands of situational opportunity theories are essentially RAT extended to different opportunistic contexts that induce offending (Wilcox & Cullen, 2018). One such strand focuses on how situational crime opportunities help explain the concentration of crimes in certain physical spaces (Wilcox & Cullen, 2018). For example, Brantingham and Brantingham (2008) propose a crime pattern theory, arguing that suitable targets for traditional crimes tend to fall within the familiar physical space of offenders.

Despite the wide recognition of the importance of situational opportunities, Wilcox and Cullen (2018) point out some issues regarding unresolved specification suffered by situational opportunity theories of crime, such as how situational opportunity may mediate the effect of low self-control. One strategy suggested by Wilcox and Cullen (2018) for addressing the unresolved specification is to use a hybrid approach, i.e., using traditional criminological theories to enrich opportunity theories. To answer the call for the hybrid approach and to highlight features of malicious computer abuse opportunities, we integrate relevant constructs in other criminological theories and follow the research on theory contextualization (Hong et al., 2014; Johns, 2006, 2017) to build a contextualized version of RAT for employee MCA of organizational digital assets.

There are two general approaches for theory contextualization, i.e., single context vs. cross-context (Hong et al., 2014). The former contextualizes a general theory in a single context by adding, removing, and/or decomposing its core constructs and by

integrating context-relevant antecedents and moderators into the theory. The cross-context approach attempts to replicate theoretical models in different contexts and then apply theory-grounded meta-analyses to consolidate the findings to build a context-contingent theory. Hong et al. (2014) proposed six guidelines for single-context theory contextualization (see details in Section 4 of their paper). In this study, we adopted the single-context approach and took five steps to enrich our RAT-based core framework with context-specific antecedents and moderators. Table 1 summarizes these steps and the mapping to the guidelines suggested by Hong et al. (2014). Besides the above steps, we also tested the research model under three different MCA situational scenarios (see details in Section 4). The three scenarios provide further contextual richness for the occurrence of MCAs.

As our study focuses on the factors that lead individual employees to commit MCA at the workplace, we take an insider perspective when applying RAT. In particular, we consider MCA at the workplace as the result of individual employees with offending motivations who make calculative assessments based on their assessment of target suitability (accessibility, usability, and visibility) and the level of guardianship (e.g., security policies, law enforcement, and security technologies in place). Therefore, as illustrated in Figure 1, we argue, based on RAT, that an employee's intention to commit MCA is driven by three essential but independent forces: (1) the offender motivation, (2) the target suitability, and (3) the guardianship provided to the target. These three forces could take different forms for different types of deviant acts in different social and organizational contexts. For example, when evaluating target suitability in the context of a street crime, a potential offender would likely consider the physical size of the target, whereas, for MCA, the accessibility of the data may be a primary consideration. In the following subsections, we further articulate the specific forms of each driving force in the context of MCA in organizations.

Table 1. Summary of Theory Contextualization Following the Guidelines by Hong et al. (2014).

	Mapping Guideline (Hong et al., 2014)	**Activities Performed in this Study**
Step 0	Guideline 1: Identify a general theory and use it as the basis to guide the theory contextualization.	Select RAT as the general theory.
Step 1	Guideline 3: Thorough evaluation of the context to identify context-specific factors.	Identify context-specific subdimensions of the three RAT core constructs since opportunities that enable traditional crimes are quite different from those enabling MCA.
Step 2	Guideline 3: Thorough evaluation of the context to identify context-specific factors.	Identify contextual factors that influence the core constructs of RAT. In particular, we identified four such factors, i.e., low self-control, hack self-efficacy, deterrence, and personal moral beliefs based on criminological literature.
Step 3	Guideline 4: Modeling context-specific factors.	Model context-specific subdimensions identified in Step 2 as the formative indicators of these three RAT core constructs.
Step 4	Guideline 4: Modeling context-specific factors.	Model low self-control, hacking self-efficacy, and deterrence as the direct antecedents of the RAT core constructs and explicitly test the mediating effects of RAT core constructs.
Step 5	Guideline 5: Examination of the interplay between the IT artifact and other factors	Model personal moral beliefs as a moderator that conditions the effect of RAT core constructs on MCA intention.

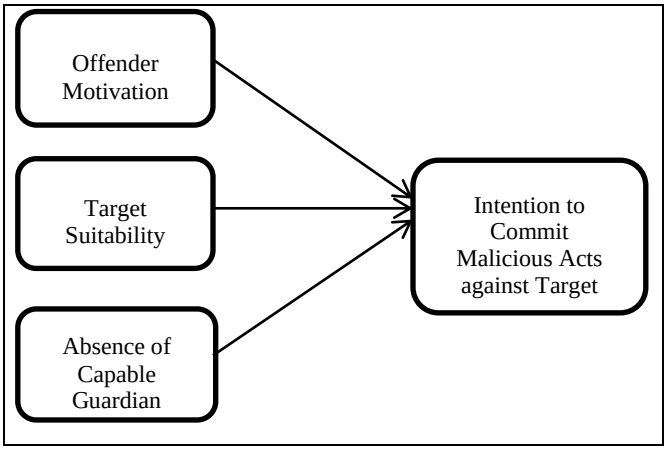

Figure 1. Conceptual Model Based on RAT

2.2 Offender Motivation

RAT suggests that a crime needs an offender who is motivated to commit the criminal act. However, RAT assumes the existence of such motivated offenders without specifying the underlying forces that may transform an ordinary individual into a motivated offender (Cohen & Felson, 1979; Yar, 2005). It is not clear how offender motivation develops and congeals in an individual to facilitate such a transformation. Since we cannot assume that every employee in an organization is a motivated offender, understanding how an ordinary employee becomes a motivated offender is paramount to information security theory and practice. To fill the gap, we draw on the information systems and criminology literatures to explore offender motivation in organizational settings.

Offenders usually engage in crimes because of self-interest, which is defined as anything that the offenders perceive to be of personal value or personally beneficial (Herbert, Green, & Larrogoite, 1998). The recognized motivations for crime range from material benefits to noneconomic gains (Burt & Simons, 2003), involving both intrinsic as well as extrinsic motivations. The offenders could be motivated by extrinsic values such as financial gains from the illegal acts as well as intrinsic benefits such as thrill, esteem, status, and peer-group acceptance (Burt & Simons, 2003; Cohen, Kluegel, & Land, 1981). However, not all offenders are susceptible to the influence of intrinsic and extrinsic values of deviant acts to the same degree; individual self-control appears to play a significant role in the evaluation of intrinsic and extrinsic values and thus in the formation of offender motivation (Gottfredson & Hirschi, 1990; Hu et al., 2011). In addition to extrinsic and intrinsic values expected from committing a deviant act, the motivation of an offender may also entail the assessment of harmfulness to others, given that lack of harmfulness is often used by offenders to justify their actions according to neutralization theory (Siponen & Vance, 2010). For example, those who commit computer crimes were found to deny the harmfulness of their actions (Parker, 1998). In a study of white-collar crimes, offenders convicted of economic offenses unanimously denied that their actions were motivated by a criminal mind or victimizing intent (Benson, 1985). Therefore, lack of harmfulness may act as another key dimension inherent in the motivation of insider offenders.

2.3 Target Suitability

A suitable target refers to a person or an object that is attractive and available as a victim to the offender (Cohen & Felson, 1979; Felson, 1998). An offender is assumed to be a rational decision maker who assesses the value and availability of the target before deciding whether to engage in a criminal act. Cohen and Felson (1979) and Felson (1998) articulate four different target suitability measures based on the potential offender's viewpoint: value (V), inertia (I), visibility (V), and access (A) of the target, or VIVA. In essence, they argue that target suitability is likely to reflect such things as the material or symbolic value of a personal or property target for offenders, the inertia of the target against illegal treatment by offenders (including the weight, size, and attached or locked features of property inhibiting its removal, as well as the physical capacity of personal victims to resist criminal acts with or without weapons), the physical visibility of the target, and easy access to and away from the offense location.

The three properties of suitable targets, i.e., inertia, physical visibility, and easy access to and away from the offense location are contextualized to "street crimes" that involve physical objects. To adapt these properties to the MCA context targeted at digital assets within an organization, we operationalize target suitability as the perceived suitability of digital assets based on potential offenders' evaluation of their *accessibility*, *visibility*, and *usability*. The rationale for such operationalization is discussed in detail below.

In the context of MCA in organizations, accessibility refers to the extent to which a potential offender has access to the target (i.e., access to digital assets, either authorized or unauthorized). The inside offender can use internal computers to bypass or penetrate organizational cybersecurity defense to gain access to digital targets. In addition, the potential offender can utilize various technologies (e.g., anonymous remailer, encryption tools, third-party servers, and systems) to maintain anonymity and strengthen the level of accessibility, thus providing the potential offender with the ability to get away easily in the context of the digital environment.

Another tenet of target suitability is visibility. RAT indicates that the level of target visibility increases the target suitability (Yar, 2005). In the context of MCA in an organization, visibility refers to the extent to which a potential offender becomes aware of the existence of a valuable digital target and knows where the desired target resides (e.g., a document folder, a database server). According to Yar (2005), "the typology of cyberspace is largely unlimited by barriers of physical distance, this renders virtually present entities visible, hence advertising their existence to the possible pool of motivated offenders" (p. 421). Wang et al. (2015) operationalized visibility as users who are given access to the targeted digital assets. However, potential offenders may recognize the existence of valuable digital assets through various means such as file and database names, internal memos, operational procedures, digital portals and directories, advertisement, and search engines. Organizations that are careless about disclosing the existence or ownership of confidential and valuable digital assets (e.g., credit card records or information about individual identity, product design, and key manufacturing know-how) are

likely to attract the attention of both internal and external offenders.

The inertia of crime targets is another component of target suitability, which refers to the physical properties of objects (e.g., weight and volume) that might offer varying degrees of resistance to effective predation (Cohen & Felson, 1979; Felson, 1998). Although the targets of MCA do not possess such physical properties, digital goods could retain inertial properties to some degree. For example, Yar (2005) notes that the level of inertia of digital targets may be impacted by the volume of a target (e.g., file size) if the potential offender has limited technological means (e.g., insufficient storage capacity or limited network bandwidth). However, given the abundance of high- capacity storage devices and high-speed digital networks in today's digital environment, the issue of file size has become less significant.

In the context of MCA, we expand the concept of physical inertia to digital usability of the target and define it as the degree to which the potential offender can appropriate the information contained in the target once it is acquired. Copying an encrypted database without being able to decrypt the data or having just one fraction of the data while the rest is distributed over multiple servers in multiple locations would render the target useless to the offender. In this vein, we predict that the usability issue of the encrypted digital target is likely to weaken the level of target suitability. Usability could be considered as digitally equivalent to physical inertia.

2.4 Security Guardianship

RAT assumes that a motivated offender assesses the level of security guardianship of the target before deciding whether to commit a crime. In this study, we refer to security guardianship as a set of organizational security measures, policies, controls, and programs for protecting digital assets. This construct is distinct from technical measures designed to reduce the suitability of specific targets such as encryption. To protect digital assets against potential computer abuse, most organizations have established security policies and guidelines to delineate penalties and disciplinary actions and rely on monitoring software and hardware to detect violations of these security policies. Organizations also implement security education, training, and awareness (SETA) programs (D'Arcy, Hovav, & Galletta, 2009; Karjalainen & Siponen, 2011). SETA programs are necessary not only for increasing employee awareness of security policies and enforcement measures but also to help employees understand the reasons underlying the security policies and the consequences of security violations. Security policies and controls, computer and network monitoring, and SETA programs are all necessary and complementary components serving as the cornerstones of security guardianship. Therefore, we operationalize the construct of absence of capable guardianship in three subdimensions, i.e., the absence of security policies, security monitoring, and SETA programs. When present, these tools can effectively convey the appropriate security conduct for ordinary employees (D'Arcy et al., 2009).

3 Research Model and Hypotheses

To facilitate the development of our research hypotheses, we first present a parsimonious RAT model (Figure 1) that delineates the roles of offender motivation, target suitability, and absence of capable guardianship in the formation of an individual's MCA intention. We now present a contextualized model (Figure 2) by integrating two sets of exogenous variables to the core RAT model in order to address the major issues of the RAT framework discussed above.

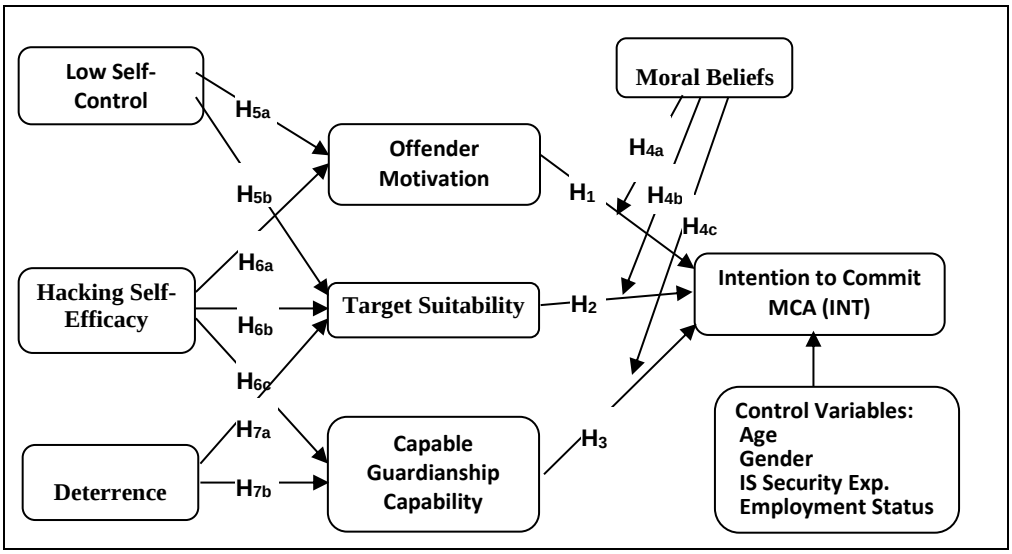

Figure 2. Research Model

In this model, we suggest that an employee's intention to commit MCA is the result of a calculative assessment of target suitability and security guardianship by the motivated offender in the presence of the moderators and antecedents of the three key RAT constructs. The construct of individual moral beliefs is introduced as an important moderator constraining the effects of three core constructs in RAT, while an employee's criminal propensity (i.e., low self-control), capability of committing MCA (i.e., hacking self-efficacy), and deterrence measures are used as the antecedents of the core RAT constructs.

We postulate that employees are more motivated to commit computer abuse when they possess low self-control and/or have high hacking self-efficacy. This model also suggests that target suitability as perceived by the potential offender is inevitably subject to the influence of the low self-control and hacking self-efficacy of the potential offender. The assessment of security guardianship by potential offenders is influenced by hacking self-efficacy and deterrence measures in an organization. Deterrence measures, such as the probability of being caught and the speed and severity of punishment, should help inform potential offenders about the level of security guardianship deployed in the organization. In addition, deterrence likely factors into potential offenders' assessment of target suitability because strong deterrence should make the target less suitable for MCA. These hypothesized relationships are shown in Figure 2 and elaborated in more detail in the following subsections.

3.1 Core Relationships in Routine Activity Theory

According to RAT, the occurrence of a crime is the result of a convergence of a motivated offender, a suitable target, and the absence of a capable guardian for the target in time and space (Cohen & Felson, 1979). All three factors are considered essential for a criminal act to occur. Drawing on RAT, we argue that employees are motivated to commit malicious computer abuse when they discover that digital assets in corporate computer systems are valuable, and they further develop an intention to commit MCA when digital assets are perceived to be useful, visible and accessible, and when the security protections for the assets are inadequate or even absent. In order to better operationalize the construct of "absence of capable guardianship," we refer to the "presence of capable guardianship" in this research. Guardianship, e.g., in the form of SETA programs, influences computer abuse intention "by simple presence to prevent crimes and by absence to make crime more likely" (Hollis-Peel et al., 2011). Therefore, following the logic of RAT, we propose that:

H1: An employee's offending motivation is positively related to the employee's intention to commit MCA in organizational settings.

H2: An employee's perceived target suitability of digital assets is positively related to the employee's intention to commit MCA in organizational settings.

H3: An employee's perceived presence of capable guardianship for the targeted digital assets is negatively related to the employee's intention to commit MCA in organizational settings.

3.2 Role of Moral Beliefs

Moral beliefs refer to an individual's beliefs about the normative appropriateness of a behavior, which are tied to one's innate moral standards (Wenzel, 2005). Personal moral beliefs prohibiting deviant behaviors can be considered as one type of self-regulatory mechanism that relies on one's intrinsic motivation to stay away from deviant behaviors. Those with high moral beliefs prohibiting a behavior will likely dismiss that behavior quickly or rule out that behavior as a possible choice of actions. Some studies have found a direct inhibitive impact of moral beliefs on employee computer abuse or ISP violations (D'Arcy & Lowry, 2019; D'Arcy & Devaraj, 2012; Li et al., 2014; Vance & Siponen, 2012). According to criminology literature, moral beliefs could also condition the assessment of costs and benefits expected from committing deviant acts (Paternoster & Simpson, 1996). More specifically, the cost-benefit assessment would play a less important role or even exert no effect in the existence of high moral beliefs prohibiting certain deviant acts. Moral beliefs have been suggested as a moderator capable of adjusting individual decision-making processes to perform deviant behaviors in many different contexts, such as corporate crimes (Paternoster & Simpson, 1996), tax evasion (Wenzel, 2005), and internet abuse in the workplace (Li et al., 2010). D'Arcy et al. (2009) included moral beliefs as a control variable for predicting information security misuses but confirmed its moderating role in a post hoc analysis.

Until now, the moderating role of personal moral beliefs has only received minimal attention in information security studies. To advance the understanding of the moderating role of moral beliefs and answer the recent call for more contextualized theory building (Hong et al., 2014; Johns, 2017), we incorporate moral beliefs as a contextual moderator instead of a direct antecedent, which helps us glean more context-sensitive insights into the relationship between core RAT constructs and MCA intentions.

In this study, we define moral beliefs as an employee's normative beliefs about whether it is right or wrong to commit computer abuse against organizations. Presumably, an employee would be less attracted to

computer abuse opportunities and less influenced by target suitability and security guardianship if the employee believed it was morally wrong to do engage in such abuse. Thus, we anticipate that the effects of offender motivation, a suitable target, and the absence of a capable guardian are conditioned on personal moral beliefs prohibiting MCA. Therefore,

H4a: An employee's moral beliefs prohibiting MCA negatively moderate the relationship between the employee's MCA motivation and MCA intention.

H4b: An employee's moral beliefs prohibiting MCA negatively moderate the relationship between the perceived target suitability and MCA intention.

H4c: An employee's moral beliefs prohibiting MCA positively moderate the relationship between the perceived presence of capable guardianship and MCA intention.

3.3 Role of Low Self-Control

Gottfredson and Hirschi (1990) articulate a general theory of crime centered on the concept of low self-control, also known as self-control theory. They define low self-control (LSC) as the tendency of individuals to act on impulse and with little regard for long-term consequences. This theory provides an important and unique view of the sources of crime and deviant behavior. LSC can explain various forms of crimes, from acts of physical violence to white-collar fraud, that individuals pursue their own interest in various social and organizational settings. Prior studies in information security suggest that one's MCA motivation could be influenced by this characteristic of low self-control (Hu et al., 2011). Those with LSC are shown to be more responsive to immediate gratification from crimes such as rewards, pleasures, and thrills (Wright, 2004). They were found to be more motivated to violate digital privacy to seek thrill and excitement (Morris & Higgins, 2008). Therefore, we anticipate that LSC fortifies one's motivation to commit MCA. At the same time, it has been suggested that LSC influences perceived characteristics of crime opportunities such as the accessibility and vulnerability of targets (Nagin & Paternoster, 1993). LSC, being associated with low ability to see the potential costs associated with criminal acts, has been found to significantly reduce the perceived costs of deviant acts (Vaughan et al., 2019). Such biased cost estimation may make the potential offender believe that a target is more suitable than it actually is. Hence, we posit that:

H5a: An employee's low self-control is positively related to the employee's MCA motivation.

H5b: An employee's low self-control is positively related to the employee's perceived target suitability of digital assets.

3.4 Role of Hacking Self-Efficacy

We use hacking self-efficacy to evaluate an individual's mental ability to commit MCA. Originating from social cognitive theory (Bandura, 1986), self-efficacy refers to an individual's beliefs about his or her capabilities to produce designated levels of performance. Self-efficacy is domain specific and can thus vary across activities requiring different skills and resources (Bandura, 1997). In the context of IS, computer self-efficacy is considered to be an important factor related to the acquisition of computing skills and adaptation to new information technology (Compeau & Higgins, 1995). Previous studies on self-efficacy have mostly focused on the context of conventional tasks such as job performance, and have devoted little attention to antisocial behaviors such as crime (Brezina & Topalli, 2012). It is not clear how crime-related self-efficacy would influence offenders' decision-making processes.

To fill this research gap, we introduce the construct of hacking self-efficacy, which is specific to the MCA context, and examine it as the antecedent for core RAT constructs driving MCA decisions. Following Wood and Bandura (1989), we define hacking self-efficacy as the belief in one's ability to mobilize the motivation, cognitive resources, and courses of action needed to gain access to desired digital assets. The emphasis is on whether an individual employee believes she or he has the required knowledge, skill, or ability to commit MCA in the organization. Such efficacy beliefs have caused many offenders of physical crimes to express pride in their ability to exploit crime opportunities, such as compromising locking devices and alarms (Brezina & Topalli, 2012).

In the context of MCA, hacking self-efficacy is expected to influence employees' assessment of crime opportunities in terms of suitability of the desired digital target and effectiveness of security guardianship in organizations. Therefore, we argue that heightened hacking self-efficacy may cause an employee to believe that he or she has the ability to overcome technical challenges and to perceive that little effort is needed to commit MCA in the organization. We posit that employees with a high level of hacking self-efficacy will be more likely to activate their MCA motivations and perceive digital assets to be relatively easy to compromise, thus judging them to be suitable potential targets. Along the same line, heightened hacking ability may cause motivated offenders to perceive relatively weak levels of security guardianship of the digital asset targets. Thus, we hypothesize:

H6a: An employee's hacking self-efficacy is positively related to the employee's MCA motivation.

H6b: An employee's hacking self-efficacy is positively related to the perceived target suitability of digital assets.

H6c: An employee's hacking self-efficacy is negatively related to the perceived presence of capable guardianship for digital assets.

3.5 Role of Deterrence

Deterrence measures such as formal sanctions are enacted by organizations or law enforcement agencies and have been widely examined as a mechanism for deterring criminal behaviors in various contexts such as corporate crimes (Paternoster & Simpson, 1996), information systems misuse (D'Arcy et al., 2009), and information security (Hu et al., 2011). Deterrence focuses on punishments such as demotion, job termination, or prosecution, which would increase the cost of criminal behaviors. The effect of deterrence has been mostly examined through individuals' perceptions about detection probability and sanction severity, as well as sanction celerity or the speed of punishment (Antia et al., 2006; Howe & Brandau, 1988; Howe & Loftus, 1996; Simpson & Koper, 1992). All three dimensions of deterrence have received some support in reducing criminal behaviors. For example, detection probability has been negatively related to software piracy (Peace, Galletta, & Thong, 2003) and the abuse of internet access in the workplace (Li et al., 2010). A high level of perceived sanction severity has been found to reduce the misuse of IS assets (D'Arcy et al., 2009) and increase compliance with security policies (Herath & Rao, 2009). However, Hu et al. (2011) show that the effectiveness of deterrence in organizational information security settings is insignificant based on a rational choice behavioral framework.

According to RAT, motivated offenders assess the degree of guardianship or form awareness of various security countermeasures before engaging in a criminal act. From an individual's perspective, those motivated offenders would estimate the probability of their being caught by the organization (i.e., perceived detection probability). Also, they would estimate the severity and the speed of punishments should they get caught (i.e., perceived sanction severity and celerity). As these deterrence dimensions constitute threats to human assets (Johnson et al., 2015), they should help inform potential offenders about the level of security guardianship deployed in the organization. A heightened focus on deterrence should increase employees' awareness of security guardianships. In an organization with strong and clear deterrence mechanisms, employees are more likely to perceive high levels of security guardianship and view digital assets to be more difficult to compromise. Therefore, we propose:

H7a: An employee's perceived deterrence against MCA is negatively related to the employee's perceived target suitability of digital assets.

H7b: An employee's perceived deterrence against MCA is positively related to the employee's perceived presence of capable guardianship of digital assets.

3.6 Control Variables

While the three elements in the RAT model may explain the primary antecedents of MCA intentions, other significant factors should not be ignored. For example, employment status (part-time vs. full-time) may play a role in influencing MCA intentions because of factors related to time, experience, and exposure to digital assets. Different from the context of volitional noncompliance of organizational security policies, IS security experience may increase an insider's intention to commit MCA as well because employees who know a great deal about the security technology and practices of the organization may have more MCA opportunities. In addition, age and gender have often been included to explain IS misuses (Leonard & Cronan, 2001; Leonard, Cronan, & Kreie, 2004). For example, men have been shown to have higher intentions to misuse organizational IS resources than women (Leonard & Cronan, 2001). Also, younger people were found to be more likely to engage in deviant computer usage behaviors than older people (Gattiker & Kelley, 1999). Toward that end, we include four control variables for an employee's intention to commit MCA at the workplace, based on the extant literature: age, sex, IS security experience, and employment status (D'Arcy et al., 2009; Hu et al., 2011; Siponen & Vance, 2010).

4 Research Methodology

4.1 Measurement Instrument

To maximize measurement reliability and validity, we adopted appropriate published scales to measure most of the latent constructs with slight rewording to reflect our research context. The research model includes both first-order and second-order constructs (Table 2). Instruments for measuring lack of harmfulness, perceived accessibility, perceived visibility, and perceived usability were developed for this study. In particular, we created two items using words "harmful" and "damaging" and reverse coding to measure the lack of harmfulness of each MCA scenario. To measure perceived accessibility, we created three items with similar wording to capture how easily the confidential data could be accessed.

Table 2. Operationalization and Sources of Latent Constructs.

Second-order construct	Second-order formative scale justification	First-order construct	Sources
		Moral beliefs (MRB)	Hu et al. (2011)
Low self-control (LSC)	The four first-order factors are not interchangeable and could vary independently. For example, risk seeking trait may or may not co-exist with temper.	Impulsivity (IMP)	Grasmick et al. (1993)
		Risk seeking (RSK)	
		Self-centeredness (SCT)	
		Temper (TMP)	
		Hacking self-efficacy (HSE)	Gist & Mitchell (1987)
Deterrence (DET)	The three first-order factors represent different approaches for enforcing deterrence. They are not interchangeable and have been found to exert different impacts (Li et al., 2010).	Perceived certainty (CER)	Antia et al. (2006)
		Perceived severity (SVR)	
		Perceived celerity (CEL)	
Offender motivation (MOV)	The three first-order factors represent different motivators that could drive MCA independently. They are not interchangeable.	Perceived extrinsic value (PEV)	Paternoster & Simpson (1996)
		Perceived intrinsic value (PIV)	Piquero & Tibbetts (1996)
		Lack of harmfulness (LHM)	Developed for this study
Target suitability (STG)	The three first-order factors represent different criteria for assessing target suitability. They are not interchangeable and do not change in the same direction. For example, a visible digital asset may not be accessible and directly usable.	Perceived accessibility (PAC)	Developed for this study
		Perceived visibility (PVS)	
		Perceived inertia (Usability-PUS)	
Capable guardianship (CGS)	The three first-order factors represent different security measures that are not interchangeable and co-vary. For example, a company with strong SETA program may not have strong monitoring.	SETA	D'Arcy et al. (2009)
		Security policies (POL)	
		Computer monitoring (MOR)	
		Intention to commit MCA (INT)	

Perceived visibility consists of three items measuring the extent to which a subject would know where the data are stored if the subject were in the same situation described in the MCA scenario. Perceived usability consists of three items reflecting the extent to which the confidential data could be used without difficulty. The content validity and wording of these self-developed scales were checked by four domain experts before they were further validated in the pilot study using student subjects and the final study using the industrial panel operated by Qualtrics.

We introduced five second-order factors into our research model. The primary purpose of using second-order constructs is to create a more parsimonious model that focuses the attention on the central arguments of RAT. All first-order constructs were operationalized as reflective constructs. Following the suggestions in Confetelli and Bassellier (2009) and MacKenzie, Podsakoff, and Podsakoff (2011), the five second-order constructs were implemented as formative scales. The major distinguishing features of a formative scale are that the formative indicators are not interchangeable and do not necessarily increase or decrease at the same time, as would be the case for reflective measures. These distinguishing features apply to all five formative scales in this study. Table 2 summarizes the construct measures, their sources, and the justification for formative second-order scales. All constructs were measured using 7-point Likert scales from 1 (*strongly disagree*) to 7 (*strongly agree*) (see Appendix B).

4.2 Data Collection

As noted by Holsapple et al. (2008), empirical studies in this context can be challenging because the nature of the underlying activity is illegal and may, therefore, cause significant issues in sample selection and response bias and validity. Given the nature of this study, it is highly unlikely that reliable data can be collected via voluntarily self-reported responses to field survey questionnaires with regard to the actual criminal or deviant behavior of individual employees in organizational settings. Thus, we adopted a scenario-based cross-sectional survey strategy for data collection.

In criminology research, crime scenario-based surveys are considered to be a more reliable and realistic approach than self-reported surveys, which ask whether subjects have actually committed crimes or illicit behavior. Criminology studies have used scenarios involving various criminal activities, such as bribery (Paternoster & Simpson, 1996), theft, and sexual assault (Nagin & Paternoster, 1993), and have delivered the crime scenarios to subjects that, as a majority, report no prior criminal offenses. Recently, IS security studies, such as those by D'Arcy et al. (2009), Siponen and Vance (2010), Hu et al. (2011, 2015), Han et al. (2015), and Vance, Lowry, and Eggett (2015), have employed this method to overcome the practical data collection challenges involved in studying criminal or deviant behavior in organizational settings, such as the difficulty of collecting actual behavior data or collecting data from multiple sources (e.g., from both managers and employees). This method is particularly useful for such studies because malicious compromise of digital assets is conducted secretly, making it less visible than other types of deviant acts. Further, due to the sensitive nature of MCA perpetrated by internal employees, organizations are typically reluctant to report such MCA incidents or share them with researchers (Crosslet et al., 2013; D'Arcy, 2014). Self-reporting of actual MCA behaviors by employees is also problematic because employees may be unwilling to admit their own malicious acts because of social desirability concerns. To a certain extent, the scenario-based approach reduces the impact of social desirability concerns.

In line with the practice of these prior studies, three fictitious situational scenarios were created for this study based on published literature and our own experience to reflect the typical types of MCA, including stealing client data to sell to a noncompetitor, stealing new product design to sell to a competitor, and stealing financial data to sell to an investment firm before the scheduled public release (see Appendix E for details). We selected these three scenarios in order to increase the generalizability of our findings to typical MCA scenarios and to induce variations in the antecedents of MCA. The data breaches in these scenarios involve different types of confidential data and may inflict different degrees of harm to a firm. For example, selling product design data to a competitor may be considered more harmful than disclosing client information to a noncompeting firm. We also explicitly included one question to test the perceived realism of each scenario in the survey. The percent of subjects who *somewhat agreed* to *strongly agreed* that the scenario was realistic in the final data collection was 64%, 54%, and 60% for client data, product design, and financial data scenarios, respectively. Therefore, we determined that the extent of realism of the three scenarios is acceptable to warrant their inclusion in the data analysis (see Appendix B for the text of the measurement instrument).

Prior to the final data collection, a pilot study was administered to 102 undergraduate and graduate students of three major universities across the US in order to evaluate the content validity and improve the clarity of the survey instruments. The final survey was refined based on the results of the pilot study. The survey was then distributed in an online format to the industry panel consisting of employees from a wide range of organizations and industries using the Qualtrics online survey platform. The Qualtrics participants were profiled based on hundreds of attributes (McKinney, Yoon & Zahedi, 2002). For our study, Qualtrics randomly contacted those who were organizational employees. Qualtrics also checked IP addresses and used a sophisticated digital fingerprinting technology to ensure that no two responses were from the same subject.

Three question blocks were used as containers for scenario-specific questions, using one block for each scenario. One of these three blocks was randomly assigned to each respondent so that each respondent answered questions based on one scenario only. The scenario-specific questions included questions about perceived values, moral beliefs, target suitability, and intention to commit MCA if the respondent were in the same situation as the character described in the fictitious scenario. Besides these scenario-specific questions, respondents were then required to answer questions about demographics and questions measuring other variables. Despite the differences in scenarios, the sequence of questions was the same for all respondents.

The identity of all survey respondents was anonymous to the researchers. In the final data collection lasting about two weeks, 660 panel members attempted to take the survey and 360 of them completed the questionnaire. After further dropping eight responses that gave the same answer to almost all questions, we received a total of 352 usable responses that were used for data analysis. Among the 352 usable responses, the number of subjects in each information security scenario was 116, 128, and 108 for stealing client data, product design, and financial data, respectively.

5 Data Analysis

SmartPLS, a variance-based structural equation modeling (SEM) tool, was employed to analyze the measurement invariance, reliability, and validity of our measurement model and test the research hypotheses. We chose to use PLS primarily because PLS is more amenable for handling complex and exploratory research models with both reflective and formative constructs than covariance-based SEM techniques such as LISREL (Chin, 1998). In addition, PLS uses the bootstrap method to determine the statistical significance of path coefficients, which imposes less strict requirements on residual distributions of the

dataset than covariance-based SEM techniques (Chin, Marcolin, & Newsted, 2003).

5.1 Demographic Characteristics

Table 3 summarizes the demographic information of survey respondents. Approximately 53% of the survey respondents are male and 47% were female. About 61% of the respondents were between 25-44 years of age, and 98% reported using the internet for over 5 years. The respondents reported different types of job positions, ranging from managerial to technical positions. Questions about employing firm size also revealed a good mix of small, medium, and large firms. These demographic characteristics suggest that our sample is quite heterogeneous, which helps increase the external validity of our study.

Table 3. Demographic Information of Survey Respondents

Gender	Age (Years)	Internet Exp. (Years)	Job Position	Employment Status	Firm Size (# Employees)
Male: 52.6%	<24: 16.5%	<5: 1.7%	Executive: 8.2%	Full-time: 78.4%	1-100: 35.0%
Female: 47.4%	25-34: 37.8%	6-10: 18.2%	Manager/Supervisor: 12.8%	Part-time: 21.6%	101-250: 15.4%
	35-44: 22.7%	11-15: 39.5%	IT Professional: 17.3%		251-500: 19.0%
	45-55: 15.6%	16-20: 30.9%	Admin Staff: 24.2%		501-1,000: 10.2%
	55+: 7.4%	>20: 9.7%	Business/Professional 15.3%		1,001-5,000: 11.9%
			Technical/Engineering: 6.0%		5000+: 8.5%
			Other 16.2%		

5.2 Measurement Model

All variance-based SEM tools model latent constructs as composites, which demands the test of measurement invariance when the dataset consists of multiple groups. Since we collected data using three different scenarios, measurement invariance is a necessary requirement for conducting pooled data analysis. We performed the MICOM procedure proposed by Henseler, Ringle, and Sarstedt (2016) to test measurement invariance and applied the same algorithm settings across all three scenarios. Partial measurement invariance is established when the original composite correlations are greater than or equal to the 5% quantile. As shown in Appendix C1, all latent constructs have partial measurement invariance. However, not all constructs have equal means across the scenarios, suggesting the absence of full measurement invariance. Thus, we could not perform an analysis on the pooled data across the three scenarios. We analyzed the three scenarios separately.

Following typical practice in the literature, we deployed different procedures and criteria to test the measurement quality of reflective and formative constructs. For formative constructs, we assessed their measurement quality following the suggestions by MacKenzie, Podsakoff, and Jarvis (2005) and Diamantopoulos and Winklhofer (2001). We first examined the significance level of path weights of the five formative constructs. Lack of harmfulness has nonsignificant path weights in scenarios involving product design and financial data (Appendix C2). As suggested by prior studies, it may be necessary to retain nonsignificant indicators in a formative construct to ensure the completeness of its content domain (Mathieson, Peacock, & Chin, 2001). To maintain the content domain of offender motivation, we kept lack of harmfulness in the subsequent data analysis. We computed the variance inflation factor (VIF) to assess multicollinearity among first-order factors in each formative second-order construct. VIF values were all found to be below the threshold of 10 for excessive multicollinearity suggested by Diamantopoulos and Winklhofer (2001). Therefore, we conclude that multicollinearity is not a concern here. Overall, the instruments for measuring these five formative second-order constructs were found to have reasonable measurement quality.

Further comparing the weights of the first-order latent constructs reveals major underlying drivers for each second-order construct. For low self-control, impulsivity has the largest weight in the client scenario, whereas self-centeredness has the largest weight in the other two scenarios. For deterrence, perceived certainty of being caught is the most important subdimension for client and design scenarios while perceived severity of punishment is the dominant dimension in the financial data scenario. For offender motivation, perceived intrinsic value has the largest weights across all scenarios, followed by perceived extrinsic value. Lack of harmfulness is the least important dimension in terms of offender motivation and has a significant path weight only in the client scenario. With respect to target suitability, perceived accessibility has the largest weight in the client scenario, and perceived usability has the largest weight in the design and finance scenarios. Among the three

subdimensions of capable guardianship, computer monitoring has the highest weight across all scenarios, suggesting the importance of computer monitoring for deterrence.

We then assessed the measurement quality of reflective scales assessed based on their reliability, convergent validity, and discriminant validity. Reliability is supported if composite reliability (CR) is above 0.7 and average variance extracted (AVE) is above 0.5 (Bagozzi and Yi, 1988). As shown in Appendix C2, for all reflective scales, CR and AVE are higher than the recommended threshold for reliability. Convergent validity is suggested when factor loadings are significant and equal to 0.6 or higher (Bagozzi & Yi, 1988; Gefen & Straub, 2005). All indicators except the third item measuring perceived certainty (CER_3) were found to load significantly on their respective latent constructs and have loadings above 0.6. Therefore, we removed CER_3 and reran the data analysis. The following data analysis results are based on the remaining items without CER_3. All these reflective scales display sound convergent validity. We then tested the discriminant validity in the correlation matrix (Appendix C4). The square root of AVE of each construct should be higher than the interconstruct correlations (Fornell & Larcker, 1981). As shown in Appendix C4, all reflective constructs exhibit good discriminant validity.

Akin to other survey-based cross-sectional studies, our study may be susceptible to common method variance (CMV) bias. Following Lindell and Whitney's (2001) recommendation, we applied the partial correlation procedure based on the marker-variable technique to gauge the magnitude of CMV and, at the same time, evaluate its impact on the correlation among latent constructs. In particular, this procedure requires the selection of the second-smallest positive correlation among the manifest variables as a more conservative estimate of CMV (i.e., rm). The second smallest positive correlation was found to be 0.001. Therefore, we used 0.001 to compute CMV-adjusted correlations among latent constructs by partialing out rm from the original correlations. The CMV-adjusted correlations were only slightly different from the original correlations, with differences less than or equal to 0.002. The significance levels for all correlations among latent constructs in Appendix C4 remain the same. Considering the small difference in *t*-value, we conclude that CMV is not a problem for our study.

5.3 Hypothesis Testing

Figure 3 and Table 4 summarize the results of hypothesis testing using SmartPLS. We performed bootstrapping of 5,000 samples to compute *t*-statistics of all paths in the research model. Standardized path coefficients are given on each path. The R^2 values reflect the predictive power of the model. The model explains 66.7% to 71.6% of the variance in MCA intention, 39.9% to 51.6% of the variance in offender motivation, 23.4% to 30.3% of the variance in target suitability, and 53.8% to 65.8% of the variance in capable guardianship. This indicates an overall good fit of the model with the data.

Among the four control variables, we found that men have higher MCA intentions than women in the selling design data scenario. The other variables are statistically nonsignificant. With respect to the explicitly hypothesized core RAT relationships, offender motivation was found to have the largest path coefficient and is highly significant across all three scenarios (H1, $p < 0.001$). The next important core RAT construct is target suitability, which is significant in the client and finance scenarios (H2, $p < 0.05$). Capable guardianship was not found to be significant at the 0.05 level in the client and financial data scenarios. Counterintuitively, capable guardianship exhibits significant positive influence over MCA intention in the design scenario.

Next, we analyzed the moderation effect of moral beliefs on the core RAT relationships. We found that H4a is significant at the $p < 0.05$ level in the finance scenario with an effect size (f2)[1] of 0.04, suggesting a small effect size (Cohen, 1988). H4a was found to be significant in the finance scenario but not the other two scenarios. H4b and H4c are not significant across all three scenarios. Despite the significance of H4a in the finance scenario, its sign is positive, which contradicts our hypothesis. The interaction pattern of H4a is shown in Figure 4. The dashed line (strong moral beliefs) is still below the solid line (weak moral beliefs) but the two lines merge at the position of high motivation, suggesting that the effect of moral beliefs prohibiting MCA exists for employees with low motivation but is negligible for those with high motivation. Clearly, high moral beliefs fail to rule out MCA as a possible choice of actions among highly motivated offenders. We found that those with high moral beliefs could still be strongly motivated to commit MCA. Therefore, the effect of moral beliefs prohibiting MCA is influenced or even dominated by offender motivation. This finding is consistent with Naso's (2012) description of white-collar criminals: in contrast to antisocial offenders, white-collar criminals are "excessively self-centered … and willingly placing their personal goals ahead of moral standards" (p. 243). Such offenders may commit crimes when their financial security or lifestyle is threatened, especially when the probability of being detected is low.

[1] $f^2 = [R^2 \text{ (interaction model)} - R^2 \text{ (main effects model)}] / [1 - R^2 \text{ (main effects model)}]$.

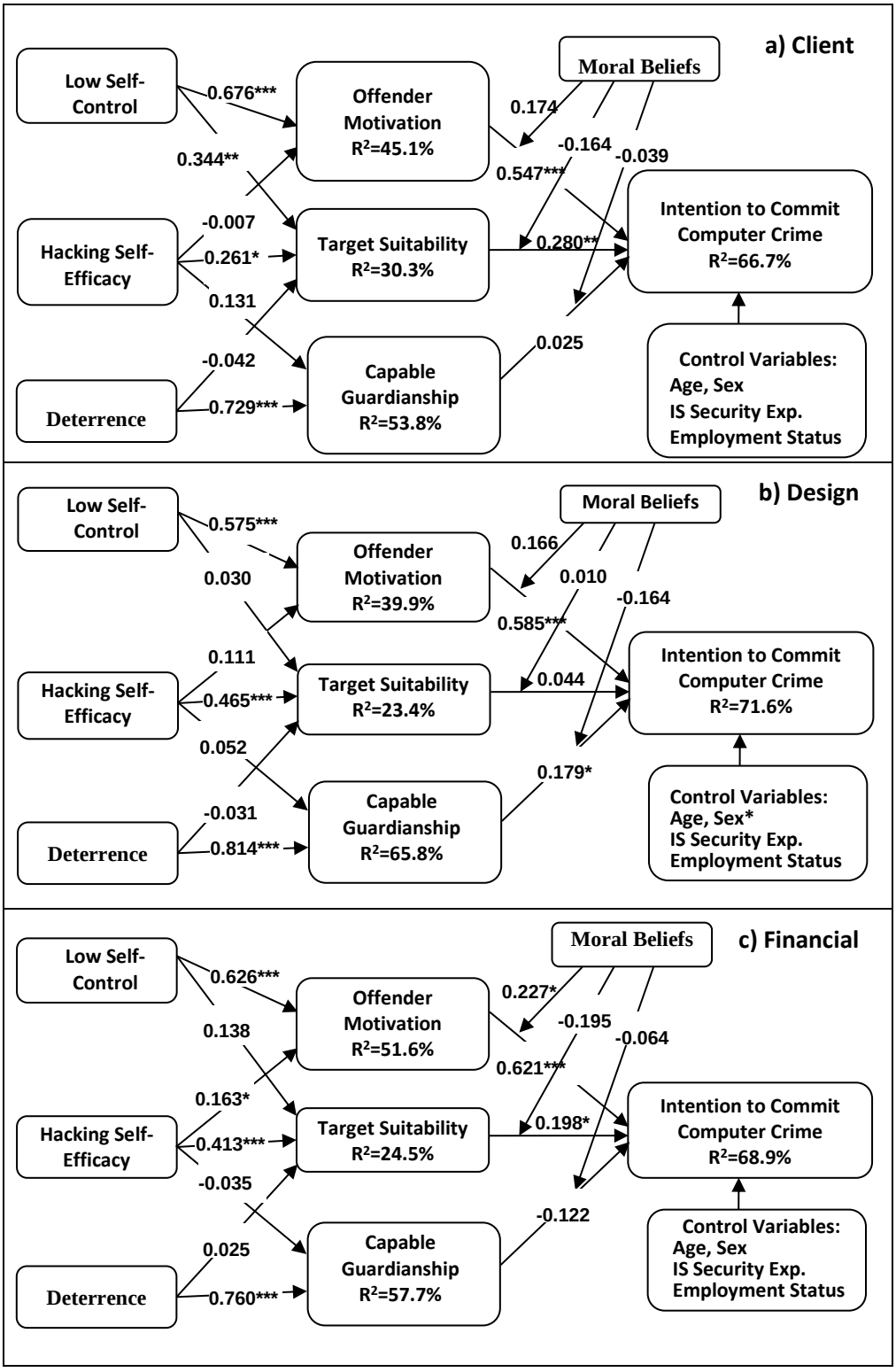

Figure 3. Results of Testing Hypotheses in (a) Client, (b) Design, and (c) Financial scenarios (*$p < 0.05$, **$p < 0.01$, ***$p < 0.001$)

Table 4. Results of the Structural Model Assessment

Path		Path Coefficient (p-value)		
		Client	Design	Financial
H1: Offender motivation → Intention		0.547 (**0.000**)	0.585 (**0.000**)	0.621 (**0.000**)
H2: Target suitability → Intention		0.280 (**0.002**)	0.044 (0.531)	0.198 (**0.029**)
H3: Capable guard. → Intention		0.025 (0.718)	**0.179* (0.012)**	-0.122 (0.095)
H4a: Moral beliefs*Offender motivation →Intention		0.174 (0.063)	0.166 (0.113)	0.227 (**0.041**)
H4b: Moral beliefs*Target suitability → Intention		-0.164 (0.065)	0.010 (0.907)	-0.195 (0.102)
H4c: Moral beliefs*Capable guard. → Intention		-0.039 (0.527)	-0.164 (0.053)	-0.064 (0.439)
H5a: Low self-control → Offender motivation		0.676 (**0.000**)	0.575 (**0.000**)	0.626 (**0.000**)
H5b: Low self-control → Suitable target		0.344 (**0.004**)	0.030 (0.762)	0.138 (0.184)
H6a: Hacking self-efficacy → Offender motivation		-0.007 (0.949)	0.111 (0.254)	0.163 (**0.031**)
H6b: Hacking self-efficacy → Target suitability		0.261 (**0.014**)	0.465 (**0.000**)	0.413 (**0.000**)
H6c: Hacking self-efficacy → Capable guard.		0.131 (0.053)	0.052 (0.325)	-0.035 (0.621)
H7a: Deterrence → Target suitability		-0.042 (0.622)	-0.031 (0.724)	0.025 (0.830)
H7b: Deterrence → Capable guard.		0.729 (**0.000**)	0.814 (**0.000**)	0.760 (**0.000**)
Age → Intention		0.008 (0.908)	-0.005 (0.926)	-0.051 (0.523)
Gender → Intention		-0.063 (0.359)	0.109 (**0.026**)	-0.073 (0.213)
IS Security Exp. → Intention		0.109 (0.177)	0.070 (0.231)	0.041 (0.510)
Employment → Intention		-0.059 (0.407)	-0.079 (0.231)	-0.044 (0.502)
R^2	Offender motivation	0.451	0.399	0.516
	Target suitability	0.303	0.234	0.245
	Capable guard.	0.538	0.658	0.577
	Intention	0.667	0.716	0.689

Note: Coefficient with unexpected signs. Note: Bolded p-values are significant (< 0.05).

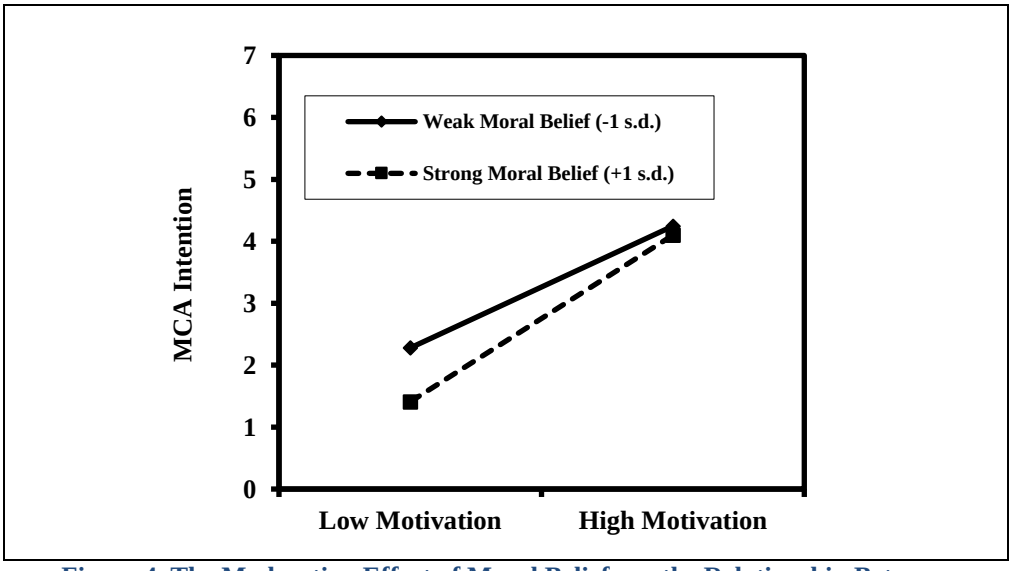

Figure 4. The Moderation Effect of Moral Beliefs on the Relationship Between Offender Motivation and MCA Intention in the Financial Data Scenario.

In addition, we found that low self-control increases offenders' motivation in all three scenarios, whereas low self-control increases target suitability only in the client scenario. Hacking self-efficacy was found to increase offenders' motivation only in the finance scenario but consistently exerted a positive impact on target suitability. Deterrence significantly increased capable guardianship but had no influence on target suitability. The implications and potential explanations of differences in hypotheses across the scenarios are provided in the discussion section.

To summarize, some of the key findings from hypothesis testing are:

- Among the three core constructs of RAT, offender motivation is the dominant driver for MCA across all scenarios. Target suitability plays a less important role and is significant in only two of the scenarios. Capable guardianship has no significant effect in reducing MCA intention.
- Moral beliefs exhibit a small moderation effect in the financial scenario only and we found that its effect could be overridden by high offender motivation.
- With respect to the antecedents of core RAT concepts, low self-control is the major driver for offender motivation. Hacking self-efficacy has a consistent and strong impact on the assessment of target suitability. Deterrence is the dominant factor influencing capable guardianship.

5.4 Robustness Testing and Alternative Models

In order to check the direct effects of the exogenous variables without the mediation of the RAT core constructs, we tested an alternative model consisting of low self-control, hacking self-efficacy, deterrence, moral belief, and control variables only. The model explained only 46.7% to 59.7% of the variance in MCA intention, compared with 67% to 72% in the full model. Low self-control and moral beliefs were significant at 0.05 level while hacking self-efficacy and deterrence had no significant direct impact across all scenarios. Internet security experience was significant only in the client scenario. This result highlights the critical roles of the RAT core constructs in explaining MCA for our data sample. We further compared the R^2 of our full model for explaining MCA intention with the R^2s of other models seeking to explain IS misuse intention in prior studies, such as D'Arcy et al (2009) ($R^2 = 0.30$), Siponen and Vance (2010) ($R^2 = 0.47$), and Hu et al. (2011) ($R^2 = 0.34$). The full model of our study based on RAT has the highest R^2 or predictive power of any of these models, further supporting the validity and power of RAT in explaining MCA.

Our results show that the RAT core constructs play different mediating roles for the three antecedents. To further explore this, we applied the Shrout and Bolger's (2002) bootstrapping method to test the mediation effect, as it has stronger statistical power than the traditional methods proposed by Baron and Kenny (1986) and Sobel (1982). To test mediation, we evaluated three paths: (1) the path from an antecedent, such as low self-control, to its mediating variables in RAT core constructs (Path A); (2) the path from the mediating variable to MCA intention (Path B); and (3) the direct path from the antecedent to MCA intention (Path C, or Path C' when tested simultaneously with the indirect paths involving Paths A and B). Five thousand bootstrap samples were generated in SmartPLS. The indirect effects were computed for each sample by multiplying the coefficients of Paths A and B. The 95% bootstrap percentile intervals could then be constructed for both indirect and direct effects (i.e., coefficient of Path C').

The existence of indirect and direct effects is tested by checking whether the interval contains zero. If the interval does not contain zero, it means that the effect is nonzero. Full mediation is suggested when the direct effect is zero but the indirect effect is nonzero. Partial mediation occurs when both the direct and indirect effects are nonzero. Table 5 shows the mediation testing results. Overall, the RAT core constructs mediate some of the effects of low self-control while fully mediating the effect of hacking self-efficacy. Deterrence basically has a null effect on MCA intention.

Considering the inconsistent impact of suitable target and capable guardianship across scenarios, we further performed a conjoint analysis (CA) of RAT core constructs on MCA intention to check the robustness of our findings. CA is a robust tool with high validity and reliability for investigating individual preferences, attitudes, and behaviors (Luo, Warkentin, & Li, 2015). CA is also flexible, which is applicable not only to product attributes in marketing literature but also to IS research investigating perceptions such as perceived security (Luo et al., 2015). In the conjoint analysis of this study, the dependent variable is the MCA intention. The independent variables are three dummy- coded attributes: offender motivation (2 levels: low, high), target suitability (2 levels: low, high), and capable guardianship (2 levels: low, high). For these three variables, a low level refers to values less than or equal to the mean, whereas a high level refers to values above the mean. Since the dependent variable has an interval scale in nature, ordinary least square (OLS) multiple regression was used to derive the part-worth utilities of all attribute levels and the statistical significance and relative importance (RI) of attributes. The relative importance of attribute *i* was computed using the following equation:

$$\text{RI}i = \frac{attribute\_utility\_range_i}{\sum_{i=1}^{n} attribute\_utility\_range_i}$$

The results of the conjoint analysis are shown in Table 6. The significance level of the RAT core constructs is consistent across the three scenarios. Offender motivation and target suitability are statistically significant (p-value < 0.05) while capable guardianship is not (p-value > 0.05). The pattern of the relative importance also stays the same across scenarios, with offender motivation being the most important factor and target suitability as the second- most important factor. Overall, the findings from the conjoint analysis are robust across scenarios and support the dominant roles of offender motivation and suitable target identified in the PLS-SEM analysis.

Table 5. Summary of Mediation Testing Results

Scenario	Antecedent	Mediator	Indirect effect (AB)			Direct effect (C')			Mediation type
			2.5% lower bound	97.5% upper bound	Has zero?	2.5% lower bound	97.5% upper bound	Has zero?	
Client	Low self-control	Offender motivation	0.081	0.439	No	0.117	0.537	No	Partial med.
		Target suitability	0.028	0.212	No				Partial med.
	Hack self-efficacy	Offender motivation	-0.082	0.079	Yes	-0.305	0.014	Yes	No effect
		Target suitability	0.014	0.178	No				Full med.
		Capable guardianship	-0.055	0.027	Yes				No effect
	Deterrrence	Target suitability	-0.078	0.040	Yes	-0.143	0.356	Yes	No effect
		Capable guard.	-0.204	0.164	Yes				No effect
Design	Low self-control	Offender motivation	0.208	0.516	No	-0.13	0.211	No	Partial med.
		Target suitability	-0.02	0.029	Yes				Only direct
	Hack self-efficacy	Offender motivation	-0.054	0.180	Yes	-0.229	0.059	Yes	No effect
		Target suitability	-0.028	0.117	Yes				No effect
		Capable guardianship	-0.011	0.030	Yes				No effect
	Deterrrence	Target suitability	-0.026	0.018	Yes	-0.146	0.305	Yes	No effect
		Capable guardianship	-0.115	0.264	Yes				No effect
Finance	Low self-control	Offender motivation	0.068	0.492	No	0.04	0.519	No	Partial med.
		Target suitability	-0.011	0.092	Yes				Only direct
	Hack self-efficacy	Offender motivation	0.004	0.158	No	-0.215	0.126	Yes	Full med.
		Target suitability	0.006	0.170	No				Full med.
		Capable guardianship	-0.015	0.036	Yes				No effect
	Deterrrence	Target suitability	-0.05	0.059	Yes	-0.177	0.245	Yes	No effect
		Capable guardianship	-0.252	0.081	Yes				No effect

Table 6. Utilities, Statistical Significance and Relative Importance of Attributes

Scenario	Attribute	Utility	p-value	RI	Ranking
Client	Offender motivation	Low (-2.182), High (2.182)	< 0.001	72.3%	1
	Target suitability	Low (-0.797), High (0.797)	< 0.01	26.4%	2
	Capable guardianship	Low (-0.037), High (0.037)	> 0.05	1.2%	3
Design	Offender motivation	Low (-2.963), High (2.963)	< 0.001	79.0%	1
	Target suitability	Low (-0.535), High (0.535)	< 0.05	14.3%	2
	Capable guardianship	Low (-0.252), High (0.252)	> 0.05	6.7%	3
Financial	Offender motivation	Low (-2.230), High (2.230)	< 0.001	65.7%	1
	Target suitability	Low (-0.747), High (0.747)	< 0.01	22.0%	2
	Capable guardianship	Low (0.417), High (-0.417)	> 0.05	12.3%	3

To summarize, some of the key findings from the robustness tests and the comparison with alternative models are:

- Our model built on RAT core constructs is stronger than the alternative research models for explaining MCA intention.
- The RAT core constructs partially mediate the effect of low self-control while fully mediating the effect of hacking self-efficacy on MCA intention.
- The RAT core constructs of offender motivation and target suitability are the dominant and most robust factors explaining MAC intention.

5.5 Post Hoc Comparison of MCA Scenarios

Despite the overall robustness of the RAT core constructs, we note the variation of the path modeling results across the three scenarios, suggesting the important influence of the MCA context. To increase the richness and practical relevance of our research findings, we further compared the means of all latent constructs using ANOVA analysis with Bonferroni tests and performed multigroup analysis (MGA) in SmartPLS to compare the difference in significant paths across the three scenarios.

We found that three latent variables, i.e., moral beliefs, perceived extrinsic value, and intention, have significant differences in their means across scenarios in ANOVA. Interestingly, the research participants in the client scenario were found to have significantly lower moral beliefs prohibiting MCA than those in the design scenario and significantly higher intentions to commit MCA than in the other two scenarios. Low moral beliefs seem to be an important factor accounting for higher intentions to steal and sell client data. As expected, the research participants in the client scenario perceived less extrinsic monetary value than those in the financial data scenario. For MGA results reported in Appendix D, we focused on identifying significantly different path coefficients involving at least one significant path at the 0.05 level and found three such paths. The paths between target suitability and intention and between low self-control and target suitability in the client scenario have significantly higher coefficients than those in the product design scenario. The coefficients for the path from capable guardian to intention also exhibit significant differences between the design and finance scenarios with the former being positive and significant and the latter being nonsignificant. We further explore these significantly different path coefficients in detail in the discussion section.

To summarize, some of the key findings from comparing the three MCA scenarios are:

- The research participants appear to factor the type of digital target into their judgment of target suitability, personal moral beliefs prohibiting MCA, and their resulting MCA intentions.
- The research participants in the client scenario appear to perceive lower monetary value, have lower moral beliefs prohibiting MCA, and higher intentions to commit MCA.
- The links between low self-control and target suitability and between target suitability and MCA intentions are stronger in the client scenario than in the product design scenario.
- Capable guardianship exhibits unexpected and unstable impacts on MCA intentions in different scenarios.

6 Discussion

Among the three core RAT constructs, we confirmed that offender motivation and target suitability are the primary drivers of employees' intention to commit MCA in organizational settings. Employees are more likely to commit MCA when they do not think their acts are harmful and when they perceive digital assets to be valuable and suitable as targets (i.e., accessible, visible, and usable). Despite support for the effects of offender motivation and target suitability, capable guardianship was found to have a null effect in the client and financial data scenarios. This null effect of capable guardianship on reducing MCA may not be surprising given the strong relationship between deterrence and capable guardianship (H7b, $p < 0.001$), making most of the variance of capable guardianship attributable to deterrence. This is also consistent with the findings of Hu et al. (2011), which are based on a completely different theoretical model and dataset. Our findings, in conjunction with those of Hu et al. (2011), highlight at least one unique aspect of the MCA offenders as compared with those committing conventional crimes: neither deterrence nor guardianship are strong mechanisms for protecting digital assets from intentional and malicious insider attacks.

At the same time, we found an unexpected significant positive effect of capable guardianship on MCA intentions in the product design scenario. An abnormal result such as this signals the potential effect of context (Johns, 2017), which prompted us to further examine the details of the situational scenarios presented in Appendix E. We submit that this unexpected positive impact may be related to how research participants interpret acceptable and authorized use of computer resources when answering survey questions measuring capable guardianship. The surrogate character in the product design scenario, i.e., Daniel, may have been perceived as having authorized access to the confidential design data because he is a senior engineer

(see Appendix E). Therefore, research participants assigned to the design scenario may not have considered the capable guardianship measures, i.e., security policy, SETA, and monitoring, to even be applicable to the behavior of Daniel, who supposedly sold the design data to a competitor. In a future study, it would be interesting to explore the impact of capable guardianship on insiders with authorized access after employees receive security training customized to the context of their specific job roles.

Our results regarding the antecedents of the three core RAT constructs are mostly consistent with our hypotheses. Low self-control and hacking self-efficacy facilitate the formation of criminal motivation and favorable judgment about target suitability for MCA in organizations. As the relative magnitude of the path coefficients demonstrate, MCA motivation is largely driven by low self-control while target suitability is predominantly influenced by hacking self-efficacy or potential offenders' knowledge, skill, and ability to use computing devices to access and steal confidential corporate data. These results clearly suggest that employees with low self-control are more motivated to commit MCA and those with high hacking self-efficacy are more likely to deem a digital target as suitable. With respect to security guardianship, deterrence was found to significantly increase the perception of capable guardianship for the targeted digital assets.

The path modeling results regarding the three antecedents show some variation in the impact of self-control and hacking self-efficacy across scenarios, i.e., H5b (low self-control → target suitability) and H6a (hacking self-efficacy → offender motivation). Diverging from the client scenario, employees with relatively low self-control do not perceive product design data and financial data to be easier to compromise or a more suitable target. This may reflect the common awareness that key design information about a firm's new products and financial data are classified as firm "top secrets" and are thus not particularly vulnerable to compromise, since doing so would require both insider knowledge and hacking skills. Therefore, potential employee offenders are rational decision makers who, although they may vary in self-control capability, consider the type of confidential data as part of their MCA decision-making processes.

We also found that hacking self-efficacy (HSE) is only significant for increasing MCA motivation in the scenario involving financial data but not for the other two scenarios. Further comparison of the correlation of HSE and the two subdimensions of motivation, i.e., perceived extrinsic value (PEV) and perceived intrinsic value (PIV), suggests that HSE has a stronger correlation with PIV in the financial scenario but with PEV in the other two scenarios (see Appendix C). Employees may glean intrinsic value from either the outcome of hacking or from the process of hacking. The character described in the financial scenario, i.e., Deborah, is in financial distress. The primary outcome of hacking is to relieve the financial distress faced by Deborah, which is meant to generate monetary value, rather than producing intrinsic value, such as feelings of pride or excitement. In this case, the source of intrinsic value would be attributed more to the hacking process instead of the hacking outcome. Therefore, we submit that the effect of hacking self-efficacy may be stronger in situations involving higher PEV from the outcome of MCA. This result suggests that when examining MCA decisions, it is important to separate PEV and PIV and identify whether PIV is derived from the outcome of MCA or from the process of performing MCA.

The MCA results based on the comparison of three situational scenarios (see Appendix D) provide further support for the important role of context in the decision-making process of potential offenders. The significant scenario differences in path coefficients for H2 (suitable target → intention) and H5b (low self-control → suitable target) suggest that the calculative assessment of target suitability and low self-control seem to exert a bigger influence on the MCA decision in the client scenario than the design scenario in the context of confidential product design data being sold to a competing firm. From the result of the ANOVA analysis with Bonferroni tests, we also found the mean moral beliefs of the design scenario are significantly higher than that of the client scenario. Employees in the design scenario seem to be self-regulated more by moral beliefs and pay less attention to the suitability of the target when the MCA involves highly confidential data that could be used by competing firms to hurt their own organization.

At the same time, we suspect that the nonsignificant effects of target suitability in the design scenario may also result from the competing influence of MCA motivation. To test the competing effect, we built an alternative model by dropping the path from MCA motivation. The path between target suitability and intention became significant at the 0.05 level in the design scenario. Selling confidential product design to a competitor could directly influence the competitiveness of the firm for which the potential offender works, which may introduce additional moral dilemmas or variations in MCA motivation, i.e., the assessment of value and harmfulness of the MCA. This would increase the relative impact of MCA motivation on intention, thereby decreasing the amount of unique variance that could be explained by target suitability. Therefore, we submit that target suitability plays a less important role in situations involving highly confidential data and serious moral issues. This result suggests that it is critical to take into account the type

of data and the third-party agency to which the confidential data is disclosed when examining an offender's security behavior.

Overall, the findings of our study support the following key points:

- The three core pillars of RAT are not equally important to MCA in organizational settings; offender motivation and target suitability are the dominant and most robust factors influencing MCA decisions.
- With respect to antecedents of the RAT core constructs, we found low self-control, hack self-efficacy, and deterrence to be the dominant drivers for offender motivation, target suitability, and capable guardianship, respectively.
- By comparing results across the three scenarios, we note the potential effect of various contextual features, such as type of digital asset, motivation for data breach by potential offenders, recipients of the stolen confidential data, etc.
- When examining employee intention to commit malicious acts, it is important to consider not only situational opportunities but also employee motivations. This is because personal moral beliefs and target suitability become less important among strongly motivated offenders.
- Perceived capable guardianship mostly has a null effect on MCA intention, but may exert an unexpected impact for potential offenders with authorized access to confidential digital assets. Further research is needed to gain a better understanding of this core RAT construct in the MCA context.

6.1 Contribution to Theory

The findings of this study have several important contributions to research on organizational information security. First, as one of the early inquires based on RAT in information security research, this study contributes to the literature by offering new insights, via the crucial lens of offender motivation, target suitability, and capable security guardianship, on MCA in an organizational context. Two of the central arguments of RAT, namely offender motivation and target suitability, are found to significantly influence an employee's intention to commit MCA in organizational settings. On the other hand, capable security guardianship mostly has a null or weak effect on MCA intention, which echoes the results of many empirical studies regarding the effect of deterrence in online as well as offline settings (D'Arcy & Herath, 2011; Hu et al., 2011; Paternoster, 1987). The conventional security guardianship enforced by organizations does not seem to be effective in preventing insiders from committing MCA. Future studies are needed to explore ways to design and deploy guardianship of an organization and to identify conditions under which guardianship can be effective. It would be interesting to expand security guardianship to measures taken by law enforcement agencies. As MCA by employees violates not only organizational policies but potentially federal and state laws as well, internal guardianship measures may take effect together with or even depend on the awareness of external guardianship measures by law enforcement agencies.

RAT assumes offender motivation without explicitly identifying the motivational sources. As a result, prior empirical studies based on RAT have largely assumed offender motivation as a given condition and only tested the effect of target suitability and security guardianship. Our study is the first that explicitly operationalizes offender motivation and tests it together with the other two tenets of RAT. In particular, we operationalized it as a second-order construct formed by intrinsic and extrinsic values and lack of harmfulness. These findings shed new light on the critical role of offender motivation among the three tenets of RAT.

Besides testing the core elements of RAT, our study further extends RAT by examining the interaction effects with moral beliefs, one of the frequently used constructs in criminology and information security research. We find that moral beliefs interact with MCA motivation such that moral beliefs significantly reduce MCA intention only when the level of MCA motivation is low. The effect of moral beliefs is contingent upon the strength of MCA motivation. Future studies are needed to further examine the effect of moral beliefs on the motivation underlying criminal acts. Also, it would be interesting to explore other potential constructs that may moderate the effect of core constructs in RAT such as employee risk propensity.

Another contribution of this study is the development and operationalization of target suitability in the context of digital assets in an organization. Until now, prior studies applying RAT have only operationalized and empirically tested the subdimensions or properties of target suitability in offline settings (Cohen & Felson, 1979; Felson, 1998). Given the few RAT-based studies in the digital context and the unique characteristics of digital assets, our study provides a valuable foundation for future studies to replicate and improve perceived accessibility, perceived visibility, and perceived usability as defining dimensions of target suitability in the context of digital assets.

Our results also suggest that various contextual factors may factor into employees' MCA decisions. For example, in contrast to outside offenders, internal offenders are also organizational employees. Their

MCA intentions may be influenced by their relationship with their organization. As suggested by the comparison of the three scenarios, employees seem to evaluate the nature of digital assets and potential victims in their MCA decisions, as lack of harmfulness influences MCA motivation only for the client scenario but not for the other two scenarios. When situations entail clear harms to employees' own organizations, such as stealing design data for competitors, employees appear to rely more on intrinsic value for motivation and to be more constrained by their inherent moral beliefs when considering committing MCA. Future studies are needed to explicitly identify and test the effects of contextual organizational factors for MCA, such as the level of confidentiality of the targeted digital assets, the extent of harm, and the relationship between the offender and victim, among others.

6.2 Implications for Practice

The findings of this study have important practical implications for reducing and preventing MCA in organizations. We contend that not all three areas identified by RAT have the same effect on effectively managing information security threats from internal employees. According to our theoretical model built on RAT, organizations could focus their security efforts on eliminating one or two of the key elements in order to significantly reduce internal MCA. The challenge to organizations, however, is to determine which of the three elements they can effectively eliminate or significantly diminish. The results of our study shed some light on this critical issue and provide certain prescriptive directions.

Given the finding that offender motivation is the most significant driver of MCA intention in all three scenarios and has the highest magnitude among the three drivers in RAT, minimization of this factor should be the top priority for organizations. Since our results suggest that low self-control and hacking self-efficacy are the two most important factors influencing employees' MCA motivation, it makes sense for organizations to screen candidates for certain organizational positions that have custodial responsibilities for valuable digital assets, such as database administrator, network manager, and network technician. This is consistent with the recommendations of Hu et al. (2011) and Hu et al. (2015), albeit from a different theoretical perspective. In comparison to offline crimes, employers may pay more attention to the impulsivity, risk-seeking, self-centeredness and hacking self-efficacy characteristics of employees when hiring and training them for jobs with potential access to digital organizational assets.

The three dimensions of digital target suitability, i.e., visibility, accessibility, and usability, are all found to have significant weights, suggesting a number of technical options for organizations to improve their defenses against insider security threats. While organizations, in general, cannot escape from the activities that generate, collect, process, and store valuable digital assets, they can certainly reduce the visibility, accessibility, and usability of these digital assets by deploying technologies such as data encryption, server virtualization, and a combination of different information security protection technologies. While none of these technologies are foolproof, together these technologies can help reduce the visibility of data, make it more difficult to gain unauthorized access, and diminish the usability of the data in cases of illegal or unauthorized acquisition.

The mixed findings regarding the role of capable security guardianship in the formation of employee intentions to commit MCA also have some significant practical implications. Although our results show that perceived security guardianship, in general, does not have a strong negative impact on MCA intentions, the data do indicate that strong perceived guardianship has a marginal deterrence effect (p-value < 0.1) on the intention to commit MCA in the financial data scenario. While more studies are clearly needed on the role of security guardianship, organizations cannot afford to ignore the significance of having strong deterrence policies and information security education and awareness training programs (SETA).

6.3 Limitations

Like most theory-based empirical studies, our study inevitably has some limitations, which also provide opportunities for future research. One major limitation is related to the scenario-based cross-sectional design used in our study, meaning that all variables are measured at one point in time, which limits our ability to confirmatively establish causal relationships. For example, the cross-sectional design has no way to unravel how deterrence and capable guardianship are causally linked, i.e., whether deterrence shapes perceived guardianship or vice versa. The cross-sectional design also increases concerns about common method variance (CMV), which increases the likelihood of inflated relationships among latent constructs (Podsakoff et al., 2003). To mitigate the issues of cross-sectional survey design, information security researchers should ideally resort to longitudinal design and/or different data sources to gauge independent and dependent variables. But the challenge of conducting such studies remains formidable in the context of MCA because of employees' reluctance to report their own MCAs and the difficulty of directly observing MCAs by managers. Longitudinal design is particularly vulnerable to the bias of social desirability for self-reported security behaviors (D'Arcy & Lowry, 2019).

To address the practical difficulties of examining MCAs in the digital world, information security researchers may: (1) explore activity logs generated by monitoring devices such as eye and mouse movement trackers to gauge employee security behaviors, and/or (2) conduct controlled experiments and use scenarios to explicitly manipulate salient variables and measure employee perceptions and projected behaviors. Recent advances in cognitive neural sciences also provide new ways to directly measure individuals' brain activities during cognitive decision-making (Hu et al., 2015), which could serve as a separate data source that could be combined with behavioral survey data to test MCA research models.

Second, because we only considered three typical MCA scenarios, we need to exercise caution in generalizing the findings to other MCA situations, as already demonstrated by the different test results from the three subsamples in relation to the effect of security guardianship on employee intention to commit MCA and other variations. The design of consistent and reliable scenarios with representative security threat cases remains a significant challenge for information security research. The third limitation is the concern about the use of behavioral intention instead of actual behavior as the dependent variable. This has been a common issue shared by most behavioral studies in the IS literature. The nature of criminality of the focal behavior has made measuring or collecting data on actual MCA behavior extremely difficult. Like criminologists, IS security scholars (e.g., D'Arcy et al. 2009; Siponen & Vance, 2010; Hu et al., 2011; Johnston et al., 2015) have adopted the notion that intention should be considered indicative of an actual behavioral act (Osgood, 1997). As such, we believe that the intention to commit MCA is a functional proxy of actual behavior, albeit an imperfect one.

Future research could leverage the theoretical framework established in this study and further explore innovative methodological approaches to collect other sources of data which may be used to infer actual behavior (e.g., system logs or sensory data collected by human interface devices such as keyboards and touch screens). Wang, Gupta, and Rao (2015) have demonstrated how survey data and system log data can be combined to provide more reliable and robust tests of theory-driven empirical models in organizational information security settings.

7 Conclusion

Insider security threats continue to pose a potentially devastating risk to organizational survival and competitiveness because they are difficult to detect, prevent, and mitigate in the increasingly connected digital world. To advance the line of research that focuses on deliberate malicious acts by employees and to operationalize and measure salient individual, system, and organizational factors, we draw on and extend the widely used routine activity theory (RAT) to understand deliberate MCA committed by employees towards organizational digital assets. Guided by the theory and tested with data from subjects holding a wide range of organizational positions, the proposed research model enhances our understanding of insider security threats by synthesizing the criminological aspects of the offender, the target, and guardianship with the individual characteristics of self-control, hacking self-efficacy, and moral beliefs, as well as organizational aspects of deterrence. This highly contextualized and relatively comprehensive theoretical model of insider MCA behavior advances the literature on organizational information security and individual decision-making. The empirical findings of this study also help organizations formulate better information security policies and management programs for managing insider security threats and thus improve the overall organizational information security posture.

References

Antia, K. D., Bergen, M. E., Dutta, S., & Fisher, R. J. (2006). How does enforcement deter gray market incidence? *Journal of Marketing Research, 70*(1), 92-106.

Bagozzi, R. P., & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science, 16*(1), 74-94.

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

Bandura, A. (1997). *Self-efficacy: The exercise of control*. W.H. Freeman.

Baron, R. M., & Kenny, D. A. (1986). The Moderator-mediator variable distinction in social psychological research: Conceptual, strategic and statistical considerations. *Journal of Personality and Social Psychology Review, 51*(6), 1173-1182.

Benson, M. L. (1985). Denying the guilty mind: Accounting for involvement in a white-collar crime. *Criminology, 23*(4), 583-607.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. *European Journal of Information Systems 18*(2), 151-164.

Brantingham, P., & Brantingham, P. (2008). Crime pattern theory. In L. M. Richard Wortley (Ed.), *Environmental criminology and crime analysis* (pp. 78-94). Willan.

Brezina, T., & Topalli, V. (2012). Criminal self-efficacy: Exploring the correlates and consequences of a successful criminal identiy. *Criminal Justice and Behavior, 39*(8), 1042-1062.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rational-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523-548.

Burt, C. H., & Simons, R. L. (2013). Self-control, thrill seeking, and crime: Motivation matters. *Criminal Justice and Behavior, 40*(11), 1326-1348.

Cenfetelli, R. T., & Bassellier, G. (2009). Interpretation of formative measurement in information systems research. *MIS Quarterly, 33*(4), 689-707.

CERT. (2016). Common Sense Guide to Mitigating Insider Threats 5th. http://resources.sei.cmu.edu/asset_files/TechnicalReport/2016_005_001_484758.pdf

Chin, W. W. (1998). Issues and opinions on structural equation modeling. *MIS Quarterly, 22*(1), 7-16.

Chin, W. W., Marcolin, B. L., & Newsted, P. R. (2003). A Partial Least Squares latent variable modeling approach for measuring interaction effects: Results from a Monte Carlo simulation study and an electronic mail adoption study. *Information Systems Research, 14*(2), 189-217.

Clarke, R. V. (2012). Opportunity makes the thief. Really? And so what? *Crime ScienceAn Interdisciplinary Journal, 1*(3), 1-9.

Cohen, J. (1988). *Statistical power analysis for the behavior sciences* (2nd ed.). Hillsdale, NJ: Lawrence Erlbaum. Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588-608.

Cohen, L. E., Kluegel, J. R., & Land, K. C. (1981). Social inequality and predatory criminal victimization: An exposition and test of a formal theory. *Americal Sociological Review, 46*(5), 505-524.

Compeau, D. R., & Higgins, C. A. (1995). Computer self efficacy: development of a measure and initial test. *MIS Quarterly, 19*(2), 189-211.

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

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of Management Information Systems, 31*(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, P. B. (2019). Cognitive affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal, 29*(1), 43-69.

D'Arcy, J., & Devaraj, S. (2012). Employee misuse of information technology resources: Testing a contemporary deterrence model. *Decision Sciences, 43*(6), 1091-1124.

Diamantopoulos, A., & Winklhofer, H. M. (2001). Index construction with formative indicators: An alternative to scale development. *Jounal of Marketing Research, 38*(2), 269-277.

Domenie, M. M. L., Leukfeldt, E. R., Wilsem, J. A. v., Jansen, J., & Stol, W. P. (2013). *Victims of offenses with a digital component among Dutch Citizens: Hacking, malware, personal and financial crimes mapped*. Eleven International.

Felson, M. (1998). *Crime and everyday life: insights and implications for society* (2nd ed.). Pine Forge.

Fornell, C., & Larcker, D. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39-50.

Gattiker, U. E., & Kelley, H. (1999). Morality and computers: Attitudes and differences in moral judgments. *Information Systems Research, 10*(3), 233-254.

Gefen, D., & Straub, D. (2005). A practical guide to factorial validity using PLS-Graph: Tutorial and annotated example. *Communications of the Association for Information Systems, 16*(5), 91-109.

Gellma, B., Blake, A., & Miller, G. (2013). Edward Snowden comes forward as source of NSA leaks, *The Washington Post*. https://www.washingtonpost.com/politics/intelligence-leaders-push-back-on-leakers-media/2013/06/09/fff80160-d122-11e2-a73e-826d299ff459_story.html?noredirect=on

Gist, M. E., & Mitchell, T. R. (1987). Self-efficacy: A theoretical analysis of its determinants and malleability. *Academy of Management Review, 17*(2), 183-211.

Gottfredson, M. R., & Hirschi, T. (1990). *A general theory of crime*. Stanford University Press.

Grasmick, H. G., Tittle, C. R., RobertJ. Bursik, J., & Arneklev, B. (1993). Testing the core empirical implications of Gottfredson and Hirschi's general thoery of crime. *Journal of Research in Crime and Delinquency, 30*(1), 5-29.

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems 28*(2), 203–236.

Han, W., Ada, S., Sharman, R., & Raj, R. (2015). Campus emergency notification systems: An examination of factors affecting compliance with alterts. *MIS Quarterly, 39*(4), 909-929.

Henseler, J., Ringle, C. M., & Sarstedt, M. (2016). Testing measurement invariance of composites using partial least squares. *International Marketing Review, 33*(3), 405-431.

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2).

Herbert, C., Green, G. S., & Larrogoite, V. (1998). Clarifying the reach of a general theory of crime for organizational offending: A comment on Reed and Yeager. *Criminology, 36*(4), 867-883.

Hollis-Peel, M. E., Reynald, D. M., Bavel, M. v., Elffers, H., & Welsh, B. C. (2011). Guardianship for crime prevention: A critical review of the literature. *Crime Law and Social Change, 56*, 53-70.

Holsapple, C. W., Iyengar, D., Jin, H., & Rao, S. (2008). Parameters for Software Pirary Research. *The Information Society, 24*(4), 199-218.

Hong, W., Chan, F. K. Y., Thong, J. Y. L., Chasalow, L. C., & Dhillon, G. (2014). A framework and guidelines for context-specific theorizing in information systems research. *Informatinon Systems Research, 25*(1), 111-136.

Howe, E. S., & Brandau, C. J. (1988). Additive effects of certainty, severity, and celerity of punishment on judgments of crime deterrence scale value. *Journal of Applied Social Psychology, 18*(9), 796-812.

Howe, E. S., & Loftus, T. C. (1996). Integration of certainty, severity and celerity information in judged deterrence value: further evidence and methodological equivalence. *Journal of Applied Social Psychology, 26*(3), 226-243.

Hsu, J., Shih, S.-P., Hung, Y. W., & Lowry, P. B. (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.

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.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with

information security policies: The role of top management and organizational culture. *Decision Sciences, 43*(4), 615-660.

Johns, G. (2006). The essential impact of context on organizational behavior. *Academy of Management Review, 31*(2), 386-408.

Johns, G. (2017). Incorporating context in organizational research: Reflections on the 2016 AMR decade award. *Academy of Management Review, 42*(4), 577-595.

Johnson, A. C., 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 Association of Information Systems, 12*(8), 518-555.

Kellett, A. (2015). *Vormetric insider threat report: Global* edition. http://enterprise-encryption.vormetric.com/rs/vormetric/images/CW_GlobalReport_2015_Insider_threat_Vormetric_Single_Pages_010915.pdf

Leonard, L. N. K., & Cronan, T. P. (2001). Illegal, inappropriate, and unethical behavior in an information technology context: A study to explain influences. *Journal of the Association of Information Systems, 1*(12), 1-31.

Leonard, L. N. K., Cronan, T. P., & Kreie., J. (2004). What influences IT ethical behavior intentions-Planned behavior, reasoned action, perceived importance, individual characteristics? *Information and Management, 42*(1), 143-158.

Leukfeldt, E., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoetical and empirical analysis. *Deviant Behavior, 37*(3), 263-280.

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., Zhang, J., & Sarathy, R. (2010). Understand the compliance with the internet use policy from the perspective of rational choice theory. *Decision Support Systems, 48*(4), 635-645.

Lindell, M. K., & Whitney, D. J. (2001). Accounting for common method variance in cross-sectional research designs. *Journal of Applied Psychology, 86*(1), 114-121.

Luo, X. R., Warkentin, M., & Li, H. (2015). Understanding technology adoption trade-offs: A conjoint analysis approach. *Journal for Computer Information Systems, 53*(3), 65-74.

MacKenzie, S. B., Podsakoff, P. M., & Jarvis, C. B. (2005). The problem of measurement model misspecification in behavioral and orgnaizational research and some recommended solutions. *Journal of Applied Psychology, 90*(4), 710-730.

MacKenzie, S. B., Podsakoff, P. M., & Podsakoff, N. P. (2011). Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques. *MIS Quarterly, 35*(2), 293-334.

Mathieson, K., Peacock, E., & Chin, W. W. (2001). Extending the technology acceptance model: The influence of perceived user resources. *Database for Advances in Information Systems, 32*(3), 86-112.

McKinney, V., Yoon, K., & Zahedi, F. (2002). The measurement of web-customer satisfaction: An expectation and disconfirmation approach. *Information Systems Research, 13*, 296-315.

Morris, R. G., & Higgins, G. E. (2008). Neutralizing potential and self-reported digital privacy: A multitheoretical exploration among college undergraduates. *Criminal Justice Review, 34*(2), 173-195.

Nagin, D. S., & Paternoster, R. (1993). Enduring individual differences and rational choice theories of crime. *Law & Society Review, 27*(3), 467-496.

Naso, R. C. (2012). When money and morality collide: White collar crime and the paradox of integrity. *Psychoanalytic Psychology, 29*(2), 241-254.

Osgood, D. W. (1997). *Motivation and delinquency: Nebraska symposium on motivation* (Vol. 44): University of Nebraska Press.

Parker, D. B. (1998). *Fighting computer crime: A new framework for protecting information*. Wiley.

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

Paternoster, R., & Simpson, S. (1996). Sanction threats and appeals to morality: Testing a rational choice model of corporate crime. *Law & Society Review, 30*(3), 549-583.

Peace, A. G., Galletta, D., & Thong, J. (2003). Software piracy in the workplace: A model and

empirical test. *Journal of Management Information Systems, 20*(1), 153-177.

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

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff., N. P. (2003). Common method biases in behavior research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology, 88*(5), 879-903.

Posey, C., Bennett, R. J., & Roberts, T. L. (2011). Understanding the mindset of the abusive insider: An examination of insiders' causal reasoning following internal security changes. *Computers & Security, 30*(6-7), 486-497.

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency, 47*(3), 267-296.

Reyns, B. W. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency, 50*(2), 216-238.

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being pursued online: Applying cyberlifestyle-routine activities theory to cyberstalking victimization. *Criminal Justice and Behavior, 38*(11), 1149-1169.

Rice, K. J., & Csmith, W. R. (2002). Socioecological models of automotive theft: Integrating routine activity and social disorganization approaches. *Journal of Research in Crime and Delinquency, 39*(3), 304-336.

Savage, C., & Huetteman, E. (2013). Manning Sentenced to 35 Years for a Pivotal Leak of U.S. Files, *New York Times*. https://www.nytimes.com/2013/08/22/us/manning-sentenced-for-leaking-government-secrets.html

Shrout, P. E., & Bolger, N. (2002). Mediation in experimental and nonexperimental studies: new procedures and recommendations. *Psychological Methods, 7*(4), 422-445.

Simpson, S. S., & Koper, C. S. (1992). Deterring corporate crime. *Criminology, 30*(3), 347-376.

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

Sobel, M. E. (1982). Asymptotic confidence intervals for direct effects in structural equation models. In S. Leinhardt (Ed.), *Sociological methodology* (pp. 290-312). American Sociological Association.

Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research, 1*(3), 255-276.

Vance, A., Lowry, P. B., & Eggett, D. (2015). Increasing accountability through user-interface design artifacts: A new approach to addressing the problem of access-policy violations. *MIS Quarterly, 39*(2), 345-366.

Vance, A., & Siponen, M. T. (2012). IS security violations: A rational choice perspective. *Journal of Organizational and End User Computing, 24*(1), 21-41.

Vaughan, T. J., Ward, J. T., Bouffard, J., & Piquero, A. R. (2019). The general factor of self-control and cost consideration: A critical test of the general theory of crime. *Crime & Delinquency, 65*(6), 731–771.

Wang, J., Gupta, M., & Rao, H. R. (2015). Insider threats in a financial institution: Analysis of attack-proneness of information systems applications. *MIS Quarterly, 39*(1), 91-112.

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.

Wenzel, M. (2005). Motivation or rationalization? Causal relations between ethics, norms and tax compliance. *Journal of Economic Psychology, 26*, 491-508.

Whitman, M. E., & Mattord, H. J. (2005). *Principles of Information Security* (2nd ed.). Thomason Course Technology.

Wilcox, P., & Cullen, F. T. (2018). Situational opportunity theories of crime. *Annual Review of Criminology, 1*(1), 123-148.

Willison, R. (2006). Understanding the offender/environment dynamic for computer crimes. *Information Technology & People, 19*(2), 170-186.

Willison, R., Lowry, P. B., & Paternoster, R. (2018). A tale of two deterrents: Considering the role of absolute and restrictive deterrence to inspire new directions in behavioral and organizational security research. *Journal of the Association of Information Systems, 19*(12), 1187-1216.

Willison, R., & Siponen, M. (2009). Overcoming the insider: Reducing employee computer crime through situational crime prevention, *Communications of the ACM*, *52*(9), 133-137.

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

Wood, R., & Bandura, A. (1989). Impact of conceptions of ability on self-regulatory mechanism and complex decision making. *Journal of Personality and Social Psychology*, *56*(3), 407-415.

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

Wright, B. R. E. (2004). Does the perceived risk of punishment deter criminally prone individuals? Rational choice, self-control, and crime. *Journal of Research in Crime and Delinquency*, *41*(2), 180-213.

Yar, M. (2005). The Novelty of "Cybercrime": An assessment in light of routine activity theory. *European Journal of Criminology*, *2*(4), 407-427.

Appendix A. Summary of Literature on Information Security Behaviors of Organizational Insiders

Table A1. Summary of Literature on the Information Security Behaviors of Organizational Insiders

Paper	Method	Main Theory/lenses	IS behaviors (with malicious intent?)	Study compromise of digital assets? (intentional compromise? identify specific digital target to compromise?)				
					Three pillars of RAT			
					MOV	STG	CGS	Holistic RAT
Straub (1990)	Survey/ cross-sectional	General deterrence theory	Computer abuse (No, study computer abuse in general)	Yes (Yes, No) Examine computer abuse in general	Yes	No	Yes	No
Boss et al. (2009)	Survey/ cross-sectional	Organizational control lens	Information security precaution-taking behavior (No)	No (No, No), Examine favorable security behaviors	No	No	Yes	No
Bulgurcu et al. (2010)	Survey/ cross-sectional	Theory of planned behavior, Rational choice theory	Information security awareness and ISP compliance (No)	No (No, No) Examine compliance in general.	No	No	Yes	No
D'Arcy et al. (2009)	Survey/ scenario/ cross-sectional	General deterrence theory	IS misuse intention (No)	Yes (Yes, Yes) Mention specific targets in the scenarios.	No	No	Yes	No
D'Arcy and Devaraj (2012)	Survey/ scenario/ cross-sectional	General deterrence theory	Technology misuse intentions (No)	Yes (Yes, Yes) Mention specific targets in the scenarios.	No	No	Yes	No
D'Arcy, Herath, & Shoss (2014)	Survey/ scenario/ cross-sectional	Coping theory, moral disengagement theory, social cognitive theory	ISP violation (No)	Yes (Yes, Yes) Mention specific targets in the scenarios.	Yes	No	Yes	No
D'Arcy & Lowry (2019)	Experience sampling methodology/ longitudinal for within-subject variables.	Rational choice theory, theory of planned behavior	ISP compliance (No)	No (No, No)	No	No	Yes	No
Guo et al. (2011)	Survey/ scenario/ cross-sectional	Theory of reasoned action, theory of planned behavior	ISP violation (No)	Yes (Yes, Yes) Mention specific targets in the scenarios.	Yes	No	Yes	No
Hu et al. (2012)	Survey/ Cross-sectional	Theory of planned behavior	ISP compliance (No)	No (No, No) Examine compliance in general.	No	No	No	No
Hsu et al. (2015)	Survey/ Paired manager and employee data	Social control theory	Information security behaviors for benefiting organizations (No)	No (No, No), Examine favorable security behaviors	No	No	Yes	No

Johnston et al. (2015)	Survey/ Cross-sectional	Fear appeal theory and deterrence theory	ISP compliance (No)	No (No, No) Examine compliance in general.	No	No	Yes	No
Lee & Lee (2002)	Conceptual model	Theory of planned behavior, social bound theory, social learning theory	Computer abuse (No, study computer abuse in general)	Yes (Yes, No) Examine computer abuse in general	No	No	Yes	No
Posey, Bennett, & Roberts (2011)	Survey/ Projective technique/ Cross-sectional	Causal reasoning theory	Projected behaviors by co-workers (Yes, some projected behaviors are malicious)	Yes (Yes, Yes) Describe targets in the projected behaviors of peers.	No	No	No	No
Siponen & Vance (2010)	Survey/ Scenario/ Cross-sectional	Neutralization theory, deterrence theory	ISP violation (No, for the purpose of getting job done and helping others)	Yes (Yes, Yes) Mention specific targets in the scenarios.	Yes	No	Yes	No
Warkentin & Willison (2009)	Editorial comments	NA	Insider threat to IS security (No, general review of insider threats)	General review of issues related to insider threats.	Yes	No	Yes	No
Willison & Siponen (2009)	Research commentary	NA	Insider computer crime (Yes)	Yes (Yes, NA) Conceptual illustration	No	Yes	Yes	No
Willison & Warkentin (2013)	Research commentary	Neutralization, organizational justice, deterrence	Computer abuse (Yes)	Yes (Yes, NA) Conceptual illustration	Yes	No	Yes	No
Willison, Lowry, & Paternoster (2018)	Research commentary	Rational choice framework, deterrence theory	Computer abuse (Yes)	Yes (Yes, NA) Conceptual illustration	Yes	Yes	Yes	Yes
Workman & Gathegi (2007)	Field experiment	Theory of planned behavior, social learning and deterrence theories	ISP Violation behaviors (No, study violation in general)	Yes (Yes, Partial) Mostly general violations such as “a security measure”.	Yes	No	Yes	No
Yar (2005)	Research commentary	Routine activity theory	Cybercrime (Yes)	Yes (Yes, NA) Conceptual illustration of RAT in cyberspace. Assume given motivation.	No	Yes	Yes	No
Leukfeldt & Yar (2016)	Secondary analysis on an archived dataset by Domenie et al. Domenie et al. (2013)	Routine activity theory	Victimization of cybercrime (Yes, but study from the perspective of victims of cybercrime instead of offenders)	Yes (Yes, No) Consider human subjects as the target to be victimized by cybercrimes such as cyberstalking and identity theft.	No	Yes	Yes	No

Note: MOV – Offender motivation of compromising digital assets, STG – Target suitability, CGS – Capable guardianship of digital assets.

Appendix B. Survey Instrument

Table B1. Section 1: Perceived Accessibility, Usability, and Visibility

Perceived accessibility (PAC)		
PAC1	I would think that the confidential data of my company are readily accessible to me. (1-strongly disagree, 4-not sure either way, 7-strongly agree)	1 2 3 4 5 6 7
PAC2	I would feel that I could access the confidential data of my company anytime I want to. (1-strongly disagree, 4-not sure either way, 7-strongly agree)	1 2 3 4 5 6 7
PAC3	I would believe that the confidential data of my company are easy to access by people like me. (1-strongly disagree, 4-not sure either way, 7-strongly agree)	1 2 3 4 5 6 7
Perceived usability (Inertia) (PUS)		
PUS1	I would think that the confidential data could be usable to me without much effort (1-strongly disagree, 4-not sure either way, 7-strongly agree)	1 2 3 4 5 6 7
PUS2	I would feel that the confidential data could be used right away (1-strongly disagree, 4-not sure either way, 7-strongly agree)	1 2 3 4 5 6 7
PUS3	I would believe that I could use the confidential data without difficulty (1-strongly disagree, 4-not sure either way, 7-strongly agree)	1 2 3 4 5 6 7
Perceived visibility (PVS)		
PVS1	I would know where specific types of confidential data are stored (1-strongly disagree, 4-not sure either way, 7-strongly agree)	1 2 3 4 5 6 7
PVS2	I would be able to locate specific types of confidential data (1-strongly disagree, 4-not sure either way, 7-strongly agree)	1 2 3 4 5 6 7
PVS3	I would be aware of the storing location of specific types of confidential data (1-strongly disagree, 4-not sure either way, 7-strongly agree).	1 2 3 4 5 6 7

Table B2. Section 2: Intention and Moral Beliefs

INT1	I would have made the same decision if I were in the same situation (1-strongly disagree, 4-not sure either way, 7-strongly agree)	1 2 3 4 5 6 7
INT2	I could see myself making the same decision if I were in the same situation. (1-strongly disagree, 4-not sure either way, 7-strongly agree)	1 2 3 4 5 6 7
RC	How realistic do you think this scenario is in your own company? (1=highly unrealistic, 4- not sure either way, 7=highly realistic)	1 2 3 4 5 6 7
MRB1	I would find it morally unacceptable to do what the character did if I were in that situation (1-strongly disagree, 4-not sure either way, 7-strongly agree)	1 2 3 4 5 6 7
MRB2	It would be against my moral beliefs to do what the character did if I were in the same situation. (1-strongly disagree, 4-not sure either way, 7-strongly agree)	1 2 3 4 5 6 7

Table B3. Section 3: Perceived Value

If you committed the act described in the scenarios, it is likely that: *1-Strongly Disagree* *4-Neutral* *7-Strongly Agree*		
PEV1	you would be able to have more material possessions	1 2 3 4 5 6 7
PEV2	you would have more money than you ever had before	1 2 3 4 5 6 7
PEV3	you would be able to afford things you could not afford	1 2 3 4 5 6 7
PEV4	you would be able to buy things you have always wanted to buy	1 2 3 4 5 6 7
PIV1	you would feel proud	1 2 3 4 5 6 7
PIV2	you would feel thrilled	1 2 3 4 5 6 7
PIV3	you would feel happy	1 2 3 4 5 6 7
PIV4	you would feel satisfied	1 2 3 4 5 6 7

Table B4. Section 4: Individual Propensity (Low Self-Control)

1-Strongly Disagree	*4-Neutral*	*7-Strongly Agree*
IMP1	I often act on the spur of the moment without stopping to think.	1 2 3 4 5 6 7
IMP2	I don't devote much thought and effort to preparing for the future.	1 2 3 4 5 6 7
IMP3	I often do whatever brings me pleasure here and now, even at the cost of some distant goal.	1 2 3 4 5 6 7
IMP4	I'm more concerned with what happens to me in the short run than in the long run.	1 2 3 4 5 6 7
RSK1	I like to test myself every now and then by doing something a little risky.	1 2 3 4 5 6 7
RSK2	Sometimes I will take a risk just for the fun of it.	1 2 3 4 5 6 7
RSK3	I sometimes find it exciting to do things for which I might get in trouble.	1 2 3 4 5 6 7
RSK4	Excitement and adventure are more important to me than security.	1 2 3 4 5 6 7
SCT1	I try to look out for myself first, even if it means making things difficult for other people.	1 2 3 4 5 6 7
SCT2	I have little sympathy for other people when they are having problems	1 2 3 4 5 6 7
SCT3	If things I do upset people, it's their problem not mine.	1 2 3 4 5 6 7
SCT4	I will try to get the things I want even when I know it's causing problems for other people.	1 2 3 4 5 6 7
TMP1	I lose my temper pretty easily.	1 2 3 4 5 6 7
TMP2	Often, when I am angry at people, I feel more like hurting them than talking to them about why I am angry.	1 2 3 4 5 6 7
TMP3	When I am really angry, other people had better stay away from me.	1 2 3 4 5 6 7
TMP4	When I have a serious disagreement with someone, it is usually hard for me to talk calmly about it without getting upset.	1 2 3 4 5 6 7

Table B5. Section 5: Hacking Self-Efficacy

1-*Strongly Disagree*	*4-Neutral*	*7-Strongly Agree*
HSE1	If I wanted to, I would be able to use my computer skills to gain unauthorized access to and obtain sensitive corporate information from my organization	1 2 3 4 5 6 7
HSE2	If I wanted to, I am confident I could get sensitive corporate information from my organization without authorization by using my computer skills	1 2 3 4 5 6 7
HSE3	If I wanted to, I believe I have the necessary computer skills to gain unauthorized access to and obtain sensitive corporate information from my organization.	1 2 3 4 5 6 7

Table B6. Section 6: Perceived Harmfulness

1-Strongly Disagree	*4-Neutral*	*7-Strongly Agree*
LHM1	I think it would be harmful to do what the character described above decided to do if I were in the same situation.	1 2 3 4 5 6 7
LHM2	I believe it would be damaging to do what the character described above decided to do if I were in the same situation.	1 2 3 4 5 6 7

Table B7. Section 7: Deterrence Measures (Certainty, Severity, Celerity)

1-Strongly Disagree	*4-Neutral*	*7-Strongly Agree*
CER1	It is routine for our company to review audit logs to identify computer abusive activities	1 2 3 4 5 6 7
CER2	It is certain that employees who commit computer abusive activities will be caught.	1 2 3 4 5 6 7
CER3	It is likely that computer abusive activities can be traced back to the violators.	1 2 3 4 5 6 7
SVR1	In our company, employees who are caught abusing computers and data are severely punished.	1 2 3 4 5 6 7
SVR2	In our company, employees who are caught abusing computers and data are critically reprimanded.	1 2 3 4 5 6 7
SVR3	In our company, employees who are caught abusing computers and data face serious consequences.	1 2 3 4 5 6 7
CEL1	In our company, the actions against employee computer abusive behavior are immediate.	1 2 3 4 5 6 7
CEL2	In our company, the actions against employee computer abusive behavior are instantaneous.	1 2 3 4 5 6 7
CEL3	In our company, the actions against employee computer abusive behavior are timely.	1 2 3 4 5 6 7

Table B8. Section 8: Security Guardianship

1-Strongly Disagree	*4-Neutral*	*7-Strongly Agree*
POL1	My company has specific guidelines that describe acceptable use of computing resources such as email and the internet	1 2 3 4 5 6 7
POL2	My company has established rules of behavior for use of computer resources.	1 2 3 4 5 6 7
POL3	My company has a formal policy that forbids employees from accessing computer systems that they are not authorized to use.	1 2 3 4 5 6 7
POL4	My company has specific guidelines that describe acceptable computer passwords and enforces regularly changing them.	1 2 3 4 5 6 7
POL5	My company has specific guidelines that govern what employees are allowed to do with their computers.	1 2 3 4 5 6 7
SETA1	In my company, employees are briefed on the consequences of modifying computerized data in an unauthorized way.	1 2 3 4 5 6 7
SETA2	My organization educates employees on their computer and information security responsibilities.	1 2 3 4 5 6 7
SETA3	In my company, employees are briefed on the consequences of accessing computer systems that they are not authorized to use.	1 2 3 4 5 6 7
MOR1	My company monitors any modification or altering of computerized data by employees.	1 2 3 4 5 6 7
MOR2	Employee computing activities are monitored by my organization.	1 2 3 4 5 6 7

Table B9. Section 9: Respondent Profile (Choose One)

Age	• < 24 • 25-34 • 35-44 • 45-55 • > 55	Education	• High school • Professional School • College • Graduate College • Other
Sex	• Male (1) • Female (0)	Employment status	• Part Time • Full Time
Job Position	• Corporate executive • Division manager/supervisor • IT Professional • Administrative staff • Business/professional • Technical/engineering • Other (please specify)	Computer usage (hours per day)	• < 2 • 2-3 • 4-5 • 6-8 • > 8
Internet Experience (Approximately how many years have you been using the Internet?)	• <5 years • 6-10 years • 11-15 years • 16-20 • >20 years	Computer access (choose one only)	• Perform data entry only • Run applications and generate reports • Access to database and date file • Add and modify data in the system • Install new programs and add new users
Prior Criminal Offense	Have you committed computer and information security violations before? • Yes • No	The number of employees in your company is	• 1-100 • 101-250 • 251-500 • 501-1,000 • 1,001-5,000 • 5,000+

The industry your company primarily belongs to:	• Manufacturing • Financial (bank, insurance, etc.) • Services (healthcare, hospitality, etc.) • Agriculture • Information Technology • Retail/wholesale • Education • Transportation/logistics • Utility/Energy • Other (Specify)_____	IS security experience: How much do you know about the concept, technology, and practice related to information security in organizations?	• 1 – I know very little about it • 2 – I heard about it • 3 – I had information security training in school or from my company • 4 – I deal with information security issues in my routine work • 5 - I am an expert in information security • 6 - I manage information security for my company

Appendix C. Results of Measurement Model Testing

Table C1. Results of Invariance Measurement Testing Using Permutation

	Compostional Invariance						Partial Measure. Invariance	Equal Mean Assessment							Full Measure. Invariance
	Correlation			5% Quantile				Difference			Confidence Interval				
	C vs. D	C vs. F	D vs. F	C vs. D	C vs. F	D vs. F		C vs. D	C vs. F	D vs. F	C vs. D	C vs. F	D vs. F	Equal	
1. Moral beliefs	1.000	1.000	1.000	0.998	0.998	0.999	Yes	-0.545	-0.276	0.273	(-0.257,0.249)	(-0.267,0.268)	(-0.255,0.257)	No	No
2. Impulsivity	1.000	1.000	1.000	1.000	1.000	1.000	Yes	0.018	-0.011	-0.030	(-0.247,0.258)	(-0.258,0.250)	(-0.256,0.251)	Yes	
3. Risk seeking	1.000	1.000	0.998	0.997	0.997	0.996	Yes	0.063	0.001	-0.059	(-0.250,0.257)	(-0.264,0.267)	(-0.263,0.255)	Yes	
4. Self-centeredness	1.000	1.000	1.000	0.999	0.998	0.998	Yes	0.026	-0.023	-0.052	(-0.251,0.253)	(-0.257,0.265)	(-0.260,0.252)	Yes	
5. Temper	1.000	0.997	0.999	0.997	0.996	0.998	Yes	0.107	-0.018	-0.117	(-0.249,0.244)	(-0.257,0.267)	(-0.260,0.258)	Yes	
6. Hack self-efficacy	1.000	1.000	1.000	1.000	1.000	1.000	Yes	0.001	-0.090	-0.089	(-0.251,0.241)	(-0.265,0.253)	(-0.268,0.263)	Yes	
7. Certainty	1.000	1.000	1.000	1.000	1.000	1.000	Yes	0.063	0.050	-0.015	(-0.250,0.246)	(-0.261,0.254)	(-0.257,0.260)	Yes	
8. Severity	0.972	0.990	0.986	0.281	0.718	0.348	Yes	0.151	0.054	-0.024	(-0.256,0.251)	(-0.252,0.258)	(-0.258,0.262)	Yes	
9. Celerity	1.000	1.000	1.000	1.000	1.000	1.000	Yes	0.179	0.078	-0.093	(-0.261,0.251)	(-0.252,0.259)	(-0.259,0.260)	Yes	
10. Extrinsic value	1.000	1.000	1.000	1.000	1.000	1.000	Yes	-0.199	-0.444	-0.262	(-0.255,0.250)	(-0.268,0.267)	(-0.253,0.263)	No	
11. Intrinsic value	1.000	1.000	1.000	1.000	1.000	1.000	Yes	0.210	0.308	0.081	(-0.254,0.247)	(-0.269,0.265)	(-0.263,0.252)	No	
12. Lack of harm.	1.000	1.000	1.000	1.000	1.000	1.000	Yes	0.237	0.238	-0.025	(-0.253,0.254)	(-0.263,0.277)	(-0.265,0.261)	Yes	
13. Accessibility	1.000	0.999	0.999	0.999	0.999	0.997	Yes	-0.028	0.055	0.084	(-0.253,0.255)	(-0.246,0.268)	(-0.261,0.254)	Yes	
14. Visibility	1.000	1.000	0.999	0.998	0.999	0.994	Yes	0.024	-0.004	-0.029	(-0.250,0.247)	(-0.266,0.271)	(-0.260,0.256)	Yes	
15. Usability	0.999	1.000	0.999	0.999	0.999	0.999	Yes	0.008	0.186	0.175	(-0.250,0.254)	(-0.262,0.274)	(-0.254,0.256)	Yes	
16. Security policies	1.000	1.000	1.000	1.000	1.000	1.000	Yes	0.040	0.003	-0.039	(-0.261,0.259)	(-0.257,0.256)	(-0.259,0.259)	Yes	
17. Monitoring	0.994	0.968	0.992	0.405	0.611	0.327	Yes	0.094	0.023	-0.035	(-0.248,0.257)	(-0.265,0.252)	(-0.248,0.258)	Yes	
18. SETA	1.000	1.000	1.000	1.000	1.000	1.000	Yes	0.058	0.103	0.047	(-0.245,0.254)	(-0.255,0.256)	(-0.250,0.257)	Yes	
19. Intention	1.000	1.000	1.000	1.000	1.000	1.000	Yes	0.326	0.349	0.013	(-0.241,0.254)	(-0.262,0.263)	(-0.247,0.251)	No	
20. Low self-control	0.999	0.999	1.000	0.999	0.999	0.999	Yes	0.056	-0.029	-0.084	(-0.251,0.248)	(-0.265,0.256)	(-0.255,0.264)	Yes	
21. Deterrence	1.000	1.000	1.000	0.998	0.997	0.999	Yes	0.130	0.068	-0.059	(-0.262,0.239)	(-0.258,0.249)	(-0.252,0.261)	Yes	
22. Motivated offender	0.968	0.972	0.995	0.952	0.949	0.961	Yes	0.150	0.193	0.022	(-0.243,0.257)	(-0.267,0.258)	(-0.245,0.256)	Yes	
23. Suitable target	0.999	0.999	0.998	0.999	0.998	0.997	Yes	0.000	0.104	0.099	(-0.250,0.245)	(-0.261,0.261)	(-0.252,0.250)	Yes	
24. Capable guard.	1.000	1.000	1.000	0.999	0.999	0.999	Yes	0.057	0.049	-0.007	(-0.252,0.243)	(-0.265,0.263)	(-0.253,0.257)	Yes	

Note: C = Client, D = Design, F = Finance.

Table C2. Weights, *T*-Statistics and *P*-Values of Formative Constructs

Scenario	Client			Design			Finance		
	Weight	*t*	*p*	Weight	t	p	Weight	*t*	*p*
Impulsivity -> Low self-control	0.316	17.586	**0.000**	0.279	15.184	**0.000**	0.259	11.579	**0.000**
Risk seeking -> Low self-control	0.268	11.645	**0.000**	0.263	13.366	**0.000**	0.312	13.398	**0.000**
Self-centeredness -> Low self-control	0.291	16.558	**0.000**	0.343	13.321	**0.000**	0.321	16.646	**0.000**
Temper -> Low self-control	0.270	12.574	**0.000**	0.233	9.276	**0.000**	0.259	12.104	**0.000**
Perceived certainty -> Deterrence	0.421	7.095	**0.000**	0.382	17.533	**0.000**	0.367	18.117	**0.000**
Perceived severity -> Deterrence	0.393	15.678	**0.000**	0.368	22.834	**0.000**	0.381	21.828	**0.000**
Perceived celerity -> Deterrence	0.342	13.823	**0.000**	0.349	22.846	**0.000**	0.350	20.733	**0.000**
Perceived extrinsic value -> Offender motivation	0.375	3.393	**0.001**	0.216	2.254	**0.024**	0.180	2.180	**0.029**
Perceived intrinsic value -> Offender motivation	0.619	5.518	**0.000**	0.861	11.359	**0.000**	0.869	11.584	**0.000**
Lack of harmfulness -> Offender motivation	0.298	2.941	**0.003**	0.049	0.604	0.546	0.141	1.463	0.144
Perceived accessibility -> Target suitability	0.412	17.797	**0.000**	0.364	13.890	**0.000**	0.402	11.720	**0.000**
Perceived visibility -> Target suitability	0.300	14.242	**0.000**	0.334	11.498	**0.000**	0.273	5.731	**0.000**
Perceived usability -> Target suitability	0.367	25.737	**0.000**	0.386	18.501	**0.000**	0.458	11.675	**0.000**
Security policies -> Capable guard.	0.342	22.816	**0.000**	0.329	16.649	**0.000**	0.362	12.726	**0.000**
Computer monitoring -> Capable guard.	0.366	19.038	**0.000**	0.391	21.448	**0.000**	0.381	19.841	**0.000**
SETA -> capable guard.	0.352	32.129	**0.000**	0.373	23.457	**0.000**	0.361	14.998	**0.000**

Note: Significant *p*-values are bolded.

Table C3. Loadings, Average Variance Extracted (AVE) and Composite Reliability (CR)

		Loading			AVE			CR		
Constructs	**Item**	**Client**	**Design**	**Finance**	**Client**	**Design**	**Finance**	**Client**	**Design**	**Finance**
1. Moral beliefs	MRB_1	0.976	0.962	0.976	0.939	0.922	0.950	0.969	0.959	0.974
	MRB_2	0.962	0.959	0.973						
2. Impulsivity	IMP_1	0.880	0.772	0.839	0.771	0.733	0.711	0.931	0.916	0.908
	IMP_2	0.846	0.863	0.805						
	IMP_3	0.915	0.906	0.872						
	IMP_4	0.870	0.878	0.855						
3. Risk seeking	RSK_1	0.851	0.858	0.863	0.779	0.783	0.769	0.934	0.935	0.930
	RSK_2	0.890	0.887	0.888						
	RSK_3	0.900	0.906	0.916						
	RSK_4	0.888	0.886	0.839						
4. Self-centeredness	SCT_1	0.867	0.869	0.857	0.782	0.785	0.745	0.935	0.936	0.921

	SCT_2	0.904	0.877	0.878						
	SCT_3	0.860	0.890	0.855						
	SCT_4	0.905	0.908	0.862						
5. Temper	TMP_1	0.766	0.907	0.847	0.682	0.847	0.793	0.896	0.957	0.939
	TMP_2	0.861	0.944	0.915						
	TMP_3	0.833	0.917	0.919						
	TMP_4	0.841	0.912	0.879						
6. Hacking self-efficacy	SE_1	0.961	0.961	0.972	0.934	0.946	0.949	0.977	0.981	0.982
	SE_2	0.977	0.984	0.981						
	SE_3	0.962	0.973	0.969						
7. Perceived certainty	CER_1	0.791	0.814	0.831	0.709	0.728	0.737	0.879	0.889	0.894
	CER_2	0.900	0.903	0.885						
8. Perceived severity	SVR_1	0.875	0.974	0.956	0.861	0.887	0.900	0.949	0.959	0.964
	SVR_2	0.969	0.934	0.936						
	SVR_3	0.938	0.916	0.954						
9. Perceived celerity	CEL_1	0.912	0.923	0.950	0.813	0.830	0.871	0.929	0.936	0.953
	CEL_2	0.914	0.929	0.927						
	CEL_3	0.878	0.880	0.923						
10. Perceived extrinsic value	PEV_1	0.899	0.854	0.872	0.893	0.861	0.852	0.971	0.961	0.958
	PEV_2	0.965	0.948	0.924						
	PEV_3	0.966	0.951	0.961						
	PEV_4	0.948	0.955	0.934						
11. Perceived intrinsic value	PIV_1	0.970	0.964	0.964	0.951	0.946	0.908	0.987	0.986	0.975
	PIV_2	0.984	0.969	0.928						
	PIV_3	0.986	0.984	0.966						
	PIV_4	0.962	0.973	0.953						
12. Lack of harmfulness	LHM_1	0.958	0.975	0.910	0.927	0.938	0.862	0.962	0.968	0.926
	LHM_2	0.967	0.961	0.947						
13. Perceived accessibility	PAC_1	0.945	0.940	0.891	0.888	0.869	0.855	0.960	0.952	0.947
	PAC_2	0.954	0.942	0.945						
	PAC_3	0.928	0.914	0.937						
14. Perceived visibility	PVS_1	0.961	0.932	0.926	0.933	0.886	0.888	0.977	0.959	0.960
	PVS_2	0.975	0.961	0.949						
	PVS_3	0.962	0.931	0.952						
15. Perceived usability	PUS_1	0.962	0.931	0.915	0.903	0.883	0.839	0.966	0.958	0.940
	PUS_2	0.951	0.934	0.929						
	PUS_3	0.939	0.954	0.904						
16. Security policies	POL_1	0.921	0.892	0.830	0.832	0.771	0.760	0.961	0.944	0.941
	POL_2	0.905	0.903	0.891						

	POL_3	0.909	0.860	0.883						
	POL_4	0.890	0.840	0.899						
	POL_5	0.934	0.894	0.854						
17. Computer monitoring	MOR_1	0.939	0.963	0.980	0.930	0.926	0.868	0.964	0.962	0.929
	MOR_2	0.990	0.962	0.880						
18. SETA	SETA_1	0.920	0.935	0.941	0.846	0.873	0.894	0.943	0.954	0.962
	SETA_2	0.904	0.918	0.951						
	SETA_3	0.935	0.950	0.945						
19. Intention	INT_1	0.986	0.982	0.978	0.972	0.963	0.957	0.986	0.981	0.978
	INT_2	0.986	0.980	0.978						

Table C4a. Mean, Standard Deviation, and Discriminant Validity (Client)

	Mean	*SD*	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
1. Moral beliefs	5.04	1.63	**0.97**																		
2. Impulsivity	3.28	1.53	-0.03	**0.88**																	
3. Risk seeking	3.28	1.49	-0.03	0.72	**0.88**																
4. Self-centeredness	2.92	1.55	0.03	0.72	0.64	**0.88**															
5. Temper	3.35	1.36	0.12	0.70	0.56	0.73	**0.83**														
6. Hacking self-efficacy	3.43	1.93	-0.01	0.49	0.55	0.60	0.50	**0.97**													
7. Perceived certainty	5.09	1.21	0.23	-0.01	0.18	-0.07	-0.08	0.00	**0.84**												
8. Perceived severity	5.34	1.27	0.10	-0.20	0.00	-0.17	-0.15	-0.06	0.55	**0.93**											
9. Perceived celerity	5.03	1.22	0.12	-0.12	0.10	-0.03	-0.08	-0.08	0.56	0.77	**0.90**										
10. Perceived extrinsic value	3.79	1.66	0.17	0.58	0.46	0.46	0.50	0.42	0.07	-0.09	0.01	**0.94**									
11. Perceived intrinsic value	3.14	1.81	-0.14	0.59	0.51	0.56	0.50	0.39	0.00	-0.07	0.07	0.61	**0.98**								
12. Lack of harmfulness	2.49	1.38	-0.50	0.22	0.21	0.28	0.13	0.03	-0.35	-0.24	-0.14	0.00	0.29	**0.96**							
13. Perceived accessibility	3.91	1.80	0.07	0.53	0.37	0.46	0.45	0.44	-0.14	-0.12	-0.06	0.55	0.59	0.22	**0.94**						
14. Perceived visibility	4.45	1.69	0.15	0.36	0.41	0.32	0.37	0.45	-0.03	0.04	-0.02	0.43	0.35	0.12	0.67	**0.97**					
15. Perceived usability	3.93	1.71	0.08	0.43	0.38	0.40	0.39	0.44	-0.11	-0.05	-0.04	0.49	0.52	0.24	0.88	0.80	**0.95**				
16. Security policies	5.35	1.37	0.17	-0.05	0.08	0.00	-0.09	0.09	0.64	0.59	0.45	0.01	-0.02	-0.22	-0.01	0.05	0.04	**0.91**			

17. Computer monitoring	4.98	1.56	0.12	-0.09	0.13	0.01	-0.03	0.11	0.65	0.62	0.54	0.03	0.06	-0.26	-0.11	-0.04	-0.06	0.83	**0.96**	
18. SETA	4.99	1.46	0.08	-0.03	0.11	0.08	-0.04	0.07	0.61	0.58	0.58	0.00	0.06	-0.14	-0.03	0.03	0.01	0.87	0.81	**0.92**
19. Intention	3.37	1.89	-0.16	0.68	0.56	0.59	0.53	0.38	-0.07	-0.07	0.03	0.50	0.70	0.42	0.69	0.43	0.60	-0.03	-0.07	0.05

Note: Diagonal numbers are the square root of the AVE values. Off-diagonal numbers are the correlations among latent constructs.

Table C4b. Mean, Standard Deviation, and Discriminant Validity (Design)

	Mean	***SD***	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**
1. Moral belief	5.91	1.44	**0.96**																		
2. Impulsivity	3.26	1.47	-0.29	**0.86**																	
3. Risk seeking	3.17	1.50	-0.26	0.78	**0.88**																
4. Self-centeredness	2.88	1.53	-0.35	0.78	0.80	**0.89**															
5. Temper	3.20	1.63	-0.27	0.62	0.66	0.72	**0.92**														
6. Hacking self-efficacy	3.43	2.04	0.05	0.38	0.44	0.46	0.27	**0.97**													
7. Perceived certainty	5.00	1.39	0.15	0.11	0.18	0.10	0.13	-0.02	**0.85**												
8. Perceived severity	5.20	1.46	0.12	-0.06	-0.01	-0.08	0.04	-0.14	0.76	**0.94**											
9. Perceived celerity	4.79	1.45	0.01	0.01	0.06	0.07	0.17	-0.10	0.65	0.81	**0.91**										
10. Perceived extrinsic value	4.11	1.54	-0.06	0.35	0.38	0.42	0.32	0.45	-0.04	-0.09	0.01	**0.93**									
11. Perceived intrinsic value	2.75	1.93	-0.40	0.55	0.49	0.65	0.48	0.31	0.04	-0.04	0.08	0.49	**0.97**								
12. Lack of harmfulness	2.15	1.45	-0.43	0.10	0.05	0.14	0.07	-0.06	-0.05	-0.07	0.01	-0.06	0.32	**0.97**							
13. Perceived accessibility	3.95	1.88	-0.14	0.21	0.21	0.27	0.12	0.40	-0.12	-0.12	-0.06	0.40	0.40	0.14	**0.93**						
14. Perceived visibility	4.42	1.66	0.04	0.11	0.14	0.24	0.02	0.46	0.03	-0.04	-0.05	0.39	0.25	0.02	0.70	**0.94**					
15. Perceived usability	3.92	1.82	-0.13	0.21	0.25	0.30	0.11	0.47	-0.07	-0.09	0.00	0.39	0.38	0.07	0.84	0.78	**0.94**				
16. Security policies	5.29	1.31	0.26	-0.07	-0.06	-0.13	-0.03	-0.02	0.62	0.64	0.58	0.02	-0.10	-0.23	0.02	0.06	-0.01	**0.88**			
17. Computer monitoring	4.89	1.56	0.20	0.00	0.04	-0.03	0.01	-0.05	0.76	0.72	0.67	-0.01	-0.01	-0.07	-0.12	-0.01	-0.07	0.70	**0.96**		
18. SETA	4.91	1.47	0.19	0.02	0.03	0.00	0.05	0.00	0.71	0.66	0.67	0.02	0.00	-0.04	-0.13	-0.06	-0.09	0.71	0.84	**0.93**	
19. Intention	2.74	1.93	-0.48	0.48	0.46	0.56	0.43	0.20	0.14	0.04	0.18	0.45	0.78	0.34	0.37	0.23	0.33	-0.05	0.09	0.10	**0.98**

Note: Diagonal numbers are the square root of the AVE values. Off-diagonal numbers are the correlations among latent constructs.

Table C4c. Mean, Standard Deviation, and Discriminant Validity (Finance)

	Mean	*SD*	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
1. Moral beliefs	5.49	1.59	**0.97**																		
2. Impulsivity	3.30	1.44	-0.20	**0.84**																	
3. Risk seeking	3.32	1.55	-0.38	0.64	**0.88**																
4. Self-centeredness	2.96	1.42	-0.34	0.69	0.70	**0.86**															
5. Temper	3.40	1.57	-0.23	0.68	0.62	0.70	**0.89**														
6. Hacking self-efficacy	3.61	1.88	-0.19	0.45	0.33	0.43	0.45	**0.97**													
7. Perceived certainty	5.03	1.26	0.16	-0.07	-0.03	0.03	0.03	0.08	**0.86**												
8. Perceived severity	5.27	1.47	0.19	-0.26	-0.13	-0.14	-0.09	-0.02	0.72	**0.95**											
9. Perceived celerity	4.92	1.49	0.03	-0.14	0.05	0.01	-0.02	0.05	0.67	0.84	**0.93**										
10. Perceived extrinsic value	4.51	1.53	0.08	0.29	0.27	0.13	0.28	0.35	0.29	0.21	0.19	**0.93**									
11. Perceived intrinsic value	2.60	1.70	-0.57	0.53	0.64	0.68	0.52	0.41	0.04	-0.09	0.12	0.16	**0.95**								
12. Lack of harmfulness	2.19	1.14	-0.57	0.30	0.42	0.36	0.25	0.27	-0.30	-0.33	-0.17	0.02	0.58	**0.93**							
13. Perceived accessibility	3.79	1.73	-0.06	0.25	0.17	0.28	0.25	0.47	0.05	-0.06	-0.05	0.36	0.32	0.22	**0.92**						
14. Perceived visibility	4.46	1.49	-0.06	0.04	0.19	0.18	0.09	0.37	0.08	0.05	0.09	0.38	0.16	0.14	0.58	**0.94**					
15. Perceived usability	3.61	1.68	-0.23	0.27	0.38	0.38	0.34	0.42	0.08	-0.04	0.06	0.32	0.52	0.38	0.76	0.59	**0.92**				
16. Security policies	5.34	1.28	0.24	-0.19	-0.10	-0.21	-0.12	0.00	0.63	0.64	0.56	0.23	-0.13	-0.33	0.11	0.17	0.14	**0.87**			
17. Computer monitoring	4.94	1.50	0.11	-0.07	0.03	-0.12	-0.08	-0.04	0.65	0.67	0.64	0.30	0.04	-0.20	0.02	0.12	0.11	0.73	**0.93**		
18. SETA	4.83	1.61	0.16	-0.07	0.02	-0.04	-0.10	0.02	0.60	0.65	0.60	0.34	-0.01	-0.18	0.13	0.20	0.15	0.68	0.78	**0.95**	
19. Intention	2.72	1.81	-0.50	0.58	0.59	0.67	0.58	0.41	0.00	-0.18	-0.04	0.16	0.75	0.56	0.42	0.25	0.55	-0.17	-0.09	-0.10	**0.98**

Note: Diagonal numbers are the square root of the AVE values. Off-diagonal numbers are the correlations among latent constructs.

Appendix D. Multigroup Analysis of Path Models

Table D1. Multigroup Analysis of Path Models

Path	Difference in Path Coefficient (Δβ)			p Value of Difference		
	C-D	C-F	D-F	C vs. D	C vs. F	D vs. F
H1: Offender motivation → Intention	0.038	0.074	0.036	0.612	0.685	0.608
H2: Target suitability → Intention	0.235	0.082	0.154	**0.023**	0.268	0.900
H3: Capable guard. → Intention	0.154	0.147	0.301	0.941	0.074	**0.002**
H5a: Low self-control → Offender motivation	0.101	0.050	0.051	0.199	0.333	0.680
H5b: Low self-control → Suitable target	0.314	0.206	0.108	**0.024**	0.098	0.778
H6a: Hacking self-efficacy → Offender motivation	0.117	0.170	0.052	0.797	0.906	0.663
H6b: Hacking self-efficacy → Target suitability	0.204	0.151	0.052	0.929	0.851	0.344
H6c: Hacking self-efficacy → Capable guard.	0.079	0.166	0.087	0.178	0.046	0.160
H7a: Deterrence → Target suitability	0.011	0.067	0.056	0.535	0.678	0.645
H7b: Deterrence → Capable guard.	0.086	0.031	0.054	0.937	0.696	0.169
Age → Intention	0.013	0.059	0.046	0.434	0.288	0.319
Gender → Intention	0.172	0.010	0.182	0.978	0.457	**0.008**
IS Security Exp. → Intention	0.039	0.068	0.029	0.350	0.254	0.365
Employment → Intention	0.020	0.015	0.035	0.412	0.562	0.656

Note: C = Client, D = Design, F = Finance.

Bolded *p*-values are significant (< 0.05) and relate to at least one significant path.

The above table only includes those main effect paths since comparing the path coefficients of a two-way interaction term (such as moral beliefs*offender motivation) between two scenarios is equivalent of examining a three-way interaction (such as moral beliefs*offender motivation*scenario), which is hard to interpret.

Appendix E: Survey Scenarios

Stealing and Selling Client Data

Chris was a database administrator in your company. His best friend was a management consultant specializing in streamlining and cost reduction for organizational clients. This friend asked Chris if he could provide a list of suppliers or clients that do business with your company. Chris was aware that company policies prohibit disclosing client information to third parties. Since the friend worked in a different industry, i.e., not a competitor of the company, Chris wanted to help. He was able to download the information for her friend.

Stealing and Selling Product Design Data

Daniel was a senior engineer in your company. His former colleague, who quit the company and joined a competitor a few years ago, approached him and asked if he could provide information about a key part in a new product your company had developed. The former colleague promised a fully paid vacation for Daniel and his family. Daniel's family hasn't had a vacation for some time, and he really wanted to make his family happy. Daniel was able to download the information from his office computer and gave it to the former colleague.

Stealing and Selling Financial Data

Deborah worked as an executive administrative assistant to the CFO in your company. She has a college classmate who worked in a Wall Street investment firm managing a multibillion-dollar portfolio. Three days before the scheduled public release of the third-quarter earnings, Deborah got a call from the friend asking if she could provide the data to him before the public release date, and promised a significant payoff in return. She was aware that the company policies prohibit disclosing financial data to outsiders before they are publicly released. Since Deborah's husband had been laid off and had been without a job for a while, they were in financial distress. Deborah was able to locate and copy the quarterly report file and called the friend about the data after she went home that day.

About the Authors

Xin (Robert) Luo is an Endowed Regent's Professor and full professor of MIS and information assurance in the Anderson School of Management at the University of New Mexico, USA. He received his PhD in MIS from Mississippi State University, USA. He has published research papers in leading journals including *Communications of the ACM, Decision Sciences, Decision Support Systems, European Journal of Information Systems, Information & Management, Journal of the Association for Information Systems, Journal of Strategic Information Systems, Information Systems Journal,* and *IEEE Transactions on Engineering Management*, etc. He has served as an ad hoc associate editor for *MIS Quarterly* and is an associate editor for *Decision Sciences, European Journal of Information Systems, Information & Management, Electronic Commerce Research,* and *Journal of Electronic Commerce Research*. He sits on the editorial board of *Journal of the Association for Information Systems*. His research interests center around information assurance, innovative technologies for strategic decision-making, and global IT management. He is the co-editor for the *International Journal of Accounting and Information Management*.

Han Li is an associate professor of MIS and information assurance at the University of New Mexico, USA. She received her doctorate in management information systems from Oklahoma State University. She has published in *Decision Sciences, Decision Support Systems, Operations Research, European Journal of Information Systems, Information Systems Journal, European Journal of Operational Research, Journal of Organizational and End User Computing, Journal of Computer Information Systems, DataBase Management, Information Management & Computer Security, Information Systems Management* and *Journal of Information Privacy and Security*. Her current research interests include Health IT, privacy and confidentiality, data and information security and the adoption and postadoption of information technology.

Qing Hu is a professor of information systems and dean of the Koppelman School of Business at Brooklyn College, The City University of New York. He earned his MS and PhD degrees in computer information systems from the University of Miami. His research primarily focuses on organizational cybersecurity and the impact of IT on organizational strategy, culture, and performance. He has published over 140 research articles in academic journals, conferences, and books, and has been an invited speaker at universities and academic conferences around the world. He is a leading scholar in behavioral cybersecurity research, and his work has been published in premier academic journals including *MIS Quarterly, Information Systems Research, Journal of Management Information Systems, California Management Review, PLoS ONE, Decision Sciences, European Journal of Information Systems, Information Systems Journal, Information & Management,* and *IEEE Transactions on Software Engineering.*

Heng Xu is a professor of information technology and analytics in Kogod School of Business at the American University, where she also serves as the director of the Kogod Cybersecurity Governance Center. Her current research focus is on information privacy, data analytics, data ethics, and cybersecurity management. Her earlier work has received many awards, including the National Science Foundation's CAREER award in 2010, and best paper awards and nominations at various leading conferences. Her work has been published in outlets across different fields such as business, psychology, law, and human-computer interaction, including *Management Information Systems Quarterly*, *Information Systems Research*, *Journal of Management*, *Psychological Methods*, *University of Pennsylvania Journal of Constitutional Law*, *Proceedings of the ACM Conference on Human Factors in Computing Systems*, and many others.