MIS Quarterly

RESEARCH ARTICLE

A LONGITUDINAL STUDY OF UNAUTHORIZED ACCESS ATTEMPTS ON INFORMATION SYSTEMS: THE ROLE OF OPPORTUNITY CONTEXTS[1]

Jingguo Wang
Department of Information Systems and Operations Management, College of Business,
University of Texas at Arlington, Arlington, TX 76019 U.S.A. {jwang@uta.edu}

Zhe Shan
Department of Information Systems and Analytics, Farmer School of Business, Miami University,
Oxford, OH 45056 U.S.A. {jayshan@miamioh.edu}

Manish Gupta
Department of Management Science and Systems, School of Management,
State University of New York at Buffalo, Amherst, NY 14260 U.S.A. {mgupta3@buffalo.edu}

H. Raghav Rao
Department of Information Systems and Cyber Security, College of Business,
University of Texas at San Antonio, San Antonio, TX 78249 U.S.A. {hr.rao@utsa.edu}

This study investigates employee behavior of unauthorized access attempts on information systems (IS) applications in a financial institution and examines how opportunity contexts facilitate such behavior. By contextualizing multilevel criminal opportunity theory, we develop a model that considers both employee- and department-level opportunity contexts. At the employee level, we hypothesize that the scope and data value of the applications that an employee has legitimately accessed, together with the time when and location where the employee initiates access, affect the likelihood of the employee making unauthorized access attempts. At the department level, we hypothesize that department size moderates the impact of employee-level contextual variables on the likelihood of an employee making unauthorized attempts. To test these hypotheses, we collected six months of access log data from an enterprise single sign-on system of a financial institution. We find the hypothesized main effects of all employee-level contextual variables and department size are supported. In addition, department size reinforces the effects of data value, off-hour access, off-site access, and their interaction term, except for that of scope, on the outcome variable. Robustness analyses indicate that the proposed model does not align with those employees who might not know the systems well enough or who might make honest mistakes. We also discuss the theoretical and practical implications of the study.

Keywords: Information security, insider threats, multilevel criminal opportunity theory, contextualization, multilevel analysis, longitudinal data, user behavior analytics

[1]Indranil Bardhan was the accepting senior editor for this paper. Michael Chau served as the associate editor.

The appendices for this paper are located in the "Online Supplements" section of *MIS Quarterly*'s website (https://misq.org).

DOI: 10.25300/MISQ/2019/14751

Introduction

Insider threats pose significant risk to an organization's digital assets. According to the 2015 Vormetric insider threat report (Vormetric 2015), 89% of organizations surveyed believe they are at risk from insider attacks, and 55% suggest privileged users pose the greatest internal threat to corporate data. Studies in behavioral information security have explored insiders' psychological drives, including neutralization (Siponen and Vance 2010; Willison and Warkentin 2013), moral beliefs and reasoning (Myyry et al. 2009), and disgruntlement (Willison and Warkentin 2013), among others, that motivate offenses, for example, violating information systems policies or abusing IT resources (Cram et al. 2018). However, it is unclear how insider threats to digital assets eventuate from individual, unique circumstances.[2] An investigation in this regard is necessary for developing effective situational prevention mechanisms to mitigate insider threats as opportunity is more tangible than motive (Padayachee 2016; Willison and Siponen 2009).

Criminal opportunity is a function of to the amount of convergence between a motivated offender and a suitable target (Cohen and Felson 1979; Wilcox et al. 2003). The opportunity that arises in an environment is often assumed to be a necessary (if not sufficient) condition for a motivated offender (i.e., someone primed to offend) to commit an offense or crime (Cohen and Felson 1979; Hindelang et al. 1978; Wilcox et al. 2003). The absence or presence of opportunity leads to when and where a crime takes place. Understanding opportunity and its structure is critical to designing effective crime prevention mechanisms. *Criminal opportunity contexts* refer to the social, physical, individual, and environmental conditions that facilitate criminal opportunity by influencing the supply of suitable targets, ineffective guardianship, and their possible overlap, given a potential offender with criminal inclinations or motives (Wilcox et al. 2003). Adapting the opportunity structure for crime (Clarke 1995), Willison (2002) describes a conceptual model for computer input fraud, referred to as crime-specific opportunity structure. The model provides a holistic conceptualization and urges consideration of the relationships between offender, organizational contexts, requisite safeguards, and the departments responsible for them.

Recognizing the importance of opportunity in offense occurrence and the interdependence between the activities and behavior patterns of victims and the decisions and behaviors of offenders (Wilcox et al. 2003), some studies have examined how environmental settings (or opportunity contexts) influence the victimization risk of targets (Miethe and Meier 1990). In investigating the causes of cybercrime victimization, prior studies suggest that an individual's online lifestyle patterns—indicated by daily online activities or choices that provide or inhibit criminal opportunity—affect one's likelihood of becoming a victim of cybercrime (Holt and Bossler 2008). In investigating the attack proneness of information systems[3] in a financial institution, Wang, Gupta, and Rao (2015)[4] suggest that IS applications' victimization risks are significantly influenced by application characteristics reflecting target suitability and the absence or presence of guardians in surroundings.

Through a victim perspective, those studies quantify the risks for a potential target. Their findings enable the development of effective mitigation strategies that largely rely on modifying the characteristics or behavioral patterns of a target to reduce suitability for potential attacks. However, such strategies could be difficult to implement when the characteristics and/or behavioral patterns of the target, such as an IS application, are difficult to change. Furthermore, such a perspective does not provide useful direct insights regarding potential offenders' behaviors and how opportunity contexts can foster illegitimate acts. A systematic theorization and empirical validation of how opportunity contexts drive malicious acts with regard to digital assets could guide organizations on how to develop pragmatic intervention strategies to alter the behaviors of potential offenders (Padayachee 2016; Willison and Siponen 2009).

Taking the perspective of potential offenders, this study focuses on aspects of what is known in the practitioner world as user behavior analytics.[5] User behavior analytics involves the examination of historical data logs to identify anomalous patterns of behavior both by legitimate and malicious users. It is a means for organizations to counter likely digital crimes that pose risk to systems in organizations. In a corporate environment, it involves monitoring of the network, the employees, and the assets.[6] In particular, this paper investigates employee behavior of making unauthorized attempts to access applications or web resources without appropriate privileges (e.g., read, write/modify, and execution). As employees could

[2] See Appendix A for a review of relevant literature.

[3] We use the terms *information systems* and *information systems applications* interchangeably to refer to software programs designed to perform a function or suite of related functions.

[4] See Appendix B for a detailed comparison of Wang, Gupta, and Rao and the current study.

[5] http://searchsecurity.techtarget.com/definition/user-behavior-analytics-UBA

[6] https://www.securityondemand.com/news-posts/exactly-behavioral-analytics/

gain access to certain organizational data that they probably should not have, unauthorized access attempts may point to the loopholes in an organization where there is a lack of adequate policies and safeguards, and the potentially damaging consequences (Shaw et al. 1999). Thus, both the industry and academic researchers consider unauthorized access attempts as a key risk indicator of insider threats. A key aspect of corporate control and risk management strategies is to execute suspicious activity monitoring that tracks unauthorized access attempts employees make on information system applications (Davis 2010, 2011).

This study contextualizes multilevel criminal opportunity theory (Wilcox et al. 2003) to the domain of insider threats and expounds on opportunity contexts. It carries out multilevel analyses that incorporate contextual variables at both the employee and department levels to explain employees' unauthorized access attempts. Multilevel models provide a convenient analytical framework with concordance between theoretical approaches and statistical analyses for data with a hierarchical structure. At the employee level, we hypothesize that the scope and data value of the applications that an employee has legitimately accessed, together with the time when, and the location where, the employee initiated the access, affect the likelihood of unauthorized attempts occurring. At the department level, we hypothesize that department size moderates the impact of the employee-level contextual variables on the likelihood of unauthorized attempts occurring.

For hypothesis testing, we gathered application access logs spanning six months (February–July 2014) from an enterprise single sign-on system (ESSO) in a financial institution in the northeast United States. According to the results, the effects of all employee-level contextual variables and department size on the likelihood of employees having unauthorized access attempts are significant. In addition, department size moderates the effects of data value, access time, access location, and their interaction, except for the effect of scope. Robustness analyses show that the variables do not well explain unauthorized attempt behavior of employees who are new to the systems (i.e., in their first one or two months of using the system). The analyses suggest that the proposed model may be a better fit for the behavior of those employees familiar with the systems who are more likely to make rational, intentional choices in their system access rather than unintentional mistakes.

Based on a natural setting in a financial organization, this study is one of the first to systematically explore how opportunity contexts drive employee behavior toward information systems. It provides empirical evidence for the important role of opportunity contexts in understanding insider threats. While most studies of insider threats focus either on the impact of individual characteristics and organizational factors on insider behavior (Cram et al. 2018; Teodor et al. 2014) or conceptually discuss the use of situational prevention techniques in mitigating insider threats (Padayachee 2016; Willison and Siponen 2009), this study bridges the literature gap by empirically illustrating the effects of opportunity contexts on insider behavior. From a practical point of view, our study will enable security managers to understand how employee behaviors change across access contexts so that management can create a dynamic risk profile of employees without relying solely on static attributes, such as demographics and personality.[7] Moreover, nowadays more and more organizations offer employees flexible work arrangements. Therefore, as the contexts within which employee access to information systems vary, such a trend brings new challenges to information security management. A study that can offer insights on how insider threats have shifted due to this workspace change can inform the design and implementation of more effective security management practices at organizations.

Theory and Hypothesis Development

Multilevel Criminal Opportunity Theory

Stemming from rational choice assumptions, multilevel criminal opportunity theory (Cohen and Felson 1979; Hindelang et al. 1978; Wilcox et al. 2003) integrates routine activity and social disorganization theories. The theory is concerned not with criminals per se (for example, their asocial tendencies) but with how criminal opportunity contexts affect the occurrence of crime. Its fundamental premise is that opportunity contexts at both the individual and community level need to be more or less favorable for offenses to occur (Wilcox et al. 2003).[8]

Criminal opportunity exists at the intersection of motivated offenders, suitable targets, and ineffective guardianship (Cohen and Felson 1979; Hindelang et al. 1978; Wilcox et al.

[7]We thank a Vice President and Manager of Information Security at the financial institution for these comments.

[8]Multilevel criminal opportunity theory assumes criminal inclination as a given and downplays individual motivations for crimes (i.e., what drives some individuals to offend). There are no defining characteristics that distinguish those who are highly motivated and those who are not (Wilcox et al 2003). In this paper, we do not assume criminal inclinations to be universal and constant among all insiders. As reflected in our regression models, we acknowledge there may be individual differences among potential offenders.

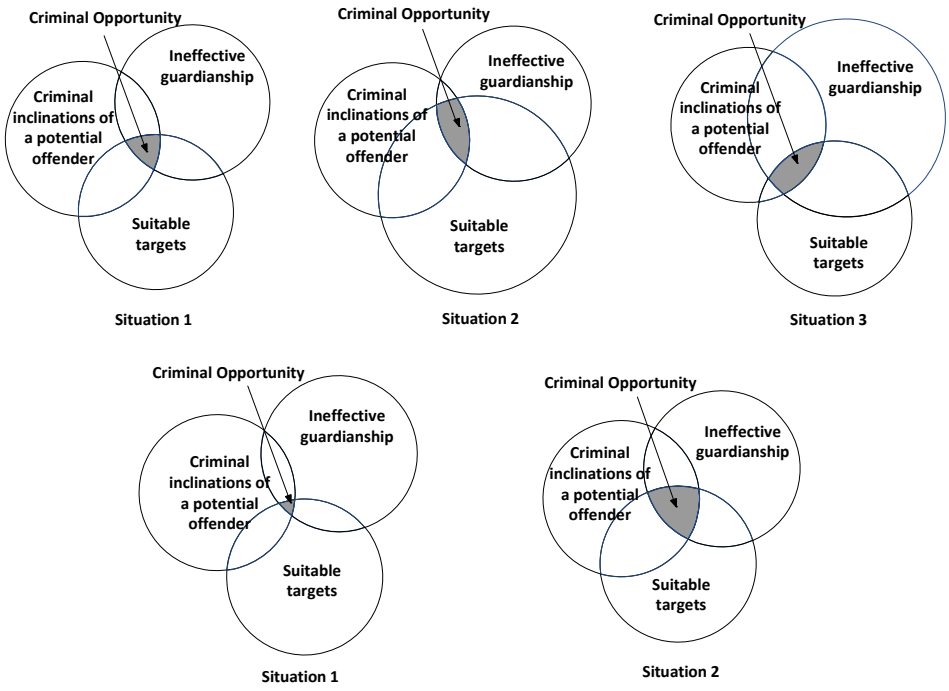


Figure 1. Varying Criminal Opportunity for a Potential Offender (Adapted from Wilcox et al. 2003)

2003). Figure 1 illustrates varying degrees of criminal opportunity given a potential offender (referred to as situations in the figure). In situations with a larger size of suitable targets (Situation 2) or ineffective guardianship (Situation 3), there is a larger convergence (compared with Situation 1). Even with the same potential offender, suitable targets, and ineffective guardianship, the amount of convergence (i.e., opportunity) may vary in different occasions (Situation 4 versus Situation 5). For instance, the larger overlap in Situation 5 versus Situation 4 could be a result of inadequate social control at the community level (Kornhauser 1978). Along these lines, multilevel criminal opportunity theory seeks to explain the likelihood of criminal acts as a function of circumstantial determinants at different levels that influence suitable targets, ineffective guardianship, and their likelihood of convergence for a given offender (Wilcox et al. 2003).

At the individual level, from the perspective of potential offenders, opportunity contexts are the factors defining their awareness of suitable targets and realization of ineffective guardianship (Wilcox et al. 2003). Individuals carry out regular activities in the environment, referred to as "action space," with which they are familiar (Horton and Reynolds 1971). Through their movements and gleaning of knowledge in the action space, potential offenders develop an "awareness space" via a process of cognitive mapping in which they classify and code the information gathered (Bernard-Butcher 1991). The awareness space includes the surrounding areas that potential offenders are aware of but are not as familiar with as the action space (Bernard-Butcher 1991). As they move in their awareness space, offenders make conscious or unconscious mental notes on the desirability of certain targets (Bernard-Butcher 1991). They search their awareness space to identify criminal opportunity and look for suitable targets (Brantingham and Brantingham 1991). With more knowledge of the environment, offenders can better estimate and minimize their risk, find where the most suitable targets are, and improve their chances of success (Van Daele and Beken 2011). In fact, offenders commit a majority of crimes in areas they visit during their routine activities (Brantingham and Brantingham 1991; Van Daele and Beken 2011). An offender's awareness space may change based on new information and as a result of searching (Andresen et al. 2016). With a larger awareness space, potential offenders have a broader target search area and are more likely to find targets in more places (Canter and Youngs 2008).

At the community level, opportunity contexts refer to the set of ambient characteristics of a community and include such constructs as aggregated target suitability (e.g., student enrollment in a school context) and aggregated capable guardianship (e.g., frequency of police patrols in a neighborhood con-

text) (Wilcox et al. 2003). As cyberspace is a different environment (Yar 2005), the opportunity for insider threats on digital assets resides in the virtual space generated by insiders' interconnection of information system applications and the traditional organizational environment consisting of the social situations in groups or departments (Willison 2006b).

Regarding the effects of community contexts, multilevel criminal opportunity theory largely draws upon social disorganization theory; it argues that the ecological characteristics of community produce social disorganization, which then gives rise to criminal acts (Kornhauser 1978; Wilcox et al. 2003). Linked to the effectiveness of social control in a community, characteristics such as size are often used to understand crime rate (Wilcox Rountree and Land 1996). Moreover, community-level factors can moderate the relationship between individual-level factors and crime (Wilcox et al. 2003). Multiple-level analyses of criminal opportunity usually emerge from the interaction among factors at individual and community levels. As opportunity contexts at different levels operate either individually or interactively, the relationship between individual-level factors and crimes is not uniform across communities. Also, the effect of individual-level target attractiveness and guardianship on victimization risk may be correlated with neighborhood socioeconomic status (Kennedy and Forde 1990).

Research Model and Hypotheses

Multilevel criminal opportunity theory provides a theoretical lens to investigate how opportunity contexts may affect employees' behavior of making unauthorized access attempts on IS applications. Following this lens, we consider opportunity contexts for unauthorized access attempts at both the employee and department levels (Table 1). Figure 2 presents the research model and hypotheses.

Employees' Behavior of Unauthorized Access Attempts

Indicators of a potential insider threat can be separated into four categories: recruitment, information collection, information transmittal, and general suspicious behavior (Center for Development of Security Excellence 2018). For the purposes of this paper, we focus on the categories of information collection and general suspicious behavior. Indicators of information collection include acquiring access to automated information systems without authorization and seeking to obtain access to critical assets inconsistent with present duty requirements. Indicators regarding general suspicious behavior include attempting to expand access to critical assets by repeatedly volunteering for assignments or duties beyond the normal scope of responsibilities and performing repeated or unrequired work outside of normal duty hours, especially unaccompanied. Recruitment is a human resources issue and information transmission is in the context of exfiltration of information from inside the organization to outside; both are beyond the scope of this paper.

Thus, being able to track insiders to understand their levels of individual risk would help in risk assessment across each insider's activities. The solution is user activity monitoring (Velez 2015), which looks at behavior and spots trends. This allows an analyst to cut through the large number of alerts, determine the situation, and take action to stop an insider threat. In this study, we track employees' unauthorized attempts to access applications or web resources without the appropriate privileges (e.g., read, write/modify, and execution). These are captured by the management consoles of the security logs that watch for failed use of privileges, failed attempts to access and modify files that an employee should not have access to, unauthorized attempts to upload files to a directory containing executable files, etc.[9] For an insider, unauthorized computer access is usually a process of trial and error (Dunne 1994).

We consider insiders' behavior of repeated attempts to access information for which they do not have authorization as the outcome variable. This behavior has been seen to be inherently destructive and wasteful (Dunne 1994). Information security managers often hope that effective deterrents for such behavior are in place. We anticipate that the results will help to develop antidotal deterrent mechanisms that can be used by information security managers in the context of discouraging unauthorized access of information assets as well as assisting them with designing response mechanisms to mitigate risks from such attempts. The findings could be used to develop effective ways of reducing unauthorized access to critical digital assets.

While unauthorized access attempts cannot be labeled as offenses or crimes in a rigorous sense, in the words of the IT security manager of the financial institution, "they are symptoms of noncompliance with rules and signals of potential crimes." We believe such behavior is consistent with the assumptions needed for the theory. First, employees in organizations such as financial institutions rely on information systems to carry out tasks on a daily basis. In other words, accessing information systems is part of their daily routine activities. Second, like traditional crimes and offenses that deviate from one's normal activities, unauthorized access at-

[9] http://www.nsi.bg/nrnm/Help/iisHelp/iis/htm/core/iidetsc.htm

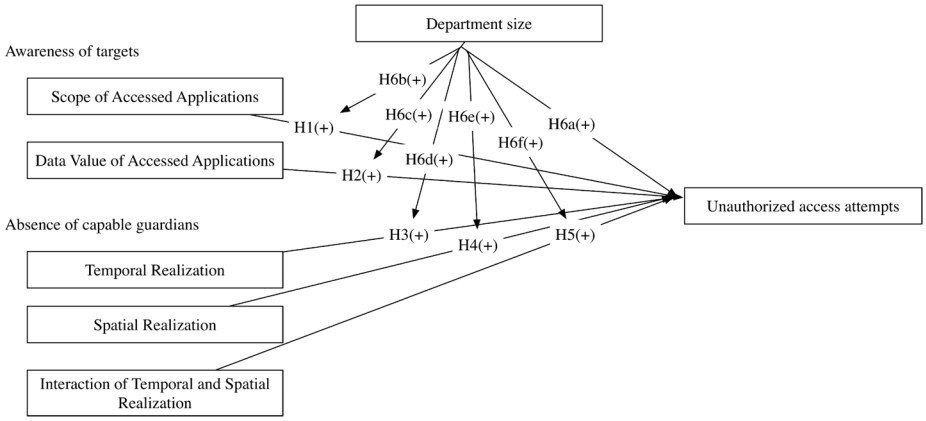


Figure 2. Research Model and Hypotheses

tempts deviate from one's daily job routines in which only authorized applications are needed to execute job tasks (Cummings et al. 2012). Because unauthorized access attempts pose significant threats to information security, they are regarded as red flags and prohibited by organizational policies (Davis 2010, 2011). Third, while unintentional attempts may not be a result of rational choices, intentional attempts, whether malicious or not, are based on an insider's rational consideration of the tradeoff between risks and benefits (Loch et al. 1992; Willison and Warkentin 2013); that is, being caught may lead to serious consequences and/or punishment, yet successful access could be rewarded with immediate gratification (e.g., satisfying one's curiosity) or potential long-term benefits (e.g., financial gains or competitive advantages) (Shaw et al. 1999).

In other words, intentional unauthorized access attempts could be the result of insiders' rational choices, as multilevel criminal opportunity theory assumes offenses or crimes to be. In fact, Silowash et al. (2012) define a malicious insider as someone who

> has or had authorized access to an organization's network, system, or data … [and] has *intentionally exceeded* or intentionally used that access in a manner that negatively affected the … organization's information or information systems (p. 3; emphasis added).

Further, Costa et al. (2016, p. 1) have pointed out that "once suspected malicious activity has been identified, organizations perform forensic investigations of affected assets."[10] We reached out to an IT security manager in the financial institution who confirmed that when there is suspicion of nefarious activity, the application access logs are examined and unauthorized access attempts are given close attention. Employees' system access logs are retained for an extensive time period for the purposes of regulation compliance, forensics examination, and internal investigations. In addition, such logs are used by a centralized log management system as a major data source for investigation of potential malicious activities.

From Opportunity Contexts to Unauthorized Access Attempts

As suggested by criminal opportunity theory, at the employee level, we focus on the opportunity contexts that capture employees' awareness of targets and their realization of ineffective guardianship. We capture employees' knowledge and awareness space of the existence and whereabouts of applications in terms of two dimensions: scope and data value of accessed applications. Scope of accessed applications refers to the range of IS applications that are legitimately executed by an employee. Data value of accessed applications refers to the worth of the data possessed by the IS applications that are legitimately executed by an employee. Given that the basic access control policy is on a need-to-know basis, these two dimensions characterize an employee's legitimate systems behavior confined within his or her daily tasks (that may change from time to time). As discussed in detail in the following subsection, we hypothesize that when employees have broader accesses to information applications, it is more likely for them to make unauthorized access attempts (H1); and that when employees have accesses to more valuable data, it is more likely for them to make unauthorized access attempts (H2).

[10]We thank an anonymous referee for alerting us to this citation.

Table 1. An Extension of Multilevel Criminal Opportunity Theory to Insider Threats

Theoretical Framework		Construct	Definition
Offenses (DV)		Unauthorized access attempts	The likelihood of an employee making repeated access attempts on an application for which he or she has no privileges.
Employee Level	Awareness of Targets	Scope of accessed applications	The range of information systems applications that are legitimately executed by an employee.
		Data value of accessed applications	The worth of the data possessed by the information systems applications that are legitimately executed by an employee.
	Realization of Ineffective Guardianship	Temporal realization	The likelihood of having ineffective guardianship at the times when an employee initiates access.
		Spatial realization	The likelihood of having ineffective guardianship at the locations where an employee initiates access.
Department Level	Community Context	Department size	The size of the department that an employee belongs to.

We capture employees' realization of the absence or presence of effective guardianship via two key aspects of access contexts: the temporal characteristic of when (termed as temporal realization) and the spatial characteristic of where (termed as spatial realization) an employee has initiated his or her application access. Temporal realization of ineffective guardianship refers to the likelihood of having ineffective guardianship at the times when an employee initiates access. Spatial realization of ineffective guardianship refers to the likelihood of having ineffective guardianship at the locations where an employee initiates access. We hypothesize that (1) when employees access at a time when there is more likely to be ineffective guardianship, they are more likely to make unauthorized attempts (H3); (2) when employees access from locations where there is more likely to be ineffective guardianship, they are more likely to make unauthorized attempts (H4); (3) temporal and spatial realization of ineffective guardianship reinforces each other's impact on unauthorized access attempts (H5).

At the community level, we focus on the effect of department size. In the pursuit of IS security, departments typically develop and implement plans, policies, etc., to ensure the security of information resources, along with user training programs and governance structures to promote compliance (Warkentin and Johnston 2008). As each department has unique characteristics beyond individual characteristics of group members, group characteristics need to be examined independently (Suleiman and Watson 2008). In particular, group size has been used to explain different social phenomena in technology (Alnuaimi et al. 2010; Suleiman and Watson 2008), for example, social loafing in technology-supported teams. Similarly, in the management and psychology literature, unit size has been one of the most studied group characteristics (Thomas and Fink 1963). Larger unit size has been found to be associated with lower levels of job satisfaction and group cohesiveness (Muchinsky and Tuttle 1979; Shaw 1981). However, this attribute has been measured in different ways, such as the number of employees, sales, market cap, and the number of installed IT platforms (Kotulic and Clark 2004), among which the number of employees, as operationalized in this paper, is the most popular (Raymond 1990; Thomas and Fink 1963). We hypothesize that department size is positively correlated to unauthorized access attempts (H6a). Moreover, it reinforces the effects of employee-level contextual variables (H6b–H6f).

Awareness of Target: Scope and Data Value of Accessed Applications

While knowledge about applications could be beneficial to performing daily duties, it may also enable potential offenders to become aware of the existence and whereabouts of potential targets (Willison 2000,2002). Indeed, through legitimate system activities, potential offenders develop an awareness space that they can explore and examine to gather information about risk factors as well as which applications may possibly be exploited (Willison 2006b). According to a CERT report on insider theft in the United States (Spooner et al. 2013), those who committed insider theft crimes often had some level of authorized access to the information they stole.

Most applications connect with each other in various ways. When employees have greater scope of access to several applications, they may have more knowledge about the systems as a whole. In other words, insiders would develop a larger awareness space and cognitive map with broader

access to applications within the organization. A larger awareness space and cognitive map facilitates a broader search that may help identify more suitable application targets for unauthorized access.

Further, data and information of applications carries different commercial values and may relate to trade secrets, sales and marketing plans, new product plans, customer and supplier information, and other proprietary data (MaRS 2009). Data and information of high commercial value has become the prime target for cyber thieves (Panda Security 2012; Ponemon 2006). In a typical case of insider threats, an insider could steal valuable information for personal advantage or financial gain (Sarkar 2010). Employees often possess different privileges to the applications and data that are relevant to their daily work based on the need-to-know security principle. For instance, giving read (but not write) permission to a module in a confidential application may prevent an employee from modifying the relevant data. As employees have access to more valuable data in their daily tasks, the targets they become awar of may be more suitable. Thus, the temptation and benefits of accessing beyond their privileges could be higher (Winkler and Gomes 2016). Further awareness of the value of application data may also make it easier for an employee to gain the data exceeding his or her privileges for personal benefits or malicious purposes in a stealthier manner and perhaps even under "a legitimate shield." Therefore, we propose that

H1: When employees have greater scope of access to information applications, they are more likely to make unauthorized access attempts.

H2: When employees have access to more valuable data, they are more likely to make unauthorized access attempts.

Realization of Ineffective Guardianship: Temporal Realization, Spatial Realization, and Their Interactions

Information system applications often include protective measures to deter and prevent unauthorized access (Wang, Gupta and Rao 2015). Solutions ranging from firewalls, intrusion detection systems, and antivirus software serve as technological guardians, while network administrators, application administrators, application auditors, and security staff act as social guardians (Yar 2005). However, individual activity patterns in terms of locations and times of access make employees more or less proximate or exposed to capable guardians in individual-level contexts (Wilcox et al. 2003). When employees access at the times (for example, off-hours) when and locations (for example, off-site) where there is not likely to have effective guardianship, their chances of being detected and caught will be lower, given that protection measures, such as network administrators and application auditors watching in real time, are less effective in deterring and preventing unauthorized access (Straub and Welke 1998; Willison 2006a). Moreover, fewer social guardians such as coworkers would be nearby, significantly decreasing the chance of any offense being witnessed (Hamblen 2011). Therefore, we propose that

H3: When employees access at times when guardianship is ineffective, they are more likely to make unauthorized attempts.

H4: When employees access from locations where guardianship is ineffective, they are more likely to make unauthorized attempts.

When the convergence of the times when and the locations where guardianship is ineffective create a vacuum of both formal (such as organizational surveillance and system administrative personnel) and informal (such as coworkers) guardianship, companies have greater difficulty monitoring insider activities.[11] Therefore, being discovered while engaging in illegitimate activities in such situations would be less of a concern for the insider (Groff 2007). In other words, the combination of the two situations (times and locations of access) creates a guardian-abated environment and thus amplifies criminal opportunity (Wilcox et al. 2003). Based on interviews with security specialists, Munshi (2013, p. 198) stated that

> insider threats increased by increased attempts to access confidential files/folders from outside the department … increased use of, for example, remote access software, during off business hours.

Elmrabit et al. (2015) also show that in general, insider IT saboteurs are often employees working at the times and locations where there is an absence of effective guardianship. Information security think tanks, such as FS-ISAC,[12] have recommended monitoring remote user accounts for login abnormalities, such as logins during non-normal working hours (FS-ISAC 2016). Therefore, we propose that

[11]https://www.observeit.com/blog/5-things-you-should-know-about-insider-threats/

[12]The Financial Services Information Sharing and Analysis Center (https://www.fsisac.com/).

H5: The interaction between temporal and spatial realization is positively associated with unauthorized access attempts.

Community-Level Opportunity: Department Size

We argue that insiders in a larger department are more likely to take advantage of the opportunities present in their environment for various reasons. For one, compared with a small department, a large one is more likely to experience problems with communication, impersonalization, and bureaucratization (Terborg and Lee 1984). Also, it may exhibit less effective supervision and control (Mullen et al. 1989); thus, opportunities for insider threats may be more likely to be exploited (Willison 2002). In addition, people learn through observing others' behavior, attitudes, and outcomes (Bandura 1977). Larger departments may allow for more information sharing and learning (due to exposure to and interaction with more people) about business processes and supporting systems, so employees in larger departments tend to have wider knowledge of system access. In other words, they are likely to form a larger awareness space and be able to find more suitable targets. Finally, given that more employees have similar roles and types of access in a larger department, some may believe that in the case of a realized data breach, the chances of being detected or held accountable are relatively low. Therefore, we propose that

H6a: Employees from larger departments are more likely to have higher unauthorized access attempts.

H6b: Department size reinforces the effect of scope of accessed applications on unauthorized access attempts. In other words, scope of accessed applications is more likely to lead to unauthorized access attempts for employees in a larger department.

H6c: Department size reinforces the effect of data value of accessed applications on unauthorized access attempts. In other words, data value of accessed applications is more likely to lead to unauthorized access attempts for employees in a larger department.

H6d: Department size reinforces the effect of temporal realization on unauthorized access attempts. In other words, temporal realization is more likely to lead to unauthorized access attempts for employees in a larger department.

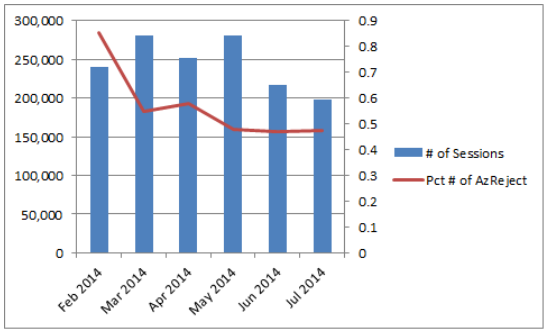
H6e: Department size reinforces the effect of spatial realization on unauthorized access attempts. In other words, spatial realization is more likely to lead to unauthorized access attempts for employees in a larger department.

H6f: Department size reinforces the effect of the interaction of temporal and spatial realization on unauthorized access attempts. In other words, the interaction of temporal and spatial realization is more likely to lead to unauthorized access attempts for employees in a larger department.

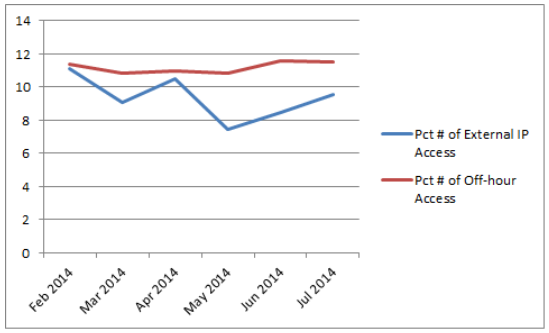
Data and Measurement

We collected access log data from an enterprise single sign-on (ESSO) system at a financial institution in the northeast United States. The ESSO system integrates 34 applications within the organization and allows employees to traverse through different applications without repeated sign-in. In other words, users can attempt to access integrated applications without reauthentication. The ESSO system tracks users' system logins and application access. It logs authentication acceptances (or AuthAccept) and authentication rejections (or AuthReject) for successful and failed user logins (for example, incorrect password). The ESSO system further tracks user access behavior after a successful login: An authorization acceptance (or AzAccept) is logged if the user attempts to access an application (or a URL link) with granted privileges, and an authorization rejection (or AzReject) is logged if the user attempts to access an application or resource without granted privileges. Each record in the ESSO log contains a user ID, timestamp, the application or resource the user requested, and the result of an event (success or fail).

We aggregated log entries into access sessions for further analyses. Sessions have been a popular unit of analysis widely used in web analytics as a metric of website usage (Weischedel and Huizingh 2006) as well as for operational analytics, including characterizing search behavior (Wang, Xiao, and Rao 2015) and identifying anomalies in networking (Meiss et al. 2009). A session is defined as a sequence of URL requests from a uniquely identified user that expired after a certain amount of inactivity. To complete a certain task, users normally visit a number of URL links in a consecutive manner. Because the standard time-out setting of the ESSO system is 20 minutes, we used the time-out method as in prior studies (Wang, Xiao, and Rao 2015) and consider that a user starts a new session after being inactive for at least 20 minutes. In other words, if two log



(a) Number of Sessions and Percentage (%) of AzReject



(b) Percentage (%) of Sessions from External IP and at Off-Hours

Figure 3. Access Sessions

entries occurred within 20 minutes, they belong to the same session of a user; otherwise, they belong to different sessions.

The dataset includes a total of 30,571,388 relevant entries over the course of six months from February to July 2014. In total, we detected 1,469,014 sessions. Figure 3(a) shows the distribution and the percentages of those sessions containing authorization rejections (i.e., AzReject). Next, for each employee in a given month, we counted their total sessions (*TotalSess)* and the number of sessions with unauthorized access attempts (*RejSess*). One concern regarding unauthorized access attempts observed in the log is that those may be unintentional mistakes due to employees being unfamiliar with their systems and privileges. To alleviate this concern and exclude those unauthorized attempts as being honest mistakes as much as possible in the analyses, we implemented a number of efforts as follows:

(1) We included only the employees present in all six months. Because new employees, or employees who do not use the applications frequently, may be more likely to make unintentional mistakes (rather than deliberate attempts) due to their unfamiliarity with the systems and their privileges, we consider that their behaviors are less likely to satisfy the rational choice assumptions needed to apply multilevel criminal opportunity theory. For the same reason, we excluded employees who had very few records of system access (i.e., an average total number of sessions is less than five per month).

(2) To further exclude those attempts that are more likely the result of honest mistakes, we calculated the dependent variable by only considering repeated unauthorized attempts. In other words, in a given month we did not consider such an attempt from an the employee who tried to access an application without authorization only once.

(3) For the sake of model identifiability and to ensure sufficient numbers of observations within each group and the numbers of groups, we excluded those departments with less than 10 employees.

(4) We controlled for the average number of *Active Days* per month of a user. Generally speaking, frequent users are more familiar with their privileges or applications (Chehimi 2013; CPPA 2015; Warkentin et al. 1997) and therefore less likely to make accidental attempts (Magklaras and Furnell 2001).

For the scope of accessed applications, we counted the number of distinct applications an employee accessed legitimately in each month. For data value of accessed applications, we first collected the confidentiality rating of the data processed by each application and calculated the average of those applications an employee had accessed legitimately in that month. To measure temporal and spatial realization of ineffective guardianship, we first labeled the sessions as off-hour access if initiated at a time outside of regular working hours of the institution (i.e., between 7:00 a.m. and 7:00 p.m.) on a working day or at any time on weekends and public holidays, given that the institution has a very low percentage of users whose regular job is offshore or outside of this interval. Also, we labeled sessions as off-site access if the initiating IP address was in the Demilitarized Zone. We then calculated the percentage of off-hour access and the percentage of off-site access per month for temporal and spatial realization of ineffective guardianship. As expected, during off hours or at off sites, protection measures such as network administrators and application auditors watching over them in real time are less effective in deterring and preventing unauthorized access (Straub and Welke 1998; Willison 2006a). Moreover, fewer coworkers would be present, significantly decreasing the chance of any offense being witnessed (Ham-

Table 2. Measurement Operationalization

Construct	Operationalization
Unauthorized access attempts	Percentage of access sessions with repeated unauthorized access attempts that an employee had in a time period. In other words, in our operationalization, we did not consider such an attempt if the employee tried to access an application without authorization only once in a time period.
Scope of accessed applications	Number of applications that an employee accessed legitimately in a time period.
Data value of accessed applications	Average of the confidentiality ratings of the data processed by the applications that an employee accessed legitimately in a time period.
Temporal Realization	Percentage of access sessions that an employee initiated at a time outside of the regular working hours of the institution in a time period.
Spatial Realization	Percentage of access sessions that an employee initiated from an external IP address in a time period.
Department size	Average number of employees of a department that an employee belonged to across six months.

blen 2011). Figure 3(b) shows both plots, which remain stable across the six months. As for the size of a department, we measured it by the average number of distinct users across six months. Table 2 summarizes the operationalization.

The final dataset includes a total number of 51,348 records with 8,588 users from 56 departments. The average number of employees in a department is 152.821 with a standard deviation of 444.666. We used the percentage of sessions with unauthorized attempts as the dependent variable. This is calculated as the ratio between the number of the sessions with authorization rejection and the total number of the sessions of an employee in a given month (i.e., *RejPCNT = RejSess/TotalSess*100*). Table 3 provides the descriptive statistics of the metrics, and Table 4 shows the correlations among those variables. Because the regression models to be fitted involve interaction terms, we centered all independent variables with their means before performing regression analyses to ensure they had meaningful zero values for an appropriate interpretation of the main effects (Gelman and Hill 2007; Hox 2002; Wang et al. 2011). Such a mean-centered model is statistically equivalent to the model with original measures (Wang et al. 2011). Department size was entered into the regressions after log transformation to reduce its skewness (Gelman and Hill 2007).

Data Analysis and Results

The dataset has a hierarchical structure in which an employee was observed over multiple months, and each employee belonged to a department. An employee's behavior observed at multiple time points may be correlated with and driven by the same individual characteristics as opposed to contextual variables. Similarly, the behavior of employees from the same department may be driven by department characteristics.

Using a multilevel model for such a dataset offers a number of advantages (Bryk and Raudenbush 1992; Hox 2002; Wang et al. 2011). First, it allows us to examine the effects of contextual variables at different levels simultaneously. It therefore avoids the Robinson effect, a phenomenon arising within traditional methods wherein research tends to use aggregated data to draw statistical inferences at the individual level. Second, a multilevel model can account for within-group observation dependence. From a statistical point of view, by considering the hierarchical structure of the data, multilevel models provide less biased and more statistically efficient estimates of regression coefficients than the traditional ones obtained by ignoring the hierarchical structure in the data. The estimates of standard errors, confidence intervals, and significance tests generally are more "conservative." Third, the multilevel model allows for the introduction of random coefficients, hence, the model takes account of the heterogeneity of relationships and allows the effects of individual-level contextual variables to vary across employees and departments. The model also allows examination of the extent to which the variation in effects of these variables is accounted for by department size. This fits the research model conceptualization (Figure 2). Fourth, given the field observation data in this study, the number of observed months varies across employees and the number of employees differs across departments; multilevel modeling is an effective method for analyzing such data.

Table 3. Descriptive Statistics (n = 51,348)

	Mean	Standard Deviation	Min	Max
Total sessions in a month (*TotalSess*)	25.147	31.008	1	338
Percentage of sessions with rejections in a month (*RejPCNT*)	.506	3.822	0	100
# Apps accessed in a month (*Apps*)	2.845	1.285	1	9
Confidentiality of applications accessed in a month (*Conf*)	3.142	0.744	1	5
Proportion of accesses initiated at off hours in a month (*Off-hour*)	.096	.158	0	1
Proportion of accesses initiated from off sites in a month (*Off-site*)	.116	.238	0	1

Table 4. Correlation Coefficients

	TotalSess	RejPCNT	Apps	Conf	Off-hour	Off-site
TotalSess	–	-.019***	.331***	.042***	.071***	-.095***
RejPCNT	–	–	.011***	-.051***	.032*	.117***
Apps	–	–	–	.003***	-.077***	-.081***
Conf	–	–	–	–	-.065***	-.412***
Off-hour	–	–	–	–	–	.107***
Off-site	–	–	–	–	–	–

***< .001; **< 0.01; *< 0.05; ^< 0.1

Model Specification

To test our hypotheses, we specified a random-coefficient model with three levels. A random-coefficient model not only allows the impacts of $Apps_{ijt}$, $Conf_{ijt}$, $Offhour_{ijt}$, $Offsite_{ijt}$, and $Offhour_{ijt}$*$Offsite_{ijt}$ to be heterogeneous across employees and departments, but also enables us to explore the interactions among the variables at the different levels. Let $RejPCNT_{ijt}$ denote the percentage of sessions with unauthorized access attempts that employee i from department j has in month t. We first have the level-1 equation:

$$\begin{aligned} \text{RejPCNT}_{ijt} = {} & \beta_{0i(j)} + \beta_{1i(j)}Apps_{ijt} + \beta_{2i(j)}Conf_{ijt} + \\ & \beta_{3i(j)}Offhour_{ijt} + \beta_{4i(j)}Offsite_{ijt} + \\ & \beta_{5i(j)}Offhour_{ijt}*Offsite_{ijt} + T_i + e_{ijt} \end{aligned} \quad (1)$$

where T_t is the fixed-effects term for month t. The level-1 error term e_{ijt} is independent and identically distributed (i.i.d.) following a normal distribution with a mean of 0 and a standard deviation of σ_e. The equation considers the level-1 intercept $\beta_{0i(j)}$ and the slope $\beta_{ki(j)}$ (including $\beta_{1i(j)}$ for $Apps_{ijt}$, $\beta_{2i(j)}$ for $Conf_{ijt}$, β_{3i} for $Offhour_{ijt}$, $\beta_{4i(j)}$ for $Offsite_{ijt}$, $\beta_{5i(j)}$ for $Offhour_{ijt}$ *$Offsite_{ijt}$) to be random coefficients and vary across employees.

Therefore, we have the level-2 (i.e., employee level) equations:

$$\begin{aligned} \beta_{0i(j)} &= \Gamma_{0j} + \delta ActiveDays_i + u_{0ij} \\ \beta_{ki(j)} &= \gamma_{kj} + u_{kij} \end{aligned} \quad (2)$$

where $ActiveDays_i$ (i.e., employee i's average active days per month) is a control variable with a fixed effect (δ) to be estimated for the intercept β_{0i}. The equation γ_{kj} (k = 0, 1, 2, 3,4, 5) is the average of the slopes in department j. The level-2 residuals u_{kij} (k = 0, 1, 2, 3, 4, 5) represent how much the i^{th} employee deviates from his or her departmental average; u_{kij} is i.i.d. following a normal distribution with a mean of 0 and a standard deviation of σ_{uk}. The level-2 equations capture employees' unobserved heterogeneity in criminal inclinations by allowing the coefficients to vary from employee to employee.

At level three (i.e., the department level), we consider that γ_{kj}(k = 0, 1, 2, 3, 4, 5) is conditional on department size. We have the level-3 equation:

$$\gamma_{kj} = \theta_{k0} + \theta_{k1}\log(DeptSize_j) + w_{kj} \quad (3)$$

where θ_{k0} (k = 0, 1, 2, 3, 4, 5) represents the average effect across departments, and θ_{k1} (k = 0, 1, 2, 3, 4, 5) represents the marginal effect of department size. And the level-3 residual w_{kj} (k = 0, 1, 2, 3, 4, 5) represents how much a department j deviates from an average effect that is a function of department size; w_{kj} is i.i.d. following a normal distribution with a mean of 0 and a standard deviation of σ_{wk}. The level-3 equation captures departmental unobserved heterogeneity by allowing the coefficients vary from department to department, conditioning on its size.

Combining level-1, level-2, and level-3 equations, we have the reduced model, that is, the single equation version of the multilevel model:

$$\begin{aligned}\text{RejPCNT}_{ijt} &= \theta_{00} + \theta_{10}Apps_{ijt} + \theta_{20}Conf_{ijt} + \theta_{30}Offhour_{ijt} \\ &+ \theta_{40}Offsite_{ijt} + \theta_{50}Offhour_{ijt} * Offsite_{ijt} + \theta_{01}\log\left(DeptSize_j\right) \\ &+ \theta_{11}Apps_{ijt} * \log\left(DeptSize_j\right) + \theta_{21}Conf_{ijt} * \log\left(DeptSize_j\right) \\ &+ \theta_{31}Ofhour_{ijt} * \log\left(DeptSize_j\right) + \theta_{41}Offsite_{ijt} * \log\left(DeptSize_j\right) \\ &+ \theta_{51}Offhour_{ijt} * Offsite_{ijt} * \log\left(DeptSize_j\right) + u_{0ij} + u_{1ij}Apps_{ijt} \\ &+ u_{2ij}Conf_{ijt} + u_{3ij}Offhour_{ijt} + u_{4ij}Offsite_{ijt} + \\ &u_{5ij}Offhour_{ijt} * Offsite_{ijt} + w_{0j} + w_{1j}Apps_{ijt} + w_{2j}Conf_{ijt} \\ &+ w_{3j}Offhour_{ijt} + w_{4j}Offsite_{ijt} + w_{5j}Offhour_{ijt} * Offsite_{ijt} \\ &+ \delta ActiveDays + T_i + e_{ijt}\end{aligned} \quad (4)$$

In this model, the fixed effects to be estimated include T_i, θ_{k0} and θ_{k1} (k = 0, 1, 2, 3, 4, 5), and d. The random effects to be estimated are the variances of the residuals, that is, e_{ijt}, u_{kij} (k = 0, 1, 2, 3, 4, 5), and w_{kj} (k = 0, 1, 2, 3, 4, 5). The combined model has a composite error structure with 13 terms.

We used the HPMIXED procedure in SAS to estimate all models. Designed for models involving a large number of fixed effects, random effects, and/or observations, the procedure is optimized with a number of specialized high-performance techniques. The procedure uses the restricted maximum likelihood (REML) method (Patterson and Thompson 1971). Compared with the full maximum likelihood method, REML estimates have less bias and lead to better estimates, especially when the number of groups is small (Bryk and Raudenbush 1992). However, with REML, the deviance statistics can only be used to examine the importance of random effects by comparing two models whose specifications differ only in their variance components. In addition, the procedure does not estimate the standard deviation of error variance.

Estimation Results

We first analyzed intra-class correlations (ICCs) at three levels: within employee (i.e., between months), between employees, and between departments. ICCs indicate the proportion of variance at different levels and reflect both within-group homogeneity and between-group heterogeneity (Shrout and Fleiss 1979). We relied on an intercept-only regression model (or an empty model) to calculate ICCs (Hox 2002) specified as

$$\begin{aligned}\text{RejPCNT}_{ijt} &= \beta_{0i(j)} + e_{ijt} \\ \beta_{0i(j)} &= \gamma_{0i} + u_{0ij} \\ \gamma_{0i} &= \theta_{00} + w_{0j}\end{aligned} \quad (5)$$

Its single-equation version is

$$\text{RejPCNT}_{ijt} = \theta_{00} + w_{0j} + u_{0ij} + e_{ijt} \quad (6)$$

We show the ICC for each level as below:

$$\begin{aligned}r_{within\ employee} &= \frac{\sigma_e^2}{\sigma_e^2 + \sigma_{u0}^2 + \sigma_{w0}^2} = \frac{11.605}{11.605 + 2.913 + 0.157} = .791 \\ r_{between\ employee} &= \frac{\sigma_{u0}^2}{\sigma_e^2 + \sigma_{u0}^2 + \sigma_{w0}^2} = \frac{2.913}{11.605 + 2.913 + 0.157} = .198 \\ r_{between\ department} &= \frac{\sigma_{w0}^2}{\sigma_e^2 + \sigma_{u0}^2 + \sigma_{w0}^2} = \frac{0.157}{11.605 + 2.913 + 0.157} = .011\end{aligned} \quad (7)$$

The results suggest that 79.1% of the total variance in $RejPCNT_{ijt}$ is within-employee (or between-month) variance, 19.8% is between-employee variance,[13] and 1.1% is between-department variance.

Table 5 summarizes the converged results of the model. As we can see, the fixed effects of *apps*, *off-hour accesses, conf, off-site accesses*, and *log(DeptSize)* all significantly support H1, H2, H3, H4, and H5(a). The cross-level interaction terms are significant, except *Apps*Log(DeptSize)*, therefore supporting H6(c), H6(d) H6(e), and H6(f), but not H6(b). We also see that *ActiveDays* negatively impacts unauthorized attempts, indicating that more active users are less likely to make unauthorized attempts. The model explains 52.3% within employee variance (i.e., level-1 residual variance), 34.2% between employee variance (i.e., level-2 residual variance), and 70.1% between department variance (i.e., level-3 residual variance).[14]

[13] Another way to calculate it is to add both variance components for employees and departments in the numerator of the equation (Hox 2002), which can be interpreted as the expected correlation between two randomly chosen employees within the same department. The value is not much different from the one we have reported.

[14] It is calculated based on the proportion of variance explained suggested in Raudenbush and Bryk (2002): for σ_e^2, $\sigma_{\mu 0}^2$, σ_{w0}^2 at different levels:

$$\frac{\sigma^2(Empty\ Model) - \sigma^2(Full\ Model)}{\sigma^2(Empty\ Model)} = 100\%$$

Table 5. Percentage of Sessions with Unauthorized Attempts in a Month: Three-level Models (n = 51,348)

Model Parameters	Estimated Fixed Effects	Estimated Variance of Random Components	
Month Fixed Effect	Included	Residual (σ_e^2)	5.532
Intercept	Included	*Employee-Level Variance*	
Apps	0.112**	Intercept (σ_{u0}^2)	1.917
Conf	0.064*	Apps (σ_{u1}^2)	0.104
Off-hour	1.770***	Conf (σ_{u2}^2)	0.785
Off-site	5.163***	Off-hour (σ_{u3}^2)	9.595
Off-hour*Off-site	16.635***	Off-site (σ_{u4}^2)	137.580
Log(DeptSize)	0.084*	Off-hour*Off-site (σ_{u5}^2)	1480.130
Apps* Log(DeptSize)	0.023	*Department-Level Variance*	
Conf * Log(DeptSize)	0.058**	Intercept (σ_{w0}^2)	0.047
Off-hour * Log(DeptSize)	0.888***	Apps (σ_{w1}^2)	0.018
Off-site * Log(DeptSize)	0.882**	Conf (σ_{w2}^2)	0.003
Off-hour * Off-site * Log(DeptSize)	7.186***	Off-hour (σ_{w3}^2)	0.876
ActiveDays	-0.042***	Off-site (σ_{w4}^2)	3.717
MODEL FIT		Off-hour*Off-site (σ_{w5}^2)	38.534
Deviance	257667		
AIC	257693		

***< .001; **< 0.01; *< 0.05

Robustness Analyses

We employed the same process described above and estimated the two-level models without including the random components at the department level or w_{kj}. We obtained similar results as in Table 5, but all three-level models have smaller deviance and AIC as compared with their corresponding two-level models. Chi-square tests indicate the three-level models provide a significantly better fit with the data ($p < 0.001$) than the corresponding two-level models, thus justifying the use of three-level models for data analysis.

Multilevel criminal opportunity theory has stemmed from rational choice assumptions. If unauthorized access attempts are honest mistakes and not the result of rational choices, then the model may not explain such attempts well.[15] Considering that new users might be more likely to make honest mistakes, we verify this conjecture based on the behavior of new employees who joined the institution in March 2014 or later. We estimated the models based on the new employees' behavior in their first month and in their first two months separately. Table 6 summarizes the results. As new employees have only limited observations (i.e., one for first month, or two for the first and second months) in the data set, we therefore omitted the employee level but include the department level in this regression. For new employees' first-month behavior, only *off-site* is significant. For new employees' first two months, *off-site* and *off-hour*off-site* are marginally significant. These results are very different from those in Table 5. Therefore, we conclude that the proposed model does not sufficiently explain new employees' unauthorized access attempts. This could be due to the fact that new employees' unauthorized access attempts behavior (honest mistakes) are not driven by their rational choice, the assumption behind the multilevel criminal opportunity theory.

Another concern is that the results could be driven by reverse causality (or simultaneity bias). Offenders who want illegitimate access may choose to work at off sites and/or at off hours. In other words, rational choices guide motivated offenders to work at off sites and/or at off hours.[16] To address this issue, we followed prior studies (Steele et al. 2007) and developed a simultaneous equation model (SEM). We collected data for two instrumental variables (one for off-hour access, the other for off-site access), both based on employees' job (or role) needs for off-hour or off-site access.

[15]We thank an anonymous referee for pointing this out.

[16]We thank Dr. Pamela Wilcox for the insight into this situation (private communication).

Table 6. Model Estimation with New Users

	New Users (first month n = 4507)	New Users (first two months n = 7245)
FIXED EFFECTS		
Month Fixed Effect	–	Included
Intercept	Included	Included
Apps	0.235	0.215
Conf	0.112	0.066
Off-hour	1.222	2.039
Off-site	20.946***	16.727***
Off-hour*Off-site	14.511	26.309*
Log(DeptSize)	-0.228	-0.437
Apps*Log(DeptSize)	-0.231	-0.065
Conf*Log(DeptSize)	0.042	-0.068
Off-hour*Log(DeptSize)	-1.132	-0.088
Off-site*Log(DeptSize)	2.592	0.508
Off-hour* Off-site* Log(DeptSize)	-2.811	2.800
VARIANCE of RANDOM COMPONENTS		
Residual (σ_e^2)	104.940	107.150
Department-Level Variance		
Intercept (σ_{w0}^2)	3.752	7.499
Apps (σ_{w1}^2)	0.250	0.145
Conf (σ_{w2}^2)	0.015	0.085
Off-hour (σ_{w3}^2)	46.501	17.949
Off-site (σ_{w4}^2)	355.640	367.670
Off-hour*Off-site (σ_{w5}^2)	1747.780	1884.460
MODEL FIT		
Deviance	34018	55496
AIC	34032	55510

***< .001; **< 0.01; *< 0.05; ^< 0.1

The instrumental variable for off-hour access is at the department level. In this financial institution, some departments have business needs that may require some (but not all) employees in the department to sometimes work outside of the institution's regular working hours. This means that while the standard working hours for all employees in this department are normally within the regular hours of the institution, business needs could arise in an *ad hoc* manner and require some employees to work off-hours on some days and others on different days. For example, there are several back-office operations, such as check sorting, information technology maintenance, and account reconciliation, that need to be done outside of regular hours when requested or as assigned to their calendar on an *ad hoc* basis.

To determine the need of working off-hours, we contacted a manager of human resources in the institution. The manager reviewed the objectives of each department along with its need to work outside of regular business hours. Based on the nature of departmental operations, a rating of 1 to 5 was assigned as the value for the variable *off-hour-needed*. This rating reflected the likelihood of a department having *ad hoc* business requests for some employees to work outside of regular institutional hours. Most of the front-office departments available only during business hours were rated 1 or 2, depending on whether there were any pre-opening and post-closure activities in that department. Since no department has an extreme demand for working off-hours, the highest rating is 4. An example is the investment service department. A majority of the employees in the department finish their job duties during regular hours and leave for the day. But different employees on different days may have to work longer to account for the daily performance of financial portfolios.

Table 7. Percentage of Sessions with Unauthorized Attempts in a Month: Three-level Models (n = 51,348)

Model Parameters	Model 1	Model 2		
		Attempts	Off-hour	Off-site
FIXED EFFECTS				
Month Fixed Effect	Included	Included	Included	Included
Intercept	Included	Included	Included	Included
Unauthorized Attempts	–	–	0.001	0.007**
Off-hour-Needed	–	–	0.020^	–
Internet-Enabled	–	–	–	0.407***
Apps	0.138***	0.152***	–	–
Conf	0.012	0.019	–	–
Off-hour	1.414***	1.567***	–	–
Off-site	2.815***	3.762***	–	–
Off-hour*Off-site	7.256***	8.755***	–	–
Log(DeptSize)	0.028	0.030	-0.016^	-0.011
Apps*Log(DeptSize)	0.010	0.015*	–	–
Conf *Log(DeptSize)	0.048**	0.060***	–	–
Off-hour*Log(DeptSize)	0.789***	1.017***	–	–
Off-site*Log(DeptSize)	0.396***	0.494***	–	–
Off-hour* Off-site* Log(DeptSize)	3.646***	4.620***	–	–
ActiveDays	0.051***	0.052***	0.004*	0.001
VARIANCE of RANDOM COMPONENTS				
Residual (σ_e^2)	11.125	3.282		
Intercept ($\sigma_{\mu 0}^2$) (Employee)	3.097	4.5834	0	0
Intercept (σ_{w0}^2) (Department)	0.098	0.102	0.001	0.004
MODEL FIT				
Deviance	277940	639687		
AIC	277946	639697		

***< .001; **< 0.01; *< 0.05; ^< 0.1

The instrumental variable for off-site access is at the employee level. We considered that an employee's role could be defined based on the applications they could legitimately access. Because of the nature of the business they support, some applications allow users access from off-site locations via the internet. We therefore defined a metric: *internet-enabled*, which is the percentage of internet-accessible applications in an employee's system profile. We also confirmed with the VP of Information Security at the institution that the system interfaces and functions are the same for internet-based and intranet-based visits. Therefore, employees are not more likely to make mistakes on internet-enabled systems than on others due to the design of the applications.

As these two variables (*off-hour-needed* and *internet-enabled*) are derived based on the business requirements of employee roles, theoretically, they should not lead to intentional unauthorized attempts and therefore serve the purpose of the instrumental variables. To make the SEM model manageable, we did not include random coefficients but only the random intercept in the hierarchical model. For comparison purposes, we first estimated the model without introducing the instrumental variables (Model 1). Then, we followed the estimation approach described in Steele et al. (2007) to estimate the simultaneous model (Model 2). We first performed likelihood ratio tests to determine whether off-hour and off-site access are significantly related to their corresponding instrumental variable. We find that *off-hour-needed* is significant for off-site access and *internet-enabled* is significant for off-hour access, all with $p < 0.001$.

With off-hour or off-site access as the dependent variable, we fitted and compared two models: with and without the instrument variable. Table 7 summarizes the results. It shows that the likelihood of off-hour access is positively influenced by *off-hour-needed* and employees' average active days per

month, but not by unauthorized access attempts and department size. The likelihood of off-site access is positively influenced by unauthorized access attempts and internet-enabled, but not by department size and average active days per month. We can also see that with the introduction of the instrumental variables, the result of Model 2 is largely consistent with that of Model 1 and those in Table 5. Note that the interaction between apps and department size is now significant.

Discussion and Conclusion

This study utilizes user behavioral analytics and extends multilevel criminal opportunity theory to better understand how opportunity contexts lead to unauthorized access attempts on information systems. It uses six months of log data from the ESSO system in a financial institution for hypothesis testing in response to the call for studies to utilize field data and advance our understanding of insider behavior. For data analyses, we employed multilevel modeling as an effective way to examine the data with a hierarchical structure and better estimate the effects of variables at different levels as well as their cross-level interactions. Table 8 summarizes the results of hypothesis testing. The results indicate that the number and the confidentiality of accessible applications, access time, access location, and department size, as well as their interactions, play important roles in employees' number of unauthorized access attempts. This study highlights the importance of contextual explanations of insider activities and sheds lights on the role of opportunity contexts in insider threats.

Contribution to Theory

So far as we are aware, this is among the first studies that examine the predictive validity of multilevel criminal opportunity theory in the context of information systems security. Multilevel criminal opportunity theory is a general theoretical framework that offers an explanation of the situational causes of crimes. The testing of the theory often requires contextualization (Hong et al. 2013; Johns 2006), given different types of crimes with varying environmental settings. Such contextualization often occurs in construct identification, model formulation, measurement, and result interpretation (Rousseau and Fried 2001). While much research in criminology has utilized the theory for different traditional crimes, such as predatory crimes (Cohen and Felson 1979; Hindelang et al. 1978; Wilcox et al. 2003), none has been carried out in the context of information security. This study makes an effort to contextualize the theory to insider threats, thereby extending the utilization of multilevel criminal opportunity theory. Our contextualization is important, given the difficulty in data collection from an offender perspective that relies on primary (as opposed to secondary) data collection methods over time.

The use of large-scale field data along with quantitative methods is an important strength of this work. Such an approach not only helps accomplish the main objective of understanding the impact of opportunity contexts on insider behavior, but also provides an analytic tool in identifying contributing factors to insider threats in different organizations (Johns 2006). Due to their dependence on information technologies and the highly sensitive nature of the stored data, financial institutions are especially susceptible to insider threats (Randazzo et al. 2004), but they are also particularly conservative in sharing security-related data (Kotulic and Clark 2004). Access to log data has presented a unique opportunity for user behavior analytics through suspicious activity monitoring (Nurse et al. 2014) to understand insider behavior in a natural setting inside a financial institution. While prior research has relied primarily on behavioral intentions or qualitative analyses to understand insider threats as discussed in the literature review, the use of field data in this paper fills this void.

Although opportunity is a necessary condition of computer crimes, prior empirical studies in behavioral information security and insider threats have mostly examined organization factors and individual motives or traits driving insider behavior that pose threats to digital assets. To date, few empirical studies have been dedicated to investigating how opportunity contexts lead to insider exploitation of digital assets. By extending multilevel criminal opportunity theory to the domain of insider threats, this study provides empirical evidence for the importance of opportunity contexts in insider threats. Together with other like-minded theories that focus on the importance of opportunity in insider threats (Padayachee 2016; Willison and Siponen 2009), this study advances information security research for situational prevention.

Furthermore, the study incorporates both individual-level and department-level factors and examines the effects of opportunity contexts. Our analyses validate the claim rooted in crime opportunity theory: opportunity contexts for insider threats consist of factors at different levels in an organization (Wilcox et al. 2003). Taking account of the ways in which individual-community interactions work, we find significant moderating effects of department size. The results demonstrate that the effects of individual-level contexts may be amplified in some departments due to departmental characteristics. Therefore, it is important to take account of both individual and community characteristics in investigating insider threats.

Table 8. Results of Hypothesis Testing

Hypothesis	Results
H1: When employees have greater scope of access to information applications, they are more likely to make unauthorized access attempts.	Supported
H2: When employees have access to more valuable data, they are more likely to make unauthorized access attempts.	Supported
H3: When employees access at times when guardianship is ineffective, they are more likely to make unauthorized attempts.	Supported
H4: When employees access from locations where guardianship is ineffective, they are more likely to make unauthorized attempts.	Supported
H5: The interaction between temporal and spatial realization is positively associated with unauthorized access attempts.	Supported
H6(a): Employees from larger departments are more likely to have higher unauthorized access attempts.	Supported
H6(b): Department size reinforces the effect of scope of accessed applications on unauthorized access attempts.	Not Supported
H6(c): Department size reinforces the effect of data value of accessed applications on unauthorized access attempts.	Supported
H6(d): Department size reinforces the effect of temporal realization on unauthorized access attempts.	Supported
H6(e): Department size reinforces the effect of spatial realization on unauthorized access attempts.	Supported
H6(f): Department size reinforces the effect of the interaction of temporal and spatial realization on unauthorized access attempts.	Supported

Implications for Practice

With the increasing trend of allowing employees to have a flexible schedule in organizations, more and more employees work after regular hours and/or from remote locations. Since many millennials are joining the workforce, such a practice may not only reduce a company's costs related to office space, equipment, parking, etc., but may also help boost employee morale and productivity by improving work–life balance (Kossek and Ozeki 1999). However, these practices pose unique challenges to information security management. In addition, recent trends around augmenting company staff by hiring more contractors and allowing vendors remote access have exacerbated the already risk-prone environment (Colwill 2009).

Empowering workers with access to systems and data from anywhere and at any time is rapidly morphing the traditional threat landscape, suggesting the need for a major recalibration of access management practices and strategy (Yue et al. 2007). Our study helps security managers better understand how employee activities may change along with their surroundings. Therefore, management can create a dynamic risk profile for employees, one that not only relies on static attributes of the users, but also considers the characteristics of where and when access is initiated. As a VP of Information Security in the financial institution whose data we used notes:

> *As security and risk managers, we are always reviewing our practices and controls that form our security posture to be able to adapt to trends in emerging threats. Allowing off-site and off-hour accesses has resulted in the emergence of new patterns of access that pose real threats to our security program. A study that can provide insights into how threats have shifted is very valuable for our institution to adapt our control environment.*

In the light of two recent simultaneously occurring phenomena—advancements in authentication and authorization technologies and realization of the benefits of those technologies—companies are increasingly adopting policy-based adaptive authentication methods for both employee- and customer-facing systems. Furthermore, risk-based adaptive authentication systems are being used as "step-up" measures to challenge selected "authenticated users" based on a set of predefined policies. The challenge (e.g., out-of-band questions, second factor, call-back at a registered phone number) is posed to those users based on their risk profiles. Our results suggest the risk profiles for adaptive authentication should consider time of user access, access location, the history of application access, and characteristics of the department the user is in.

Companies can also take cues from the results of this study to ensure application access privileges for larger departments are engineered with elevated risk considerations, particularly when off-hour and/or off-site access is allowed. Those considerations could include fine-grained access and policy-based review of access logs.

Finally, for security managers, our findings can inform the development of situational crime prevention techniques through changes in the conditions and circumstances that foster insider crimes. Compared with traditional approaches such as modifying the psychological drives of potential offenders or the features or behavioral patterns of potential victims, opportunity-driven crime prevention methods could be easier to implement and generate more productive outcomes (Padayachee 2016; Willison and Siponen 2009).

Limitations and Future Studies

Our study has several limitations. First, we relied on the systems access data from one organization; thus, the generalizability of the study may be improved with data from multiple organizations. Second, unauthorized access attempts could be honest mistakes. The explanatory power of the model may be further improved if we can completely eliminate unintentional mistakes and identify malicious attempts. Third, because of the limitation of the data, our models did not incorporate employee traits. Future research can investigate how individual traits explain individual-level variance of unauthorized access attempts and the impact of contextual variables. Fourth, our research model only considers that insiders develop their awareness space via their own experiences. It is also possible that insiders learn about information systems from their coworkers. Fifth, we need to interpret new users' behavior with caution. Detailed individual differences among new users could be further explored. For example, some potential offenders may be conservative or exploratory when they join a new firm. How to identity those new users may be an interesting direction for further exploration. Last, we shall also be aware that the authorization events recorded by the single sign-on system are only at the page (or URL) level. It cannot observe if the restrictions to data access is embedded within application code logic or enforced at the database level.

Acknowledgments

We thank the senior editor, Indranil Bardhan, the associate editor, and the anonymous reviewers of this paper, whose guidance and suggestions have significantly improved the lucidity of the paper. We also thank the various VPs and managers of the financial institution for their time regarding this paper. An earlier version of the paper was presented at the University of Delaware, Mississippi State University, University of Alabama, American University, Temple University, Arizona State University, and University of Texas at Austin. We thank the attendees for their valuable comments. This research was supported by the National Science Foundation under grants SES-1420758 and SES-1724725. The usual disclaimer applies.

References

Alnuaimi, O. A., Robert Jr., L. P., and Maruping, L. M. 2010. "Team Size, Dispersion, and Social Loafing in Technology-Supported Teams: A Perspective on the Theory of Moral Disengagement," *Journal of Management Information Systems* (27:1), pp. 203-230.

Andresen, M. A., Brantingham, P. J., and Kinney, J. B. 2016. *Classics in Environmental Criminology*, Boca Raton, FL: CRC Press.

Bandura, A. 1977. "Social Learning Theory," Englewood Cliffs, NJ: Prentice-Hall.

Bernard-Butcher, D. 1991. "Crime in the Third Dimension: A Study of Burglary Patterns in a High-Density Residential Area," Doctoral Dissertation, Simon Fraser University, Burnaby, BC, Canada.

Brantingham, P. J., and Brantingham, P. L. 1991. *Environmental Criminology*, Prospect Heights, IL: Waveland.

Bryk, A. S., and Raudenbush, S. W. 1992. *Hierarchical Linear Models*, Newbury Park, CA: SAGE Publications.

Canter, D. V., and Youngs, D. E. 2008. *Principles of Geographical Offender Profiling*, Farnham, England: Ashgate Publishing Ltd.

Center for Development of Security Excellence. 2018. "The Insider Threat and Its Indicators," National Insider Threat Special Interest Group (https://securityawareness.usalearning.gov/thwarting/data/pdf/Insider_Threat_Indicators.pdf; accessed January 10, 2019).

Chehimi, N. 2013. *The Social Web in the Hotel Industry*, Tier, Germany: Springer Gabler.

Clarke, R. V. 1995. "Situational Crime Prevention," in *Building a Safer Society, Strategic Approaches to Crime Prevention, Crime and Justice: A Review of Research,* M. Tonry and D. Farrington (eds.), Chicago: University of Chicago, pp. 91-150.

Cohen, L. E., and Felson, M. 1979. "Social Change and Crime Rate Trends: A Routine Activity Approach," *American Sociological Review* (44:4), pp. 588-608.

Colwill, C. 2009. "Human Factors in Information Security: The Insider Threat—Who Can You Trust These Days?," *Information Security Technical Report* (14:4), pp. 186-196.

Costa, D. L., Albrethsen, M. J., Collins, M. L., Perl, S. J., Silowash, G. J., and Spooner, D. L. 2016. "An Insider Threat Indicator Ontology," CERT Center and Carnegie Mellon University Software Engineering Institute (https://resources.sei.cmu.edu/asset_files/TechnicalReport/2016_005_001_454627.pdf; accessed January 10, 2019).

CPPA. 2015. "Utah.Gov: Connecting Residents and Government," Center for Public Policy & Administration, The University of Utah (https://digitallibrary.utah.gov/awweb/awarchive?item75172; accessed February 7, 2019).

Cram, W. A., Proudfoot, J. G., and D'Arcy, J. 2018. "Organizational Information Security Policies: A Review and Research Framework," *European Journal of Information Systems* (26:6), pp. 605-641.

Cummings, A., Lewellen, T., McIntire, D., Moore, A. P., and Trzeciak, R. 2012. "Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector," Carnegie Mellon University (https://resources.sei.cmu.edu/asset_files/SpecialReport/2012_003_001_28137.pdf; accessed February 7, 2019).

Davis, M. A. 2010. "Global Threat Local Pain: 2010 Strategic Security Survey," *Information Week*.

Davis, M. A. 2011. "Research: 2011 Strategic Security Survey: CEOs Take Notice," *Information Week*.

Dunne, R. L. 1994. "Deterring Unauthorized Access to Computers: Controlling Behavior in Cyberspace through a Contract Law Paradigm," *Jurimetrics* (35:1), pp. 1-15.

Elmrabit, N., Yang, S. H., and Yang, L. 2015. "Insider Threats in Information Security Categories and Approaches," in *Proceedings of 21st International Conference on Automation and Computing,* Glasgow, September 11-12, pp. 1-6.

FS-ISAC. 2016. "Securing Merchant Terminals and Ecommerce Systems," Financial Services-Information Sharing and Analysis Center (https://www.fsisac.com/sites/default/files/news/Alert_SecuringMerchantTerminals-Dec2016-FIN.pdf; accessed January 10, 2019).

Gelman, A., and Hill, J. 2007. *Data Analysis Using Regression and Multilevel/Hierarchical Models*, Cambridge, UK: Cambridge University Press.

Groff, E. R. 2007. "'Situating' Simulation to Model Human Spatio-Temporal Interactions: An Example Using Crime Events," *Transactions in GIS* (11:4), pp. 507-530.

Hamblen, M. 2011. "Workers Want to Choose Their Mobile Devices, Survey Finds," *Computerworld*, October 21.

Hindelang, M. J., Gottfredson, M. R., and Garofalo, J. 1978. *Victims of Personal Crime: An Empirical Foundation for a Theory of Personal Victimization*, Cambridge, MA: Ballinger Publishing Co.

Holt, T. J., and Bossler, A. M. 2008. "Examining the Applicability of Lifestyle–Routine Activities Theory for Cybercrime Victimization," *Deviant Behavior* (30:1), pp. 1-25.

Hong, W., Chan, F. K. Y., Thong, J. Y. L., Chasalow, L. C., and Dhillon, G. 2013. "A Framework and Guidelines for Context-Specific Theorizing in Information Systems Research," *Information Systems Research* (25:1), pp. 111-136.

Horton, F. E., and Reynolds, D. R. 1971. "Effects of Urban Spatial Structure on Individual Behavior," *Economic Geography* (47:1), pp. 36-48.

Hox, J. 2002. *Multilevel Analysis: Techniques and Applications*, Mahwah, NJ: Lawrence Erlbaum Associates.

Johns, G. 2006. "The Essential Impact of Context on Organizational Behavior," *The Academy of Management Review* (31:2), pp. 386-408.

Kennedy, L. W., and Forde, D. R. 1990. "Routine Activities and Crime: An Analysis of Victimization in Canada," *Criminology* (28:1), pp. 137-152.

Kornhauser, R. R. 1978. *Social Sources of Delinquency: An Appraisal of Analytic Models*, Chicago: University of Chicago Press.

Kossek, E. E., and Ozeki, C. 1999. "Bridging the Work-Family Policy and Productivity Gap: A Literature Review," *Community, Work & Family* (2:1), pp. 7-32.

Kotulic, A. G., and Clark, J. G. 2004. "Why There Aren't More Information Security Research Studies," *Information & Management* (41:5), pp. 597-607.

Loch, K. D., Carr, H. H., and Warkentin, M. E. 1992. "Threats to Information Systems: Today's Reality, Yesterday's Understanding," *MIS Quarterly* (16:2), pp. 173-186.

Magklaras, G., and Furnell, S. 2001. "Insider Threat Prediction Tool: Evaluating the Probability of IT Misuse," *Computers & Security* (21:1), pp. 62-73.

MaRS. 2009. "Confidential Information and Know-How: IP Strategy for Startups" (https://www.marsdd.com/mars-library/confidential-information-and-trade-secrets/).

Meiss, M., Duncan, J., Gonçalves, B., Ramasco, J. J., and Menczer, F. 2009. "What's in a Session: Tracking Individual Behavior on the Web," in *Proceedings of the 20th ACM Conference on Hypertext and Hypermedia*, New York: ACM, pp. 173-182.

Miethe, T. D., and Meier, R. F. 1990. "Opportunity, Choice, and Criminal Victimization: A Test of a Theoretical Model," *Journal of Research in Crime and Delinquency* (27:3), pp. 243-266.

Muchinsky, P. M., and Tuttle, M. L. 1979. "Employee Turnover: An Empirical and Methodological Assessment," *Journal of Vocational Behavior* (14:1), pp. 43-77.

Mullen, B., Symons, C., Hu, L.-T., and Salas, E. 1989. "Group Size, Leadership Behavior, and Subordinate Satisfaction," *The Journal of General Psychology* (116:2), pp. 155-170.

Munshi, A. M. 2013. "A Study of Insider Threat Behaviour: Developing a Holistic Insider Threat Model," unpublished paper, School of Information Systems, Curtin University (https://espace.curtin.edu.au/bitstream/handle/20.500.11937/1668/204962_Munshi%202014.pdf?sequence=2; accessed January 10, 2019).

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., and Vance, A. 2009. "What Levels of Moral Reasoning and Values Explain Adherence to Information Security Rules? An Empirical Study," *European Journal of Information Systems* (18:2), pp. 126-139.

Nurse, J. R. C., Legg, P. A., Buckley, O., Agrafiotis, I., Wright, G., Whitty, M., Upton, D., Goldsmith, M., and Creese, S. 2014. "A Critical Reflection on the Threat from Human Insiders—Its Nature, Industry Perceptions, and Detection Approaches," in *Proceedings of the 2nd International Conference on Human Aspects of Information Security, Privacy, and Trust*, pp. 270-281.

Padayachee, K. 2016. "An Assessment of Opportunity-Reducing Techniques in Information Security: An Insider Threat Perspective," *Decision Support Systems* (92), pp. 47-56.

Panda Security. 2012. "Confidential Business Information Prime Target for Cyber-Thieves, According to Pandalabs" (https://www.pandasecurity.com/mediacenter/press-releases/confidential-business-information-prime-target-for-cyber-thieves-according-to-pandalabs/; accessed January 10, 2019).

Patterson, H. D., and Thompson, R. 1971. "Recovery of Inter-Block Information When Block Sizes Are Unequal," *Biometrika* (58), pp. 545-554.

Ponemon, L. 2006. "Confidential Data at Risk," CSO Online, August 1.

Randazzo, M. R., Keeney, M., Kowalski, E., Cappelli, D., and Moore, A. 2004. "Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector," U.S. Secret Service and CERT Coordination Center/Carnegie Mellon University Software Engineering Institute.

Raudenbusch, S. W., and Bryk, A. S. 2002. *Hierarchical Linear Models: Applications and Data Analysis Methods* (2nd ed.), Thousand Oaks, CA: SAGE Publications, Inc.

Raymond, L. 1990. "Organizational Context and Information Systems Success: A Contingency Approach," *Journal of Management Information Systems* (6:4), pp. 5-20.

Rousseau, D. M., and Fried, Y. 2001. "Location, Location, Location: Contextualizing Organizational Research," *Journal of Organizational Behavior* (22:1), pp. 1-13.

Sarkar, K. R. 2010. "Assessing Insider Threats to Information Security Using Technical, Behavioural and Organisational Measures," *Information Security Technical Report* (15:3), pp. 112-133.

Shaw, E. D., Post, J. M., and Ruby, K. G. 1999. "Inside the Mind of the Insider," *Security Management* (43:12), pp. 34-44.

Shaw, M. E. 1981. *Group Dynamics: The Psychology of Small Group Behavior*, New York: McGraw-Hill.

Shrout, P. E., and Fleiss, J. L. 1979. "Intraclass Correlations: Uses in Assessing Rater Reliability," *Psychological Bulletin* (86), pp. 420-428.

Silowash, G., Cappelli, D., Moore, A., Trzeciak, R., Shimeall, T. J., and Flynn, L. 2012. "Common Sense Guide to Mitigating Insider Threats," Technical Report, Carnegie Mellon University Software Engineering Institute (https://resources.sei.cmu.edu/asset_files/TechnicalReport/2016_005_001_484758.pdf; accessed January 10, 2019).

Siponen, M., and Vance, A. 2010. "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations," *MIS Quarterly* (34:3), pp. 487-502.

Spooner, D., Cappelli, D., Moore, A., and Trzeciak, R. 2013. "Spotlight On: Insider Theft of Intellectual Property inside the U.S. Involving Foreign Governments or Organizations," CERT Program and Carnegie Mellon University Software Engineering Institute (https://resources.sei.cmu.edu/asset_files/WhitePaper/2009_019_001_43429.pdf; accessed February 7, 2019).

Steele, F., Vignoles, A., and Jenkins, A. 2007. "The Effect of School Resources on Pupil Attainment: A Multilevel Simultaneous Equation Modelling Approach," *Journal of the Royal Statistical Society: Series A* (170:3), pp. 801-824.

Straub, D., and Welke, R. 1998. "Coping with Systems Risk: Security Planning Models for Management Decision Making," *MIS Quarterly* (22:4), pp. 441-469.

Suleiman, J., and Watson, R. 2008. "Social Loafing in Technology-Supported Teams," *Computer Supported Cooperative Work* (17:4), pp. 291-309.

Teodor, S., Jonas, H., Kristoffer, L., and Johan, B. 2014. "Variables Influencing Information Security Policy Compliance: A Systematic Review of Quantitative Studies," *Information Management & Computer Security* (22:1), pp. 42-75.

Terborg, J. R., and Lee, T. W. 1984. "A Predictive Study of Organizational Turnover Rates," *The Academy of Management Journal* (27:4), pp. 793-810.

Thomas, E. J., and Fink, C. F. 1963. "Effects of Group Size," *Psychological Bulletin* (60:4), pp. 371-384.

Van Daele, S., and Beken, T. V. 2011. "Out of Sight, Out of Mind? Awareness Space and Mobile Offenders," *European Journal of Crime, Criminal Law and Criminal Justice* (19:2), pp. 125-137.

Velez, D. 2015. "Fighting the Insider Threat: It's Time to Think About Behavior Not Just Data," Raytheon|Websense.

Vormetric. 2015. "2015 Vormetric Insider Threat Report: Trends and Future Directions in Data Security," Global Edition, The Enterprise Strategy Group, Vormetric Data Security,(http://enterprise-encryption.vormetric.com/rs/vormetric/images/CW_GlobalReport_2015_Insider_threat_Vormetric_Single_Pages_010915.pdf; accessed January 10, 2019.

Wang, J., Gupta, M., and Rao, H. R. 2015. "Insider Threats in a Financial Institution: Analysis of Attack-Proneness of Information Systems Applications," *MIS Quarterly* (39:1), pp. 91-112.

Wang, J., Xiao, N., and Rao, H. R. 2015. "An Exploration of Risk Characteristics of Information Security Threats and Related Public Information Search Behavior," *Information Systems Research* (26:3), pp. 619-633.

Wang, J., Xie, H., and Fisher, J. H. 2011. *Multilevel Models: Applications Using SAS*. Berlin: Walter de Gruyter GmbH & Co. KG.

Warkentin, M., and Johnston, A. C. 2008. "IT Governance and Organizational Design for Security Management," in *Information Security: Policies, Processes, and Practices,* D. W. Straub, S. E. Goodman, and R. Baskerville (eds.), Armonk, NY: M. E. Sharpe, pp. 46-68.

Warkentin, M. E., Sayeed, L., and Hightower, R. 1997. "Virtual Teams Versus Face-to-Face Teams: An Exploratory Study of a Web-Based Conference System," *Decision Sciences* (28:4), pp. 975-996.

Weischedel, B., and Huizingh, E. K. 2006. "Website Optimization with Web Metrics: A Case Study," in *Proceedings of the 8th International Conference on Electronic Commerce*, New York: ACM, pp. 463-470.

Wilcox, P., Land, K. C., and Hunt, S. A. 2003. *Criminal Circumstance: A Dynamic Multicontextual Criminal Opportunity Theory*, New York: Aldine de Gruyter.

Wilcox Rountree, P., and Land, K. C. 1996. "The Generalizability of Multilevel Models of Burglary Victimization: A Cross-City Comparison," *Social Science Research* (29), pp. 284-305.

Willison, R. 2000. "Understanding and Addressing Criminal Opportunity: The Application of Situational Crime Prevention to Is Security," *Journal of Financial Crime* (7:3), pp. 201-210.

Willison, R. 2002. "Opportunities for Computer Abuse: Assessing a Crime Specific Approach in the Case of Barings Bank," doctoral dissertation Department of Information Systems, London School of Economics and Political Science (http://etheses.lse.ac.uk/1881/1/U213406.pdf).

Willison, R. 2006a. "Understanding the Offender/Environment Dynamic for Computer Crimes," *Information Technology & People* (19:2), pp. 170-186.

Willison, R. 2006b. "Understanding the Perpetration of Employee Computer Crime in the Organisational Context," *Information and Organization* (16:4), pp. 304-324.

Willison, R., and Siponen, M. 2009. "Overcoming the Insider: Reducing Employee Computer Crime through Situational Crime Prevention," *Communications of the ACM* (52:9), pp. 133-137.

Willison, R., and Warkentin, M. 2013. "Beyond Deterrence: An Expanded View of Employee Computer Abuse," *MIS Quarterly* (37:1), pp. 1-20.

Winkler, I., and Gomes, A. T. 2016. *Advanced Persistent Security: A Cyberwarfare Approach to Implementing Adaptive Enterprise Protection, Detection, and Reaction Strategies*, Amsterdam: Syngress.

Yar, M. 2005. "The Novelty of 'Cybercrime'—An Assessment in Light of Routine Activity Theory," *European Journal of Criminology* (2:4), pp. 407-427.

Yue, W. T., Çakanyildirm, M., Ryu, Y. U., and Liu, D. 2007. "Network Externalities, Layered Protection and It Security Risk Management," *Decision Support Systems* (44:1), pp. 1-16.

About the Authors

Jingguo Wang is a professor of Information Systems. He graduated from University at Buffalo, State University of New York. His work has been published in *MIS Quarterly, Information Systems Research, Journal of Management Information Systems*, and *Journal of the AIS,* among others. His current research interests include information security. His research has been supported by National Science Foundation and the University of Texas at Arlington.

Zhe Shan is an assistant professor of Information Systems and Analytics. He earned his Ph.D. in Business Administration and Operations Research from Penn State University Smeal College of Business in 2011. His research interests include FinTech innovation, information security, patient-center healthcare, and business process analytics.

Manish Gupta is Senior Audit Manager at one of the 15 largest banks in the United States, overseeing entire enterprise wide security and technology audit portfolios. He is also adjunct assistant professor at State University of New York at Buffalo teaching graduate courses in IT auditing and IT risk management since 2012. His research has won best paper awards and has been published in *MIS Quarterly, Decision Support Systems*, *Journal of Organizational and End User Computing*, and various ACM Transactions, among others. Manish received his Ph.D. (Management/MIS) and MBA (Finance and MIS) from State University of New York at Buffalo in 2011 and 2003, respectively.

H. Raghav Rao is AT&T Chair Professor of ISCS, College of Business and Prof of Computer Science (courtesy appointment) at the University of Texas, San Antonio. He graduated from Purdue University.

MIS Quarterly

RESEARCH ARTICLE

A LONGITUDINAL STUDY OF UNAUTHORIZED ACCESS ATTEMPTS ON INFORMATION SYSTEMS: THE ROLE OF OPPORTUNITY CONTEXTS

Jingguo Wang
Department of Information Systems and Operations Management, College of Business,
University of Texas at Arlington, Arlington, TX 76019 U.S.A. {jwang@uta.edu}

Zhe Shan
Department of Information Systems and Analytics, Farmer School of Business, Miami University,
Oxford, OH 45056 U.S.A. {jayshan@miamioh.edu}

Manish Gupta
Department of Management Science and Systems, School of Management,
State University of New York at Buffalo, Amherst, NY 14260 U.S.A. {mgupta3@buffalo.edu}

H. Raghav Rao
Department of Information Systems and Cyber Security, College of Business,
University of Texas at San Antonio, San Antonio, TX 78249 U.S.A. {hr.rao@utsa.edu}

Appendix A

Prior Studies of Insider Threats

Researchers have used the lens of social sciences to examine the characteristics of insider threats to understand motivation and subsequently develop appropriate organizational policies (Hunker and Probst 2011). Based on a database of insider threat cases, researchers in the CERT Insider Threat Center conducted a number of case studies to examine personal predispositions, organizational factors, and behavioral cues of malicious insiders (Cappelli et al. 2008; Cummings et al. 2012; Randazzo et al. 2004). Other researchers have also suggested various individual characteristics and organizational factors that may lead to insider threats (Costa et al. 2016; Liang et al. 2016; Magklaras and Furnell 2001, 2005; Shaw et al. 1998). Relying on those findings, predictive and analytical models have been proposed to identify malicious insiders (e.g., Band et al. 2006; Bishop et al. 2010; Maybury et al. 2005; Moore et al. 2008a; Nurse et al. 2014; Schultz 2002; Shaw et al. 1998). In particular, Gheyas and Abdallah (2016) provide a systematic literature review and meta-analysis of studies in detection and prediction of malicious insiders. Table A1 lists some example studies.

Additionally, a major stream of studies in the area of information systems examines what motivates employees to comply with or violate organizational security policies. Table A2 lists some example studies. Both Cram et al. (2018) and Teodor et al. (2014) carry out an extensive review of relevant journal articles and summarize organizational and individual factors (e.g., dispositional traits, sanctions, rewards, etc.). Most have conducted cross-sectional surveys to collect data, with the respondents' intention as the dependent variable.

Moreover, several studies have drawn upon environmental criminology and situational crime prevention (SCP) to address system risk from the offender's perspective (Willison 2006; Willison and Backhouse 2006; Willison and Siponen 2009). The fundamental premise of SCP is that crimes (cybercrimes or others) occur when a person has both motive and opportunity, so by either removing motive or denying a malicious

user an opportunity, one can help prevent crimes (Cullen and Agnew 2011). In short, SCP believes manipulating opportunities is a more promising crime prevention strategy than trying to make people less criminally inclined (Clarke 1980). Similar concepts such as problem-oriented policing and crime prevention through environmental design all seek to reduce opportunities for crime in practical ways at low social and economic cost (Cohen et al. 1980). Along this line, some conceptual frameworks have been proposed to mitigate insider threats from an opportunity-based perspective (Beebe and Rao 2005; Padayachee 2013, 2015, 2016; Willison 2006; Willison and Backhouse 2006; Willison and Siponen 2009). However, most of these discussions and investigations are conceptual or qualitative in nature. Empirical evidence through the application of environmental criminology such as multilevel criminal opportunity theory is sparse.

To help fill in the literature gap, this study empirically investigates the applicability of environmental criminology, specifically multilevel criminal opportunity theory, to explain unauthorized access attempts. We contextualize the aforementioned theory in the domain of insider threats and examine the role of opportunity contexts in driving insider threats to information systems in a financial institution.

Table A1 Example Studies in Insider Threats

Reference	Methodology	Theory	Data	Major Findings
Shaw et al. (1998)	Qualitative study	N/A	Interviews with convicted criminals	Psychological characteristics, such as computer dependency, ethical flexibility, and lack of empathy as potential indicators of a risk for destructive and potentially illegal behavior.
Straub and Welke (1998)	Qualitative study	General deterrence theory, and model of managerial decision making	Two information services Fortune 500 firms	Managers should initiate a theory-based security program that includes (1) use of a security risk planning model, (2) education in security awareness, and (3) Countermeasure Matrix analysis.
Shaw et al. (1999)	Case Study	N/A	46 cases with sufficient details from a DoD-sponsored project in 1997	Staff security awareness should be considered as sine qua non for a sound insider strategy, and describe three levels of user awareness: perception, understanding, and prediction.
Willison (2000)	Conceptual development	Situational crime prevention (SCP): Environmental criminology	N/A	Crimes (cyber crimes or others) occur when a person has both motive and opportunity—so by either removing motive or denying a malicious user an opportunity, we can help prevent crime.
Lee and Lee (2002)	Conceptual development	Theory of planned behavior, social bond theory and social learning theory	N/A	Model of computer abuse uses social criminology theories to account for why a person commits computer abuse and what factors significantly affect the computer abuse decision.
Beebe and Rao (2005)	Conceptual development	Situational crime prevention theory	NA	Situational crime prevention theory may offer new insights into improving IS security effectiveness by reducing the criminal's anticipated rewards from the crime.
Theoharidou et al. (2005)	Critical analysis	Criminology theories	800 organizations	ISO17799 follows the General Deterrence Theory. Consequently, it emphasizes on measures such as posing sanctions, reinforcing access control, and implementing training and awareness programs.
Band et al. (2006) and Moore et al. (2008b)	Analytical modeling	System dynamics	Insider IT sabotage and espionage cases	Behaviors, motivations, and personality disorders are associated with insider crimes such as antisocial or narcissistic personality.
Willison (2006); Willison and Backhouse (2006)	Case study	Routine activity theory, environmental criminology, rational choice perspective	Baring Bank case	It addresses systems risk from the offender's perspective. A model known as "crime-specific opportunity structure" is proposed. The model aids the conceptualization of the relationship between the offender, the organizational context, the requisite safeguards and the departments responsible for them.
Humphreys (2008)	Critical analysis	NA	NA	ISO/IEC 27001 can be used by different sectors and various organizations. It provides a flexible holistic approach to information security in the sense that it addresses people, process, legal and IT aspects.
Colwill (2009)	Critical analysis	Human factors and security risk management	N/A	Insider threats to information security cannot be totally eliminated but it can be assessed and managed. Human factors provide practical levers to gain a better understanding of the real risks facing organizations in today's global commercial environment.

Reference	Methodology	Theory	Data	Major Findings
Bishop et al. (2010)	Analytical modeling	Predictive analytics	N/A	Traditional cyber security audit data and psychosocial data can be integrated to predict possible insider exploits. However, certain types of errors that one expects in a predictive system can affect the usefulness of the results.
Munshi et al. (2012)	Critical analysis	Various theories used in insider threats research	Academic research and reported incidents	A holistic conceptual model is needed to encapsulate a broader perspective of the insider situation and reflect more closely empirical experiences.
Padayachee (2013), Padayachee (2015), Padayachee (2016)	Conceptual development	Rational choice theory, routine activities theory, situational crime prevention	A three-round Delphi process with 23 experts from the industry	A conceptual framework was developed to mitigate the insider threat from an opportunity-based perspective. The exploratory evaluation of opportunity-reducing techniques may inform organizations in designing controls and are situationally appropriate to mitigate insider threats.
Willison and Warkentin (2013)	Conceptual development	N/A	N/A	Extends Straub and Welke's (1998) security action cycle framework and proposes three areas for empirical investigation—techniques of neutralization (rationalization), expressive/instrumental criminal motivations, and disgruntlement as a result of perceptions of organizational injustice.
Liang et al. (2016)	Analytical modeling	Trait theory	133 real-world cases of offenders from military units, intelligence agencies, and business organizations	It validates malicious insider characteristics identified in previous research, thereby establishing a foundation for more comprehensive research in the future.

Table A2. Example Studies in Information Security

Reference	Research Question	Methodology	Theory	Independent Variables	Dependent Variables	Data	Major Findings
Abuse and Misuse of IS Resources							
Straub and Nance (1990)	1. How is computer abuse discovered in organizations? 2. How are identified computer abusers disciplined?	Field study	Deterrence theory	Abuse type, target asset, organization size, organization industry	Incident discovery: accidental discovery, normal system controls.	Victimization surveys of 1,063 randomly selected members of the Data Processing Management Association	Detection and punishment of violators reduce computer abuse.
Straub (1990)	1. Have IS security deterrents been effective in lowering computer abuse? 2. Can rival explanations explain lower incidence of computer abuse?	Survey study	Deterrence theory	Deterrents: IS security efforts, dissemination of information about penalties, guidelines for acceptable system use, policies for system use	Computer abuse: number of incidents, actual dollar loss, opportunity dollar loss	Survey collected from 1,211 randomly selected organizations	Use of IS security deterrents resulted in a decreased incidence of computer abuse. The effective deterrents increase employees' risk of getting caught .
Gopal and Sanders (1997)	How do preventive and deterrent controls to counter software piracy impact on software publisher profits?	Analytical modeling, survey study	Deterrence theory	Preventive control, deterrent control	Profitability		Policy statements prohibiting software piracy and warning of its legal consequences resulted in lower piracy intentions. Preventive controls decrease profits, but deterrent controls can potentially increase profits.
				Deterrence information, ethical index, gender, age	Club size	Questionnaires collected from 130 MBA students	
Lee et al. (2004)	How do social control theory and general deterrence theory explain computer abuse?	Survey study	Social control theory, general deterrence theory	Security awareness, physical security system, attachment, commitment, involvement, norms, self defense, etc.	Invaders' abuse, Insiders' abuse	Questionnaires to 500 MBA students and 500 middle managers in six Korean companies.	Deterrence factors influence self defense intention (SDI) and organizational factors significantly affect induction control intention (ICI).

Reference	Research Question	Methodology	Theory	Independent Variables	Dependent Variables	Data	Major Findings
D'Arcy et al. (2009)	How to develop an extended deterrence theory model to better explain the relationships between security countermeasures, sanction perceptions, and IS misuse?	Field study	Deterrence theory	User awareness, SETA program, computer monitoring	IS misuse intention	269 computer users from eight different companies	Three practices deter IS misuse: user awareness of security policies; security education, training, and awareness programs; and computer monitoring. Perceived severity of sanctions is more effective in reducing IS misuse than certainty of sanctions.
Policy Compliance							
Harrington (1996)	1. Do codes deter unethical behavior of IS employees? 2. Is the effect of codes moderated by the psychological traits of the IS employee?	Survey study	Deterrence theory	RD, Robin Hood, Rationalization, Intention, Less Damaging Judgment, Less Damaging Intention	Cracking Judgement, Cracking intention, Copy S/W Judgement, Copy S/W Intention, etc.	Questionnaire given to 219 IS employees in 9 organizations in the northeastern Ohio area	Codes of ethics applied to the organization generically did not affect employees' judgements or intentions to commit computer abuse.
Myyry et al. (2009)	What levels of moral reasoning and values explain adherence to information security rules?	Survey study	Theory of cognitive moral development; theory of motivational types of values	Preconventional reasoning, conventional reasoning, postconventional reasoning, openness to change, conversation.	Hypothetical compliance with information security policy, actual compliance with information security policy	132 respondents (clerical employees in a technical service center, or part-time master's students with work experience in Finland)	People who exhibit preconventional moral reasoning are more likely to obey the policies.
Siponen and Vance (2010)	Can neutralization theory provide a compelling explanation for IS security policy violations and offers new insight into how employees rationalize this behavior?	Field study	Neutralization theory, deterrence theory	Defense of Necessity, appeal to higher loyalties, condemn the condemners, metaphor of the ledger, denial of injury, denial of responsibility, etc.	Intention to violate IS security policy	Over 360 administrative personnel from three organizations in Finland	Employees may use neutralization techniques to minimize the perceived harm of their policy violations. This rationalizing behavior reduces the deterring effect of sanctions.
Bulgurcu et al. (2010)	1. What are the broad classes of an employee's beliefs about the overall assessment of consequences of compliance or noncompliance that influence attitude toward compliance and, in turn, intention to comply with the ISP? 2. What are an employee's beliefs about the outcomes of compliance and noncompliance that influence beliefs about the overall assessment of consequences?	Survey study	Theory of planned behavior	Information security awareness, perceived benefit of compliance, intrinsic benefit, safety of resources, rewards, perceived cost of compliance, work impediment, perceived cost of noncompliance, intrinsic cost, vulnerability of resources, sanctions, attitude, normative beliefs, self-efficacy to comply	Intention to comply	464 panel members provided by a US professional market research company	Employee's intention to comply with the information security policies is significantly influenced by attitude, normative beliefs, and self-efficacy to comply. Outcome beliefs significantly affect beliefs about overall assessment of consequences, and therefore significantly affect an employee's attitude. Furthermore, information security awareness positively affects both attitude and outcome beliefs.

Reference	Research Question	Methodology	Theory	Independent Variables	Dependent Variables	Data	Major Findings
Johnston and Warkentin (2010)	How do fear appeals modify end user behavioral intentions associated with recommended individual computer security actions?	Laboratory experiment	Protection motivation theory	Perceived threat severity, perceived threat susceptibility, response efficacy, social influence, self efficacy	Behavioral intent	275 faculty, staff, and students from multiple units at one large university	Fear appeals do impact end user behavioral intentions to comply with recommended individual acts of security, but the impact is not uniform across all end users.
Guo et al. (2011)	What factors influence end user attitudes and behavior toward organizational IS security?	Survey study	Composite behavior model (an extension to the theory of reasoned action)	Attitude toward security policy, relative advantage for job performance, perceived security risk, perceived sanctions, etc.	NMSV intention	335 computer users via both paper-based (approached at business buildings) and Web-based surveys	Utilitarian outcomes, normative outcomes, and self-identity outcomes are key determinants of end user intentions to engage in non-malicious security violation.
Xue et al. (2011), similar studies: Liang et al. (2013), Chen et al. (2012)	How does punishment affect employee compliance intention in mandatory IT settings?	Field survey	Punishment research and justice theory	Actual punishment, Punishment expectancy, Perceived justice of punishment, Satisfaction, Perceived usefulness, Perceived ease of use	Compliance intention	118 ERP users at one of China's top 500 enterprises	IT compliance intention is strongly influenced by perceived justice of punishment, which is negatively influenced by actual punishment.
D'Arcy et al. (2014)	How does employee stress caused by burdensome and ambiguous information security requirements impact employee's deliberate information security policy violations?	Survey study	Coping theory	Security-related stress: overload, complexity, uncertainty; Moral disengagement: reconstrue conduct, obscure or distort, devalue the target	ISP violation intention	539 employee users	Security-related stress engenders an emotion-focused coping response in the form of moral disengagement from ISP violations, which in turn increases one's susceptibility to this behavior.
Vance et al. (2015)	1. How can UI design artifacts increase perceptions of accountability in the users of a broad-access system? 2. Can increases in user accountability reduce intentions to violate access policies?	Design science	Accountability theory	Identifiability, expectation of evaluation, awareness of monitoring, social presence, perceived accountability	Intention to violate the access policy	114 employees with administrative access to the academic records system of a large private university	Four user-interface design artifacts were developed to raise users' accountability perceptions within systems and in turn decrease access-policy violations.
Hsu et al. (2015)	1. What are the consequences of organizational in-role and extra-role security behaviors on the effectiveness of ISPs? 2. What is the role of formal and social controls in enhancing in-role and extra-role security behaviors in organizations?	Survey study	Social control theory	Department level: extra-role behaviors, in-role behaviors	Department level: ISP effectiveness	IS managers and employees at many organizations	Extra-role behaviors are important in improving ISP effectiveness. Formal control and social control individually and interactively enhance both in- and extra-role security behaviors.
				Individual level: involvement, attachment, belief, commitment, specification, evaluation, reward, social control, formal control	Individual level: extra-role behaviors, In-role behaviors		

Appendix B

Comparison Between the Current Study and Wang et al. (2015)

Table B1 Comparison between the Current Study and Wang et al. (2015)

	Wang et al (2015)	Current Study
Research Question	What kinds of IS applications are more likely to experience unauthorized attempts?	Under what circumstances will insiders be more likely to make unauthorized attempts?
Unit of analysis	IS Application.	Employee-month.
Dependent Variables	1. The inter-arrival times of two consecutive unauthorized attempts on an application. 2. The number of unauthorized attempts on an application in a unit time.	The number of repeated unauthorized attempts an employee had in a month.
Theoretical Framework	Routine activity theory.	Multilevel criminal opportunity theory.
Hypotheses	Application characteristics that reflect value, inertia, visibility, and accessibility contributes to the victimization risk of an application.	Insiders accessing the IS applications under the contexts presenting an opportunity to exploit will be more likely to make unauthorized attempts.
Analysis Techniques	1. Survival analysis with a Weibull hazard model. 2. Count data analysis with a zero-inflated Poisson-Gamma model.	Multilevel linear regression.
Findings	The study investigates victimization risk and attack proneness associated with IS applications. It supports the empirical application of routine activity theory in understanding insider threats, and provide a picture of how different applications have different levels of exposure to such threats.	This study investigates how opportunity contexts impact employees' unauthorized access attempts on IS applications. It contextualizes multilevel criminal opportunity theory and suggests the important roles of contextual variables in leading to insider threats. Further, it shows that the results do not align with employees who might not know the systems well enough and could be making mistakes.

References

Band, S. R., Cappelli, D. M., Fischer, L. F., Moore, A. P., Shaw, E. D., and Trzeciak, R. F. 2006. "Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis," Carnegie Mellon University Software Engineering Institute.

Beebe, N. L., and Rao, V. S. 2005. "Using Situational Crime Prevention Theory to Explain the Effectiveness of Information Systems Security," in *Proceedings of the 2005 SoftWars Conference*, Las Vegas, NV, pp. 1-18.

Bishop, M., Engle, S., Frincke, D. A., Gates, C., Greitzer, F. L., Peisert, S., and Whalen, S. 2010. "A Risk Management Approach to the 'Insider Threat,'" in *Insider Threats in Cyber Security*, C. W. Probst, J. Hunker, D. Gollmann, and M. Bishop (eds.), New York: Springer, pp. 115-137.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Quarterly* (34:3), pp. 523-548.

Cappelli, D. M., Desai, A. G., Moore, A. P., Shimeall, T. J., Weaver, E. A., and Willke, B. J. 2008. "Management and Education of the Risk of Insider Threat (Merit): System Dynamics Modeling of Computer System Sabotage," Carnegie Mellon University Software Engineering Institute (http://www.dtic.mil/docs/citations/ADA632604).

Chen, Y., Ramamurthy, K., and Wen, K.-W. 2012. "Organizations' Information Security Policy Compliance: Stick or Carrot Approach?," *Journal of Management Information Systems* (29:3), pp. 157-188.

Clarke, R. V. 1980. "Situational Crime Prevention: Theory and Practice," *British Journal of Criminology* (20), pp. 136-137.

Cohen, L. E., Felson, M., and Land, K. C. 1980. "Property Crime Rates in the United States: A Macrodynamic Analysis, 1947-1977; with Ex Ante Forecasts for the Mid-1980s," *American Journal of Sociology* (86:1), pp. 90-118.

Colwill, C. 2009. "Human Factors in Information Security: The Insider Threat—Who Can You Trust These Days?," *Information Security Technical Report* (14:4), pp. 186-196.

Costa, D. L., Albrethsen, M. J., Collins, M. L., Perl, S. J., Silowash, G. J., and Spooner, D. L. 2016. "An Insider Threat Indicator Ontology," CERT Center and Carnegie Mellon University Software Engineering Institute (http://resources.sei.cmu.edu/asset_files/TechnicalReport/2016_005_001_454627.pdf).

Cram, W. A., Proudfoot, J. G., and D'Arcy, J. 2018. "Organizational Information Security Policies: A Review and Research Framework," *European Journal of Information Systems* (26:6), pp. 605-641.

Cullen, F. T., and Agnew, R. 2011. *Criminologyical Theory: Past to Present*, Oxford, UK: Oxford University Press.

Cummings, A., Lewellen, T., McIntire, D., Moore, A. P., and Trzeciak, R. 2012. "Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector," Carnegie Mellon University (http://www.dtic.mil/docs/citations/ADA610430).

D'Arcy, J., Herath, T., and Shoss, M. K. 2014. "Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective," *Journal of Management Information Systems* (31:2), pp. 285-318.

D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (20:1), pp. 79-98.

Gheyas, I. A., and Abdallah, A. E. 2016. "Detection and Prediction of Insider Threats to Cyber Security: A Systematic Literature Review and Meta-Analysis," *Big Data Analytics* (1:1), Article 6.

Gopal, R. D., and Sanders, G. L. 1997. "Preventive and Deterrent Controls for Software Piracy," *Journal of Management Information Systems* (13:4), pp. 29-47.

Guo, K. H., Yuan, Y., Archer, N. P., and Connelly, C. E. 2011. "Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model," *Journal of Management Information Systems* (28:2), pp. 203-236.

Harrington, S. J. 1996. "The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions," *MIS Quarterly* (20:3), pp. 257-278.

Hsu, J. S.-C., Shih, S.-P., Hung, Y. W., and Lowry, P. B. 2015. "The Role of Extra-Role Behaviors and Social Controls in Information Security Policy Effectiveness," *Information Systems Research* (26:2), pp. 282-300.

Humphreys, E. 2008. "Information Security Management Standards: Compliance, Governance and Risk Management," *Information Security Technical Report* (13:4), pp. 247-255.

Hunker, J., and Probst, C. W. 2011. "Insiders and Insider Threats—An Overview of Definitions and Mitigation Techniques," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications* (2:1), pp. 4-27.

Johnston, A. C., and Warkentin, M. 2010. "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly* (34:3), pp. 549-566.

Lee, J., and Lee, Y. 2002. "A Holistic Model of Computer Abuse within Organizations," *Information Management & Computer Security* (10:2), pp. 57-63.

Lee, S. M., Lee, S.-G., and Yoo, S. 2004. "An Integrative Model of Computer Abuse Based on Social Control and General Deterrence Theories," *Information & Management* (41:6), pp. 707-718.

Liang, H., Xue, Y., and Wu, L. 2013. "Ensuring Employees' It Compliance: Carrot or Stick?," *Information Systems Research* (24:2), pp. 279-294.

Liang, N., Biros, D. P., and Luse, A. 2016. "An Empirical Validation of Malicious Insider Characteristics," *Journal of Management Information Systems* (33:2), pp. 361-392.

Magklaras, G., and Furnell, S. 2001. "Insider Threat Prediction Tool: Evaluating the Probability of It Misuse," *Computers & Security* (21:1), pp. 62-73.

Magklaras, G. B., and Furnell, S. M. 2005. "A Preliminary Model of End User Sophistication for Insider Threat Prediction in IT Systems," *Computer & Security* (24), pp. 371-380.

Maybury, M., Chase, P., Cheikes, B., Brackney, D., Matzner, S., Hetherington, T., Wood, B., Sibley, C., Marin, J., and Longstaff, T. 2005. "Analysis and Detection of Malicious Insiders," MITRE Corp. (http://www.dtic.mil/docs/citations/ADA456356).

Moore, A. P., Cappelli, D. M., and Trzeciak, R. F. 2008a. "The "Big Picture" of Insider IT Sabotage across U.S. Critical Infrastructures," CERT Center and Carnegie Mellon University Software Engineering Institute (http://link.springer.com/chapter/10.1007/978-0-387-77322-3_3).

Moore, A. P., Cappelli, D. M., and Trzeciak, R. F. 2008b. *The "Big Picture" of Insider IT Sabotage across US Critical Infrastructures*, New York: Springer.

Munshi, A., Dell, P., and Armstrong, H. 2012. "Insider Threat Behavior Factors: A Comparison of Theory with Reported Incidents," in *Proceedings of 45th Hawaii International Conference on System Science*, Los Alamitos, CA: IEEE Computer Society Press, pp. 2402-2411.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., and Vance, A. 2009. "What Levels of Moral Reasoning and Values Explain Adherence to Information Security Rules? An Empirical Study," *European Journal of Information Systems* (18:2), pp. 126-139.

Nurse, J. R. C., Legg, P. A., Buckley, O., Agrafiotis, I., Wright, G., Whitty, M., Upton, D., Goldsmith, M., and Creese, S. 2014. "A Critical Reflection on the Threat from Human Insiders—Its Nature, Industry Perceptions, and Detection Approaches," in *Proceedings of the 2nd International Conference on Human Aspects of Information Security, Privacy, and Trust*, New York: Springer, pp. 270-281.

Padayachee, K. 2013. "A Conceptual Opportunity-Based Framework to Mitigate the Insider Threat," in *Proceedings of the Information Security for South Africa 2013 Conference*, pp. 1-8.

Padayachee, K. 2015. "A Framework of Opportunity-Reducing Techniques to Mitigate the Insider Threat," in *Proceedings of the Information Security for South Africa 2015 Conference*, pp. 1-8.

Padayachee, K. 2016. "An Assessment of Opportunity-Reducing Techniques in Information Security: An Insider Threat Perspective," *Decision Support Systems* (92), pp. 47-56.

Randazzo, M. R., Keeney, M., Kowalski, E., Cappelli, D., and Moore, A. 2004. "Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector," U.S. Secret Service and CERT Coordination Center/Carnegie Mellon University Software Engineering Institute (http://www.secretservice.gov/ntac/its_report_040820.pdf).

Schultz, E. E. 2002. "A Framework for Understanding and Predicting Insider Attacks," *Computers & Security* (21:6), pp. 526-531.

Shaw, E., Ruby, K., and Post, J. 1998. "The Insider Threat to Information Systems: The Psychology of the Dangerous Insider," *Security Awareness Bulletin* (2:98), pp. 1-10.

Shaw, E. D., Post, J. M., and Ruby, K. G. 1999. "Inside the Mind of the Insider," *Security Management* (43:12), pp. 34-44.

Siponen, M., and Vance, A. 2010. "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations," *MIS Quarterly* (34:3), pp. 487-502.

Straub, D. W. 1990. "Effective IS Security: An Empirical Study," *Information Systems Research* (1:3), pp. 255-276.

Straub, D. W., and Nance, W. D. 1990. "Discovering and Disciplining Computer Abuse in Organizations: A Field Study," *MIS Quarterly* (14:1), pp. 45-60.

Straub, D. W., and Welke, R. 1998. "Coping with Systems Risk: Security Planning Models for Management Decision Making," *MIS Quarterly* (22:4), pp. 441-469.

Teodor, S., Jonas, H., Kristoffer, L., and Johan, B. 2014. "Variables Influencing Information Security Policy Compliance: A Systematic Review of Quantitative Studies," *Information Management & Computer Security* (22:1), pp. 42-75.

Theoharidou, M., Kokolakis, S., Karyda, M., and Kiountouzis, E. 2005. "The Insider Threat to Information Systems and the Effectiveness of ISO 17799," *Computers & Security* (24:6), pp. 472-484.

Vance, A., Benjamin Lowry, P., and 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), pp. 346-366.

Wang, J., Gupta, M., and Rao, H. R. 2015. "Insider Threats in a Financial Institution: Analysis of Attack-Proneness of Information Systems Applications," *MIS Quarterly* (39:1), pp. 91-112.

Willison, R. 2000. "Understanding and Addressing Criminal Opportunity: The Application of Situational Crime Prevention to IS Security," *Journal of Financial Crime* (7:3), pp. 201-210.

Willison, R. 2006. "Understanding the Offender/Environment Dynamic for Computer Crimes," *Information Technology & People* (19:2), pp. 170-186.

Willison, R., and Backhouse, J. 2006. "Opportunities for Computer Crime: Considering Systems Risk from a Criminological Perspective," *European Journal of Information Systems* (15:4), pp. 403-414.

Willison, R., and Siponen, M. 2009. "Overcoming the Insider: Reducing Employee Computer Crime through Situational Crime Prevention," *Communications of the ACM* (52:9), pp. 133-137.

Willison, R., and Warkentin, M. 2013. "Beyond Deterrence: An Expanded View of Employee Computer Abuse," *MIS Quarterly* (37:1), pp. 1-20.

Xue, Y., Liang, H., and Wu, L. 2011. "Punishment, Justice, and Compliance in Mandatory IT Settings," *Information Systems Research* (22:2), pp. 400-414.