Communications of the Association for Information Systems

Volume 35 Article 18

12-2014

Multiple Case Study Approach to Identify Aggravating Variables of Insider Threats in Information Systems

Mathew Nicho
School of Computing and Digital Media, Robert Gordon University, United Kingdom, m.nicho1@rgu.ac.uk

Faouzi Kamoun
College of Technological Innovation, Zayed University, United Arab Emirates

Recommended Citation

Nicho, Mathew and Kamoun, Faouzi (2014) "Multiple Case Study Approach to Identify Aggravating Variables of Insider Threats in Information Systems," *Communications of the Association for Information Systems*: Vol. 35 , Article 18.
DOI: 10.17705/1CAIS.03518
Available at: https://aisel.aisnet.org/cais/vol35/iss1/18

Communications of the Association for Information Systems

CAIS

Multiple Case Study Approach to Identify Aggravating Variables of Insider Threats in Information Systems

Mathew Nicho

School of Computing and Digital Media, Robert Gordon University, United Kingdom

m.nicho1@rgu.ac.uk

Faouzi Kamoun

College of Technological Innovation, Zayed University, United Arab Emirates

Faouzi.Kamoun@zu.ac.ae

Abstract:

Malicious insiders present a serious threat to information systems due to privilege of access, knowledge of internal computer resources, and potential threats on the part of disgruntled employees or insiders collaborating with external cybercriminals. Researchers have extensively studied insiders' motivation to attack from the broader perspective of the deterrence theory and have explored the rationale for employees to disregard/overlook security policies from the perspective of neutralization theory. This research takes a step further: we explore the aggravating variables of insider threat using a multiple case study approach. Empirical research using black hat analysis of three case studies of insider threats suggests that, while neutralization plays an important role in insider attacks, it takes a cumulative set of aggravating factors to trigger an actual data breach. By identifying and aggregating the variables, this study presents a predictive model that can guide IS managers to proactively mitigate insider threats. Given the economic and legal ramifications of insider threats, this research has implications relevant both for both academics and security practitioners.

Keywords: Insider Threat, Neutralization, Data Breaches, Information Systems Security, Qualitative Research.

Volume 35, Article 18, pp. 333-356, December 2014

The manuscript was received 06/07/2013 and was with the authors 9 months for 3 revisions.

I. INTRODUCTION

End users at the workplace are said to be “the weakest link” in information systems (IS) security (Guo, Yuan, Archer, & Connelly, 2011; Paans & Herschberg, 1987). Early studies on data breaches have showed that many hackers turned out to be employees or insiders (Escamilla, 1998; Russell & Gangemi 1992, cited in Cavusoglu, Mishra, & Raghunathan, 2005). Moreover, insider attacks can be more destructive and costly than attacks from the outside due to insiders’ extensive knowledge of an organization’s computer resources (Bradford & Hu, 2005; Santos et al., 2012). Today, a firm’s information-related assets are considered among their most valuable resources (Gordon, Loeb, & Sohail, 2010), while the risk of cybercrime impacting stakeholders and damaging communities continues to grow at an ever-expanding rate (Martin & Rice, 2011). At the same time, the increasing mobility of the workforce and the convenience of working with corporate data outside the workplace has led to new security challenges. As a result, proactive controls have become important elements of a firm’s overall security architecture since completely preventing intrusions is now an unlikely scenario (Bradford & Hu, 2005).

It is estimated that the total cost incurred for one compromised record amounts to nearly US$214 (Ponnemon Institute, 2011), which includes the cost associated with the loss of sensitive organizational data, systems information, copyrighted material, trade secrets, and classified information. While statistics on cybercrime incidents (as reported, for instance, by the Identity Theft Resource Centre (ITRC), Privacy Rights Clearing House (PRCH), and the Open Security Foundation (SF)) categorize insider threats as purely intentional acts, Loch, Carr, and Warkentin (1992) classify them as being either intentional or accidental. If this accidental aspect is taken into consideration, then threat from insiders can be regarded as among the most significant contributors to cyber threats. Therefore, an empirical investigation of insider threats to identify causation factors will contribute valuable insight for practice due to the detectable, predictable, manageable, and preventable nature of insider threats as compared to external threats. In this regard, Benbasat and Zmud (1999, p. 5) state that “authors who strive to craft relevant articles for practitioners must, at a minimum, focus on the concerns of practice, provide real value to IS professionals, and apply a pragmatic rather than academic tone”.

Insider threats are among the most serious and difficult security problems to cope with because insiders have privileged access to information that external attackers aren’t aware of; thus, they can abuse organizational trust and cause serious harm while leaving little evidence (Colwill, 2009). For researchers and practitioners, a key challenge in addressing the problem of insider threats is the lack of real-world data on them, given that organizations are reluctant to report such incidents in order to safeguard their reputation from negative publicity (Hunker & Probst, 2011; Keromytis, 2008; Pfleeger, 2008; Pfleeger & Stolfo, 2009; Richardson, 2008). This lack of data is a key hurdle impeding the inductive development of validated theoretical models. In addition, most available data about insider threats is anecdotal, based on small, biased data sets (Hunker & Probst, 2011), or gathered from convenience surveys, which makes the paucity of data a challenge for insider threat researchers, who need solid data to build models, make predictions, and support valid decision making (Pfleeger & Stolfo, 2009). Indeed, the lack of empirical studies on insider threats reflects the lack of maturity of the scientific literature on this important topic. As a result of this lack of data, both practitioners and researchers have only a rudimentary understanding of the factors contributing to insider attacks (Bishop, Gollmann, Hunker, & Probst, 2008): there is as yet no common vision of the aggregating variables that lead to an insider attack. However, precisely such an understanding is required if we are to develop appropriate prevention, detection, and mitigation strategies and subsequently evaluate their effectiveness (Bishop et al., 2008).

Various socio-technical approaches have been proposed in the literature to mitigate the risk of insider threats. However, none of these approaches has provided a comprehensive and empirically validated conceptual model to counter insider threats due to a lack of real-world data that would enable one to analyze and validate the proposed approaches and solutions (Keromytis, 2008). Consequently, given the lack of empirical research on security risk management (Kotulic & Clark, 2004), IS scholars working directly with black hat data (i.e., data that are accessed directly from the source) could promote a fresh look at what is available and perhaps inspire more fruitful research into IS security (Mahmoud, Siponen, Straub, Rao, & Raghu, 2010). By focusing on identifying the mechanisms underlying computer crimes from an insider’s perspective, we hope that this research initiative will help enhance the effectiveness of organizational responses to insider threats. In particular, we wrote this work due to the fact that efficient risk management of insider attacks is largely dependent on a sound understanding of what gives rise to them. As such, in this paper, we explore the multifaceted nature of, and the causation factors behind, insider attacks by interviewing the IT managers of three different organizations that have been victims of insider attacks. In particular, our interviews focused mainly on identifying the motivational triggers, the threat/attack methodology, the actors involved, the role played by the organization's technical and non-technical IT controls, and the number of aggravating variables that affected the insider attack. As Mahmoud et al. (2010, p. 433) highlight:

> *The increasing number of scholars who are turning their attention to security research can improve the richness and depth of their research by seeking out new, even unique sources of data that show the underlying mechanisms of computer crime and the effectiveness of organizational responses to this behavior.*

Accordingly, we used a qualitative approach for our study to better understand the complex, dynamic, and often entangled factors that can contribute to an insider attack. Therefore, drawing on related literature and by analyzing three case studies (related to different sectors) that reported internal data breaches, we develop an empirically validated conceptual model that captures the aggregating variables leading to a successful insider attack. Although findings from three cases can more successfully be generalized than findings from a single case, we selected an additional case from the event management sector to ensure theoretical saturation (Yin, 2009) and found that it did not add any significant new insights to what we had already found. Hence, we believe that conducting additional case studies in the context of this research project will probably not yield new findings.

In this paper, we adopt Pfleeger and Stolfo's (2009) categorization of insiders to include employees or ex-employees, business partners, auditors, consultants, or other people and systems who receive authorized short- or long-term access to an organization's systems. Accordingly, we define “insider threat” as the action or inaction of an insider that can jeopardize the safety of data, whether at rest or in motion. We also use the term “insider threat” to refer to existing or former employees who misuse their computer-access privilege and/or authority (Garrison & Ncube, 2011).This threat can arise either intentionally or accidentally, usually as a result of ignorance, mistakes, or deliberate acts (Durgin, 2007; Lee & Lee, 2002; Lee, Lee, & Yoo , 2003, cited in Bulgurcu, Cavusoglu, & Benbasat, 2010). In addition, we use the terms “data breach”, “attack”, “cyber-attack”, and “malicious act” interchangeably in this study.

This paper is structured as follows: In Section 2, we present the theoretical background concerning the insider threat landscape, and analyze certain statistics related to cybercrime in order to assess the role of insider threats and the domains of attack. In Section 3, we review and assess the IS security models and preventive mechanisms (IT controls) used to combat cybercrime. We also identify the research gap and formulate our research question. In Section 4, we present the research methodology and outline the deductive and inductive findings from the three case studies. In Section 5, we correlate our analyzed results with our research propositions to answer our research question. Finally, in Section 6, we summarizes our main findings , highlight their implications for research and practice, and outline some directions for future research.

II. THE INSIDER THREAT LANDSCAPE

Cyber threats can arise from external, internal, or unknown sources (CSI Computer Security Institute, 2011). IS security technical controls can prevent external attacks to a great extent, but preventing insider threats depends almost entirely on internal IT controls and voluntary policies. In particular, managing internal threats using the :authorized access: route remains an issue given (1) the need to prevent illicit access while still allowing authorized access to information (Post & Kievit, 1991), and (2) the difficulty in differentiating between authorized and unauthorized internal users.

Since a few high-profile cases reported in the early 1970s, the insider threat has been a major security concern, given that “frequently security violations involve those who are authorized or have access to the sensitive data of concern” (Lehmann, 1981, p. 26). One of the earliest high-profile insider frauds occurred at the Equity Funding Corporation of America from 1964 to 1973. In that case, the corporation's management falsified records and supporting documents that possibly involved hundreds of millions of dollars in order to inflate equity (EDPACS, 1973). Almost half a century later, and despite the progress made in hardening security technologies, policies, and controls, safeguarding sensitive corporate data still remains a daunting task. In fact, the very engine that drives the progress in IT infrastructure has also created new security threats to this infrastructure, threats that cannot be predetermined and that are not revealed in a predictable manner (Abbas, Magnusson, Yngstrom, & Hemani, 2011). Remote access, extended enterprise, bring your own device, and the extranet have enhanced employee productivity, but, at the same time, have raised new IS security risks. Furthermore, while external threats can be mitigated to a certain extent using technical and non-technical controls and security polices, containing insider threats remains a challenging endeavor. For researchers, the task of examining insider threats is further complicated due to the difficulty in collecting hard facts regarding computer fraud (Richards, 1984) since most affected organizations may not disclose internal data breaches. This lack of reporting has made research into cybercrime a real challenge (Kjaerland, 2006), although available data-breach statistics can provide some guidance for better understanding the impact of the various types of insider threats.

Magnitude of Insider Threats

Based on an analysis of historical records of data breaches, Verizon (2008) estimates that the magnitude of breaches (median size as measured by the number of compromised records) committed by insider sources has exceeded those by external sources by a factor of more than ten to one. This finding confirms earlier claims that privileged parties are able to do more damage to an organization than outsiders (Verizon, 2008). As Table 1 illustrates, a basic calculation of risk (likelihood (frequency) x (number of records breached)) shows that insiders (including internal employees and authorized business partners) represent the greatest security risk to organizations.

Table 1: Risk Severity of Attacks (Adapted from Verizon, 2008)

Source	Likelihood	No. of records breached (impact)	Risk	Ratio
External	73 %	30000	21900	0.134
Internal	18 %	375000	67500	0.41
Partner	39 %	187500	73125	0.45

The Role of Insiders in Cybercrime

Since organizations that collect and report publicly available data breaches are more freely accessible in the United States (US), we looked at statistical data on intentional breaches by insiders from three U.S.-based organizations; namely, the Identity Theft Resource Centre (ITRC), the Privacy Rights Clearinghouse (PRCH), and the Open Security Foundation (OSF). In addition, since reporting mandates in the US have only been introduced during the past few years, Figure 1 shows the percentage of insider data breaches to the total number of reported breaches among all threat categories during the years 2003 through to October 2013 (insider threat data from January to October 2013 for ITRC was not available at the time of this paper’s submission).

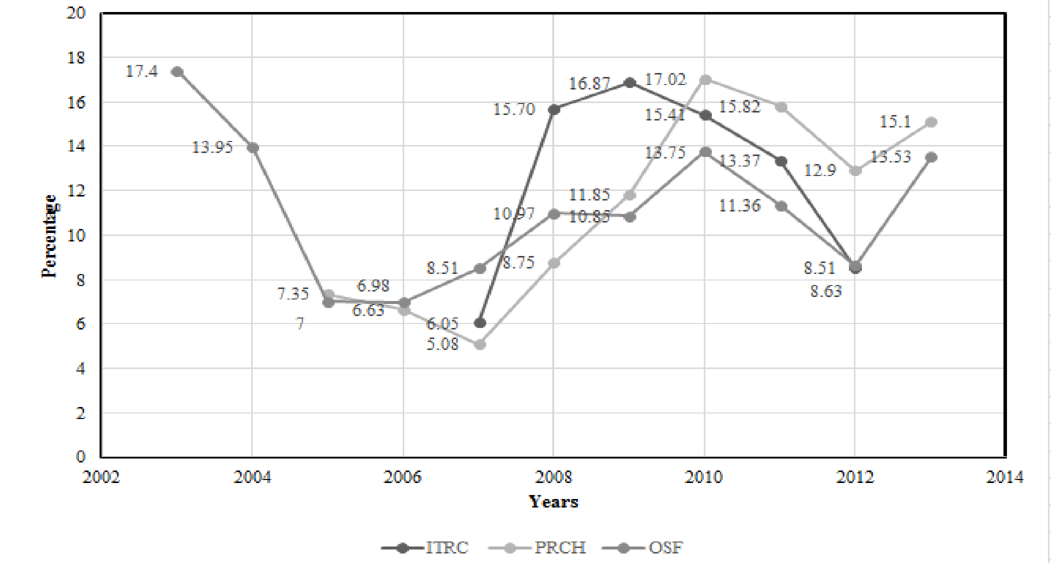


Figure 1. Percentage of Malicious Insider Threats Among all Threat Categories Listed by ITRC, PRCH, and OSH

ITRC, an organization engaged in tracing data breaches, began tracking security breaches in 2005 and, since 2007, has prepared annual reports of its findings using five categories: data on the move, accidental exposure, insider theft, subcontractors, and hacking. During the 2007-2012 period, the share of insider theft occurrences among these five categories has grown from 6.1 percent to 8.5 percent (ITRC, 2013). PRCH, a California-based organization, collects data breach statistics in order to identify trends and communicate them to relevant stakeholders. According to PRCH, the share of insider threat occurrences among eight identified data breach categories during the 2005 to 2012 period grew from 7.35 percent to 12.9 percent (Privacy Rights Clearing House, 2013). By the end of October 2013, the share of insider threats had increased to 15.1 percent. The Open Security Foundation, another non-profit

U.S. organization dedicated to tracking and reporting security breaches, revealed that the share of insider security breech occurrences increased from 7 percent in 2005 to 8.63 percent in 2012, but, by the end of September, 2013, the share of insider threats had increased once again to 13.53 percent (Datalossdb, 2013).

We should note, however, that the above statistics do not take into account the number of breached records nor the value of these records. Recall, to this effect, that insiders have both the knowledge and the access privilege to target organizations' most valuable records. In addition, while the reported data breach statistics point out the seriousness of insider attacks, the motives or the aggravating variables of these attacks are not evident in these studies. This shortcoming points out the potential role IS security theories, IT models, standards, and controls can play in exploring the intrinsic nature of insider threats, which, in turn, can point the way toward developing proper risk-mitigation strategies. Hence, taking into account their subject and object, we need to explore insider threats' dynamic nature with the appropriate theories that look into the deeper level of insider threats.

III. INFORMATION SECURITY MODELS, FRAMEWORKS, AND CONTROLS

Information security's primary goal is to protect data confidentiality, integrity, authentication, and non-repudiation, while getting the most value from security by insuring that technology investments protect the right things (Tsiakis & Stephanides, 2005). With this objective in mind, scholars have proposed numerous models and frameworks for securing enterprise information systems. Organizational security often focuses more on preventing external threats, such as hackers and viruses, which thus leaves organizations vulnerable to breaches from the inside (Spears & Barki, 2010). Therefore, the threat of IS security breaches by internal personnel could be reduced if greater emphasis were placed on internal threats that can occur when employees handle corporate data in their day-to-day jobs (Spears & Barki, 2010). A socio-technical dimension is inherent in information security, and this dimension leaves opportunities for human errors (such as mistakes, lapses, disruption, distortion, destruction, and disclosure) to trigger a data breach incident (Schultz, 2005). While researchers have proposed IS security models that incorporate technical and non-technical aspects from a holistic perspective, research on insider threats motivation and mitigation is quite limited.

One of the earliest IS security models is the detection model that Lehmann (1981) proposed. This model uses audit trails to track potential security violations. Straub's (1990) model for detecting computer abuse and disciplining those responsible for it puts more focus on evaluating investment in IT security, while Trcek's (2003) multi-planes layered model for IS security focuses on e-business systems security. Ganame, Bourgeois, Bidou, and Spies (2006) propose a distributed security operation center (SOC), which is able to detect attacks occurring simultaneously at several sites in a network, while Yadav (2010) presents a six-view perspective of system security. An aggregate of these models uses one or more of deterrence theory's four mechanisms (Straub & Welke, 1998), while using the neutralization technique (Siponen & Vance, 2010) illuminates why employees disregard/overlook IS security policies. The neutralization theory originally proposed by Sykes and Matza (1957) claims that both law-abiding citizens and those who commit crimes or rule-breaking actions justify their actions by applying techniques of neutralization (Siponen & Vance, 2010). Siponen and Vance (2010) specify six neutralization techniques; namely, defense of necessity, appeal to higher loyalty, condemn the condemners, metaphor of the ledger, denial of injury, and denial of responsibility.

Table 2 summarizes research in the security threat domain as distinguished between research using generic threat models and research using insider threat models. We can see from the table that two streams of research provide valuable insights into the occurrence of security breaches and their prevention. First, a noticeable number of studies exists that focused on building security threat models based on the assumption that threat behaviors can be explained using one or more components of deterrence theory; namely, deterrence, prevention, detection, and remedy. A second group of studies employed the motivation factor of insider threats to explain why employees violate security policies. We do not consider intention to be a direct proxy for behavior, but instead see it as "an indicator of a motivational state that exists just prior to the commission of an act. We think of it as a measured reflection of a predisposition to commit [an act]" (Paternoster & Simpson, 1996, p. 561). This motivation is driven mainly by an employee's intrinsic values, perceptions and desires. Thus, we find that neutralization significantly affects the predisposition to violate IS security policy. As Table 2 shows, most insider threat research has focused on preventing, detecting, mitigating, remediating, and punishing unwelcome acts on the part of people and systems that have legitimate access to networks (Pfleeger & Stolfo, 2009), while the motivation to attack is a domain to which less research has been devoted. In fact, out of the sixteen studies on security threats in Table 2, only two delve into the "motivation" factor, which reflects the lack of maturity of the literature on this topic and provides further motivation for our research. Out of the five insider threat models shown in Table 2, neutralization theory (Siponen & Vance, 2010) provided justification for employee violations of security policies, while the systems dynamic model (Melara, Sarriegui, Gonzalez, Sawicka, & Cooke, 2003) traced the generic precursor incidents leading to the attack. In addition, earlier research has focused mainly on the drivers behind the actual attacks, while the contribution of latent organizational system defects in data breaches has not been investigated. With this study, we address these gaps by taking a more holistic approach and employing neutralization and system dynamics theories to identify the aggregating variables involved in insider threats while using a multiple case study approach.

Table 2. Summary of Extent of Research on Generic and Insider Threats in IS

			Deterrence theory					
	Authors	**Main contributions**	**Deterrence**	**Prevention**	**Detection**	**Remedy**	Motivation	Empirical evidence
Generic threat models	Straub & Welke (1998)	Proposed a theory-based security program that includes the use of a security risk planning model, education/training in security awareness, and countermeasure matrix analysis to reduce losses from computer abuse and disasters.	✓	✓	✓	✓	-	✓
	Trček (2003)	Presented a layered multi-plane model to manage e-business systems security by integrating existing technological, organizational, and legal approaches in a balanced way.	✓	✓	✓	✓	-	-
	Ganame et al. (2006)	Developed a distributed security operation center that is able to detect network attacks occurring simultaneously at several sites	✓	✓	✓	✓	-	✓
	Yadav (2010)	Proposed a six-view perspective of a system security framework to identify a set of security risks and requirements. The framework was validated using a case study approach.	✓	✓	✓	✓	-	✓
	von Solms, van de Haar, von Solms, & Caelli (1994)	Proposed a model for information security management using data captured during security reviews.	✓	✓	✓	✓	-	-
	Beebe & Rao (2010)	Demonstrated that a meso-level application of situational crime prevention, combined with a traditional risk management process, can reduce residual information security risk.	✓	✓	✓	-	-	-
	Straub (1990)	Through empirical research, the author demonstrated how security countermeasures that include deterrent administrative procedures and preventive security software can significantly lower computer abuse.	✓	✓	✓	-	-	✓
	McLean (1992)	Proposed the use of marketing campaigns to raise security awareness.	✓	✓	-	-	-	-
	Bagchi & Udo (2003)	Used the modified Gompertz forecasting model to analyze the growth patterns of computer and Internet crimes. The authors found that a relationship exists between security breaches and the usage of some security technologies.	✓	✓	-	-	-	✓
	Straub & Nance (1990)	Used general deterrence theory to demonstrate how security measures, such as computer security awareness and security software, can help deter computer abuse.	-	-	✓	✓	-	✓
	Chinchani, Iyer, Ngo, & Upadhyaya (2004)	Proposed a target-centric threat assessment model to address complex threats by identifying and then quantifying these threats.	-	✓	✓	-	-	✓
Insider threat models	Lehmann (1981)	Proposed a tool that utilizes audit trails to enhance investigations once a security violation is detected or suspected.	-	-	✓	-	-	✓
	Bradford & Hu (2005)	Discussed augmenting intrusion detection systems with forensics tools to enhance the discovery and prosecution of internal attacks.	-	✓	✓	✓	-	-
	Siponen, Pahnila, & Mahmood (2007)	Proposed a model to explain employees' adherence to IS security policies by integrating the general deterrence theory and the theory of reasoned action with the protection motivation theory (PMT).	✓	✓	✓	✓	-	✓
	Melara et al. (2003)	Presented an insider attack model using systems dynamics and proposed policies to minimize the risk of security failures or at least to reduce the extent of damage in the event of an insider attack.	-	✓	✓	-	✓	

	Siponen & Vance (2010)	Used a theoretical model based on neutralization theory and sanctions of deterrence theory to enhance the understanding of IS security policy violations. The authors highlight the need to take into account neutralization factors when developing and implementing security policies and practices	-	-	-	✓	✓	✓

Since we look at the aggravating variables from a malicious threat perspective, we view insiders' motivation to attack from the point of view of the six neutralization techniques (Siponen & Vance, 2010). We argue that viewing insider threats through the lens of neutralization theory helps in exploring some of the dynamics of these threats from a self-motive perspective. However, in addition to the insider's motivation to attack, there are other insider threat variables that are beyond the realm of neutralization. The above analysis leads us to formulate the following exploratory research question: "What are the aggravating variables that eventually accumulate and trigger insider attacks in organizations?"

Insider Attack Motives and the Role of IT Controls

Despite the lack of theoretical and empirical evidence on the aggravating variables of insider threats, our review of the related literature helped in deriving an a priori model that captures the tentative pattern of aggravating variables. Taking this a priori model as a starting point, we adopt an exploratory research approach to derive a better-validated theoretical model inductively from multiple case study data.

A key information security problem for organizations is the lack of employee compliance with information security policies (Ernst & Young, 2008; Puhakainen, 2006, cited in Siponen & Vance, 2010). In their research on employee security policy violations, Siponen and Vance (2010) state that employees may use neutralization and rationalization techniques to justify or minimize the perceived harm of their policy violations. As such, we propose our first proposition:

> **Proposition 1**: Insiders use rationalization and neutralization to justify malicious actions/IT control violations.

Internal controls are policies, procedures, practices, and organizational structures put in place to reduce risks (Kim, Robles, Sung-Eon, Yang-Seon, & Tai-Hoon, 2008). Appropriate controls are necessary to protect organizations from legal suits for negligent duty, computer misuse, and data protection violations (Dhillon & Moores, 2001). While a "control framework is a recognized system of control categories that covers all internal controls expected in an organization" (IIARF, 2002, cited in Liu & Ridley, 2005, p. 2), an internal control provides reasonable assurance regarding the achievement of objectives in the area of operational efficiency, reliability of financial reporting, and regulatory compliance (Pathak, 2003). Today, the adoption of IS control frameworks is on the rise due to increasing pressures to comply with various data protection laws and regulations.

Given that best practices in IS security control focus almost exclusively on implementing technological controls, an effective defense against insider attacks encompasses technology-based approaches and an understanding of employees' behavior (Martinez-Moyano, Rich, Conrad, Andersen, & Stewart, 2008). Thus, managing information security can only be adequate if the emphasis on IT control goes beyond technical controls and incorporates procedural controls that consider business processes, policies, procedures, and organizational issues (Choobineh, Dhillon, Grimaila, & Rees, 2007; Ifinedo, 2009; Kruger & Kearney, 2006). Moreover, employees' lack of compliance with IS security policies is a key problem that security managers encounter in organizations (Siponen & Vance, 2010). As such, we propose our second proposition:

> **Proposition 2**: Disregard for or overlooking of technical and non-technical IS security mechanisms (policies and procedures) by company employees is an important factor in aggravating IS security violations.

User participation in IS security programs is an important factor in mitigating the incidence of intentional or accidental disregard for security policies. Further, the role of training and education as a proactive security approach remains relevant (Cone, Irvine, Thompson, & Nguyen, 2007; George et al., 2008; Puhakainen & Siponen, 2010; Thomson & von Solms, 1998). In this respect, organizational security controls that can detect, prevent, or minimize an IS security breach can only be effective if the people who are managing the IS in the organization are aware of these controls and adhere to them (Spears & Barki, 2010). As such, we propose our third proposition:

> **Proposition 3**: Ineffective communication of IS security policies and procedures increases the likelihood of insider attack.

The above three factors—namely, neutralization, disregard for IT security policies and procedures, and non-communication of IT security policies/procedures—account for the interaction of numerous dynamic variables in a successful insider attack. Moreover, in their single case study of a successful insider attack, Melara et al. (2003) note from a systems dynamics perspective that numerous precursors contribute to a malicious attack, which can include management actions or inactions. Similarly, looking through the lens of the dynamic trigger hypothesis, a chain of events can lead to an insider attack, and, despite being scattered, these events can be detected if the approach to them is properly structured. Therefore, identifying the sequence and pattern of these precursors would make predecessor factors more conspicuous and would therefore improve the chance of detecting them (Andersen et al., 2004). Consequently, the dynamic nature of the interplay among many data breach precursors leads to our fourth proposition:

Proposition 4: A series of precursors leads to a successful insider attack.

Table 3 summarizes the research question and the underlying propositions. We argue that the aggravating threat variables stem from four major factors (i.e., insiders' neutralization of malicious actions, employees' disregard for/ overlooking IT controls, management's poorly communicating policies, and a series of events/actions/inactions (precursors) that can lead to a successful malicious act).

Table 3: Research Question and Propositions

Research question	What are the aggravating variables for insider threats in organizations?
Proposition 1	Insiders use rationalization and neutralization to justify malicious actions/IT control violations.
Proposition 2	Disregard for/overlooking of technical and non-technical IS security mechanisms is an important factor in aggravating IS security violations.
Proposition 3	Ineffective communication of IT controls (security policies and procedures) increases the likelihood of insider attack.
Proposition 4	A series of precursors leads to a successful insider attack.

By adopting Yin's (1994) deductive approach, our multiple case study explains as far as possible the relationship between the dependent variable "insider threat" and the tentative pattern of independent "aggravating variables " we identified via the literature review, which we posited to be influencing triggers of insider threats.

IV. RESEARCH METHODOLOGY AND FINDINGS

Methodology

The underlying approach we used for this research study is interpretive. This approach assumes that access to reality is only possible through social constructions such as language, consciousness, and shared meanings (Myers, 1997). Because our study is exploratory in nature, we chose a case study research methodology since it "is a common way to do qualitative enquiry" (Stake, 2003, p. 443). Moreover, it "investigates a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident" (Yin, 1994, p. 13).

Following Yin's (1994) suggestion, we selected the sites not only on an opportunistic basis (as access to companies who are willing to report internal data breaches was obviously limited), but also based on firms' diversity (i.e., in their characteristics, industry, size, and ownership model). The case study's design, shown in Table 4, applies criteria used to assess IS case studies as Dubé and Paré (2001) outline. For this study, we selected cases from organizations in Dubai (United Arab Emirates) that have experienced insider attacks.

Table 4: Design of the Case Study (Adapted from Dube & Pare, 2001)

	Criteria	Description
Design of the case study	Research's purpose	Stated in Section 1
	Research questions	Stated in Section 3.
	Single versus multiple-case design	Multiple cases—three cases in three different organizations that have experienced insider attacks.
	Selection of case(s)	Organizations willing to narrate their cases of insider threat longitudinally for the purpose of research.
	Unit of analysis	Interviews with IT managers and IT application/strategy managers in the selected organizations.
	Research context	Cross-sectional study conducted over a period of fourteen months.

Research Findings

Out of the fourteen organizations we approached over a period of fourteen months to share and narrate cases of insider threats in their organizations, six consented, and, out of these six cases, only four fit the "insider threat" category. Since two cases were from the same sector, we report herein a total of three case studies. Hence, in this study, we analyzed three cases (hereafter referred to as cases A, B, and C). Due to the sensitive nature of the study, the consenting organizations requested anonymity. The insiders had different profiles and motives across the three case studies. The first incident (case A) involved an employee affiliated with an outsourcing partner who was assigned to write software code to integrate two financial systems. The second incident (case B) involved an employee who was asked to resign after two weeks' time for reasons of poor performance, and the third incident (case C) involved an application support staff member who had access to a bank's transaction processing system. The first and third cases involved manipulation of financial data for profit, while the second case involved the theft of custodial data and trade secrets. Table 5 provides the case profile of the three organizations.

Table 5: Profiles of the Case Studies Used

Criteria	Case A	Case B	Case C
Sector	Hospitality	Event management	Banking
IT controls	COBIT	No evidence of any IT control framework	ITIL, industry IS security standard
Breach reported to law enforcement agencies	No	No	No
Type of data breached	Financial	Custodial/ company secrets	Financial
Respondent (interviewee)	IT assistant manager	IT application manager	IT strategy manager
Approximate number of employees	300	100	1200
Approximate number of systems	25 servers and 150 computers	15 servers and 75 computers	200 servers and 1400 computers

We initiated the empirical stage of the research during the second quarter of 2012, which continued until the final quarter of 2013. We transcribed the interviews and cross-checked a few gray areas of the transcripts with the respondents through second follow-up interviews. We analyzed the five transcripts followed the five steps of qualitative analysis; namely, tidying up the data, finding items (the specific things in the data set that researchers code, count, and assemble into research results), creating stable sets of items, creating patterns, and assembling structures (LeCompte, 2000). We accomplished the first three steps by categorizing the raw data into themes based on the four propositions (rationalization, disregard for technical and non-technical IT controls, role of communication, and multiple triggers). The remaining two steps corroborated or negated the propositions and thus answered the research question. This deductive approach leads to inductive reasoning where we extracted specific variables under each theme to create patterns and assembling structures. The initial step involved transcribing the data using Express Scribe software and importing the digital text into the qualitative analysis software NVIVO.

Case A (Insider as an Authorized Business Partner)

The company outsourced the task of integrating its financial systems and hotel management system (HMS) to an IT company contracted to develop various software integration modules in which "they needed to test different cases and see the integration and all the stuff between systems" (IT assistant manager). The system integration required that, when a guest booked a room online with a credit card, the details of the payment transactions were transferred to the financial information system (FMS). Since FMS were the most secure system, everything was pushed on to the FMS from the HMS (instead of pulling the data) where the FMS received the data to do the consolidation. During the coding phase, the programmer, assigned by the outsourced company, entered a malicious code whereby, for every online booking transaction made, Emirati Dirham (AED) 5 (~US$1.36) was added to the original bill, and this sum was credited to his personal bank account. This amount was not visible in the HMS system but, when this information was pushed to the FMS , this amount was added and was reflected in the customer's credit card statement a month later. The irregularity was discovered by the company's IT personnel during integration project's user acceptance testing (UAT) phase. According to the respondent, one of the reasons the company's financial network was breached was because they took "minimal precautions" when taking hiring new people. Moreover, according to the respondent, the incident happened because "we did not have the expertise in the [our] team to analyze what this guy was doing".

Aggravating Variables (Neutralization): Case A

Two sets of variables are evident in this case, one on the part of the insider and the other on the part of the employer (Figure 2). These sets of variables were, respectively, active and latent factors that led to neutralization. First, the system integration task was performed by a lone programmer who, according to the respondent, "was a terrific developer. Everybody knew his talents and so he had the respect of his colleagues", which was a contributing variable. Secondly, during the programming phase, the programmer asked for either overtime or more resources (programmers) to finish the job in the scheduled time frame. His company denied this request. From the organizational side, the first variable is inadequate IT controls during the induction of outsourced personnel where the respondent said "so now what happens was when these people come on board, we used to take minimal precautions." Commenting on the second security flaw, the respondent stated that one of the "greatest threats" facing the IT department was the constraint on the IT budget, which forced outsourcing organizations to cut costs and led to undesirable incidents. A third aggravating factor was the fact that the company "did not have the expertise in the team to analyze what this guy was doing" (IT assistant manager). Finally, while the outsourcing contract was clear in terms of specifying the end results, it was not clear what software development tools and platforms will be used, which led the respondent to state that "Probably he was working on Java, with interface to an SQL database". Figure 2 summarizes the aggravating variables that led to neutralization in this particular case.

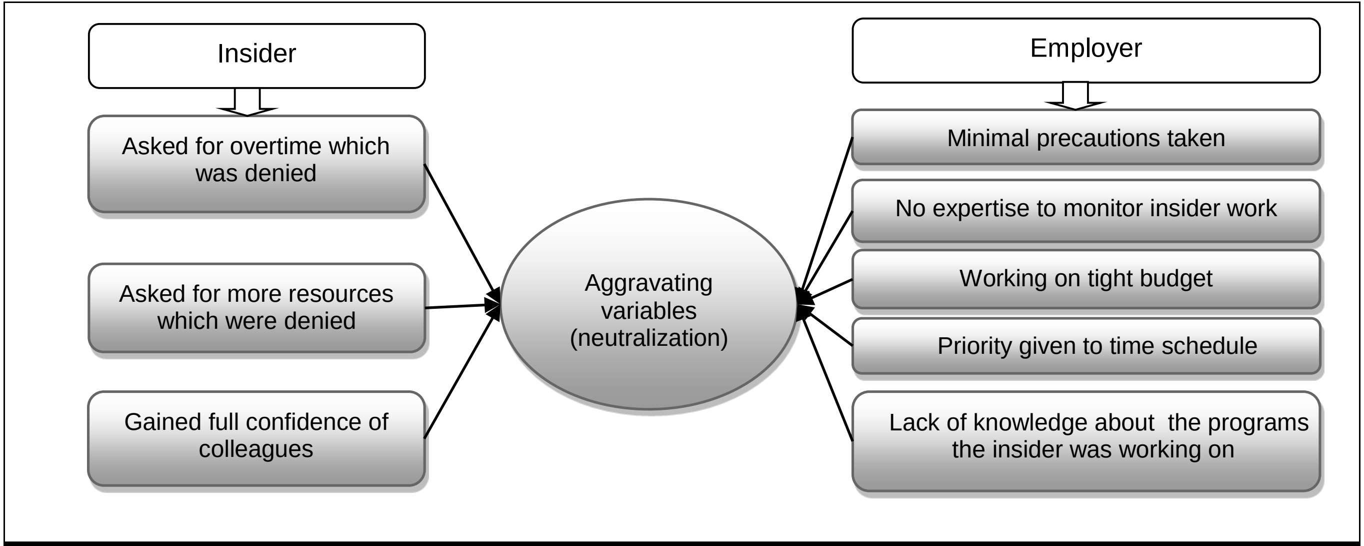

Insider
Asked for overtime which was denied
Asked for more resources which were denied
Gained full confidence of colleagues
Aggravating variables (neutralization)
Employer
Minimal precautions taken
No expertise to monitor insider work
Working on tight budget
Priority given to time schedule
Lack of knowledge about the programs the insider was working on

Figure 2. Aggravating Variables Leading to Neutralization (Case A)

Role of Compliance: Case A

The organization had a policy of segregating outsourced personnel from the production network". Thus, according to the respondent, the organization did not only apply its policy of granting the business partner "access to a separate network", but it also made "sure that all his equipment was scanned and then compliant with the policies". However, according to the respondent, the issue was that "here we have a situation wherein OK, you provide him everything as per the policies and as per the compliance work, but still this guy is doing something within these limits and he is still able to pose a threat" due to the "minimal IT controls in place". Regarding the role of technical controls the respondent stated: "then you have…another question now. Even after the evolution of technology, how can these kinds of things be minimized? I think it's again a…it's a very questionable situation". This statement implies that the technical controls were inadequate and, at the same time, indirectly points out the role of non-technical controls in IS security. Figure 3 summarizes the aggregative variables related to IT controls for case A.

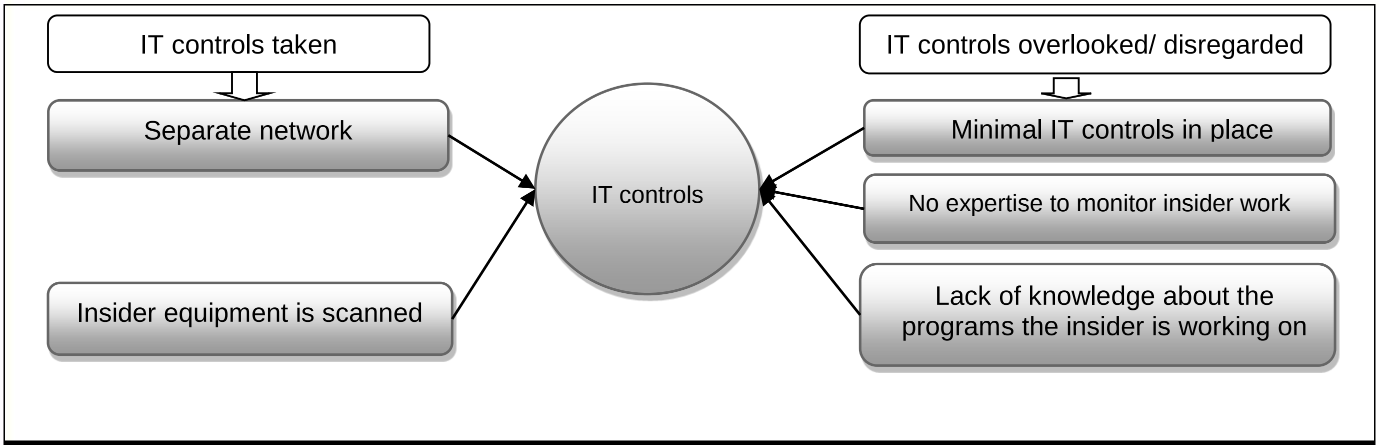

IT controls taken
Separate network
Insider equipment is scanned
IT controls
IT controls overlooked/ disregarded
Minimal IT controls in place
No expertise to monitor insider work
Lack of knowledge about the programs the insider is working on

Figure 3. Aggravating Variables for IT Controls (Case A)

Communication of Policies: Case A

In this case, the organization had policies and procedures that it communicated only to select groups of employees via orientation sessions. In this regard, the respondent stated that the company provided a single training session only to newly recruited junior staff at orientation because of the misconception that newly recruited junior staff are more prone to make mistakes than others. Middle- and senior-level employees were not provided with any orientation or training at all. Regarding the communication of policies to outsourced staff, the respondent stated that "we have communicated our policies and procedures to the project manager [of the outsourced company] and we don't know whether these have been communicated to their employees here". In this case, the company depended on the outsourced company to communicate the policies to its employees. Figure 4 depicts the aggravating variables related to communication policy for this particular case study.

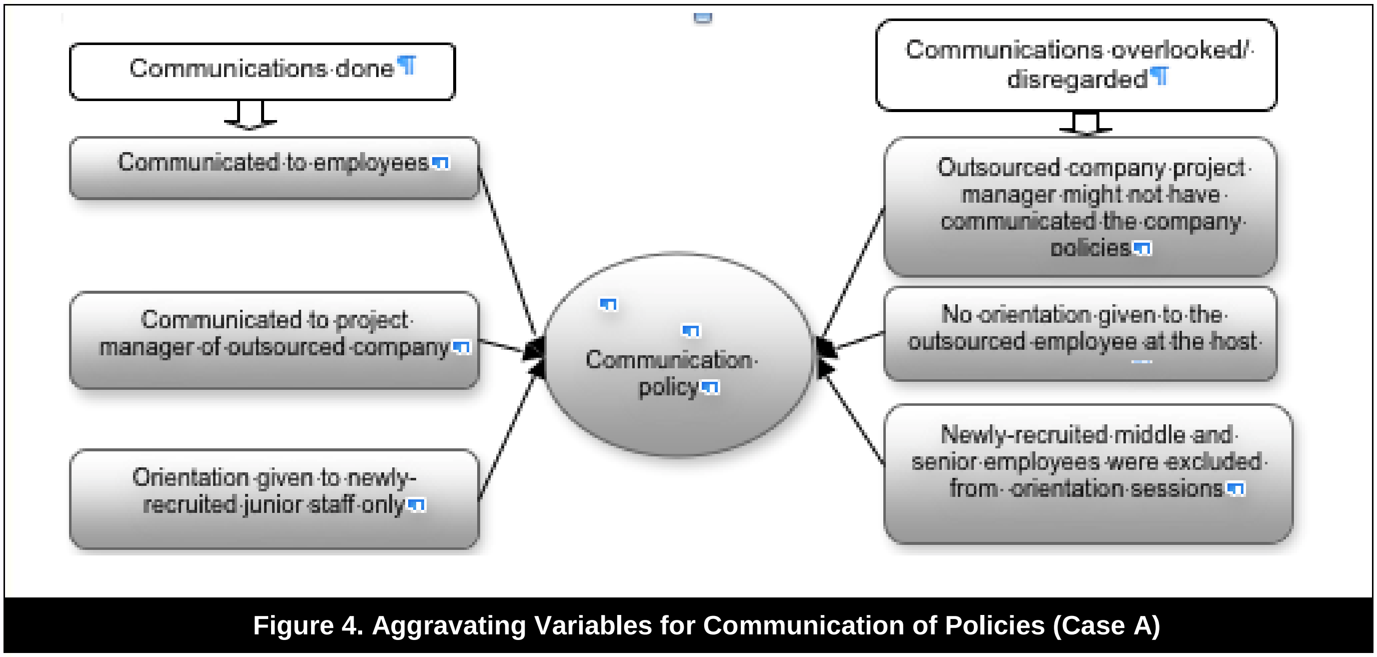

Communications done
Communicated to employees
Communicated to project manager of outsourced company
Orientation given to newly-recruited junior staff only
Communication policy
Communications overlooked/ disregarded
Outsourced company project manager might not have communicated the company policies
No orientation given to the outsourced employee at the host
Newly-recruited middle and senior employees were excluded from orientation sessions

Figure 4. Aggravating Variables for Communication of Policies (Case A)

Case B (Insider as an Employee Who Was Given Two Weeks to Leave)

This case involved a secretary in an event management company who was asked to leave due to poor performance. She was the secretary to the CEO and, since there was nobody else to take over her job, she was given two weeks' notice prior to leaving until a suitable replacement could be found. During this time, she used her privileged access (being the secretary to the CEO) to access sensitive documents, contracts, and the CEO's profile, and emailed them to the next company she was moving on to (in this case a competitor). The IT staff detected this breach through an IT control that was configured to send an alert when the email server detected certain keywords.

Aggravating Variables (Neutralization): Case B

The foremost motivational factor behind this breach was the secretary's discontent when she was asked to leave due to poor performance. In the meantime, she found a new job opportunity with a competitor and this prompted her to channel the company's custodial data and trade secrets to this competitor. In this case, the company did not take the necessary measures to limit her access to sensitive data once she was notified of her termination. In other words, she maintained her access based "on trust, because HR knew that this lady was going but they were keeping her for a short period of time" and "they didn't understand the amount of threat that this person could pose to the entire organization" (IT application manager). When the human resource personnel confronted the secretary regarding this data breach, she claimed that she was simply taking the templates that she created. Figure 5 illustrates the aggravating variables leading to neutralization for this case.

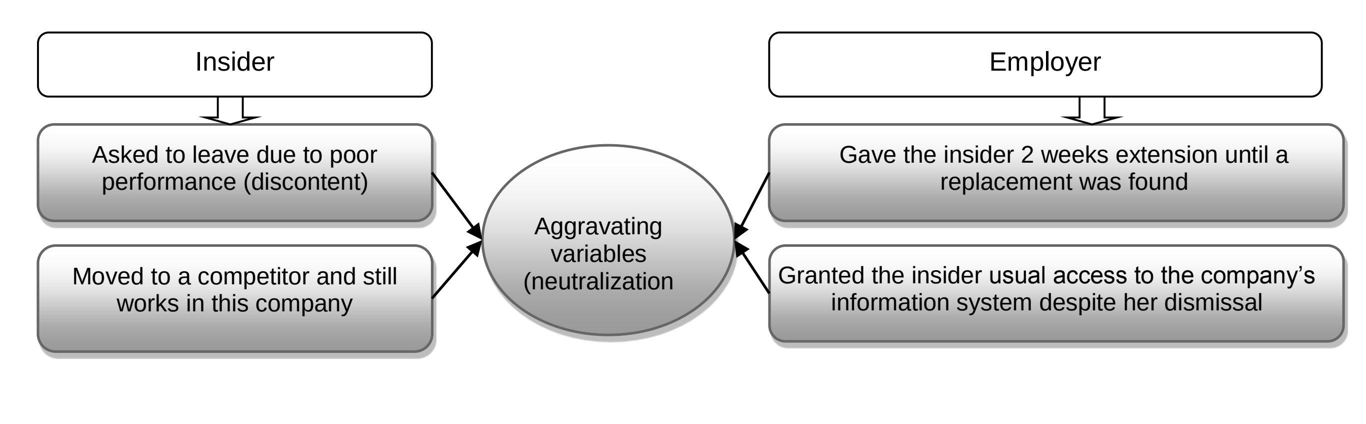

Insider
Employer
Asked to leave due to poor performance (discontent)
Moved to a competitor and still works in this company
Aggravating variables (neutralization
Gave the insider 2 weeks extension until a replacement was found
Granted the insider usual access to the company's information system despite her dismissal

Figure 5. Aggravating Variables Leading to Neutralization (Case B)

Role of Compliance: Case B

According to the respondent, during the employee's final two weeks of work, "nobody understood what she was doing" until someone on the IT team noticed "weird attachments going from one particular IP address". The data breach was detected thanks to technical controls. The company used IBM Lotus notes as the mail server: they configured policies in the outgoing email server with certain keywords, and an alert would be triggered if these keywords were detected. When they checked the secretary's inbox, they found out that she had sent copies of high-profile contracts and the curriculum vitae of the CEO to her prospective employer. The breached information contained custodial information and trade secrets. According to the respondent, the presence of IT controls stopped the breach midway. Here, the presence and use of technical controls were effective to the extent of preventing further data breaches, but not effective in preventing it at the outset. From a proactive perspective, the respondent stated that "when you put down your papers [resign or are asked to leave], your rights [IT] are trimmed. So this was overlooked". The respondent also mentioned the intensive monitoring process required when a person resigns or is dismissed. In this regard, the respondent stated that "during the notice period, your activities are closely monitored, but this was not done" in this case. Figure 6 illustrates the aggravating variables related to IT controls in this particular case.

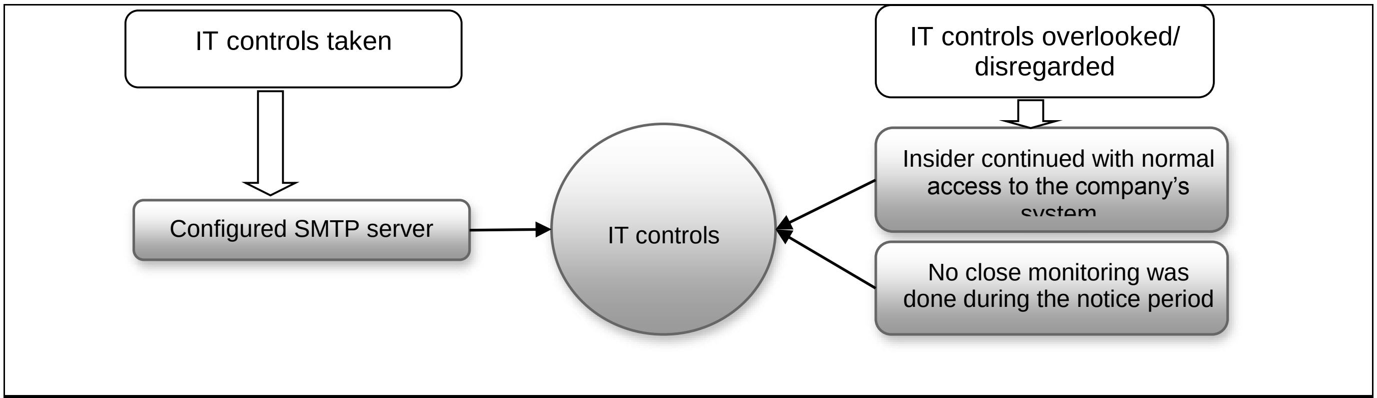

IT controls taken
IT controls overlooked/ disregarded
Configured SMTP server
IT controls
Insider continued with normal access to the company's system
No close monitoring was done during the notice period

Figure 6. Aggravating Variables for IT Controls (Case B)

Communication of Policies: Case B

According to the respondent, one factor that prompted the insider to leak company data was her possible lack of awareness of its data privacy policies. In this regard, the respondent stated “ if she’s copying the templates, why do you take the content inside the templates” and to date, the company “doesn’t know what kind of information has gone out”. When probed further, the respondent said that the case clearly indicated the lack of awareness of IT polices among staff. Regarding policy enforcement, the respondent’s comment that “nobody bothered to enforce [IT policies]” was a clear indication that the communications of IT policies were not effective, thus differentiating “communication” from “effective communication”. When asked about continuous training in IT policies and the relevance of that training, the respondent stated that “managers (IT) don’t like to send the staff for training since the priority is to finish the work” and “department heads should know the importance of training”. Figure 7 summarizes the aggravating variables of policy communication for this case study.

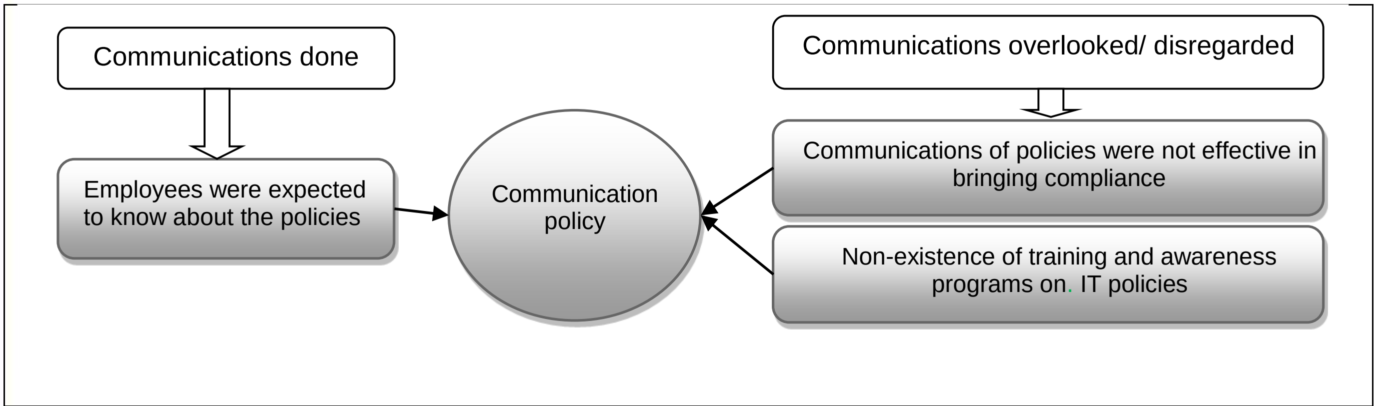

Communications done
Employees were expected to know about the policies
Communication policy
Communications overlooked/ disregarded
Communications of policies were not effective in bringing compliance
Non-existence of training and awareness programs on. IT policies

Figure 7. Aggravating Variables for Communication Policies (Case B)

Case C (Insider as Trusted Key IT Support Staff)

This case involved a local bank that provided a wide spectrum of retail and commercial banking services. The insider was a key member of the company’s application support staff who used his privileged access to insert a malicious .xls file into the bank’s batch file transfer system. The malicious file automatically executed an unauthorized transaction in favor of the insider. The bank’s corporate accounts involved monthly debit transactions whereby employees’ monthly salaries were credited to their bank accounts using a special .xls spreadsheet. This file contained the employee ID, name, account number, days worked, deductions, and amount to be debited along with the electronic payment. The double-entry process of debiting the corporate account and crediting the employee account was done through batch processing. The insider replicated the genuine salary transfer process by creating a malicious .xls file with a list of charges (credited to his account) that were executed along with the normal .xls file during the salary transfer process. Hence, when the salary was transferred to the employee’s account, the .xls file was activated and a small amount of 1 or 2 dirhams (less than $1) was debited from the bank’s corporate account and credited to the insider’s account. Since the bank had hundreds of corporate customers, the breach affected thousands of individuals.

The malicious act was discovered when, on one occasion, the operating (non-IT) staff member encountered a transaction processing error, which they suspected might be the result of an accounting error. Following the standard procedures, the employee called the application support person (the “insider”) to resolve the issue. However, in this particular case, the insider could not be reached and hence the operating staff member had to escalate the issue to a tier 2 expert agent who came to the server room to investigate the incident. While examining the batch file transfer system, the agent detected some suspicious transactions in which small amounts were debited from the bank’s corporate accounts and credited to the insider’s account in the same bank. It was revealed that a malicious accounting entry had triggered the fraudulent transaction.

Aggravating Variables (neutralization): Case C

In this case, the respondent identified three latent aggravating variables, each from the insider’s and management’s perspective. First, the insider had “a luxurious lifestyle and [was] living beyond his means”, which management was well aware of before the breach was detected but did not give much consideration. Second, the trust placed in the insider and the privilege given to him to manage the bank’s transaction processing system was another contributing factor. Other than that, the respondent could not find any aggravating variable on the part of the organization that would create discontent for the insider. While the habit of spending beyond his means gave the insider a motive to insert the malicious code, “the confidence placed in him [was] the only and main factor”, while the “free hand given by the management" along with the "privileged access" provided the key drivers for the insider to commit the data breach (IT strategy manager). Figure 8 shows the aggravating variables leading to neutralization for this case.

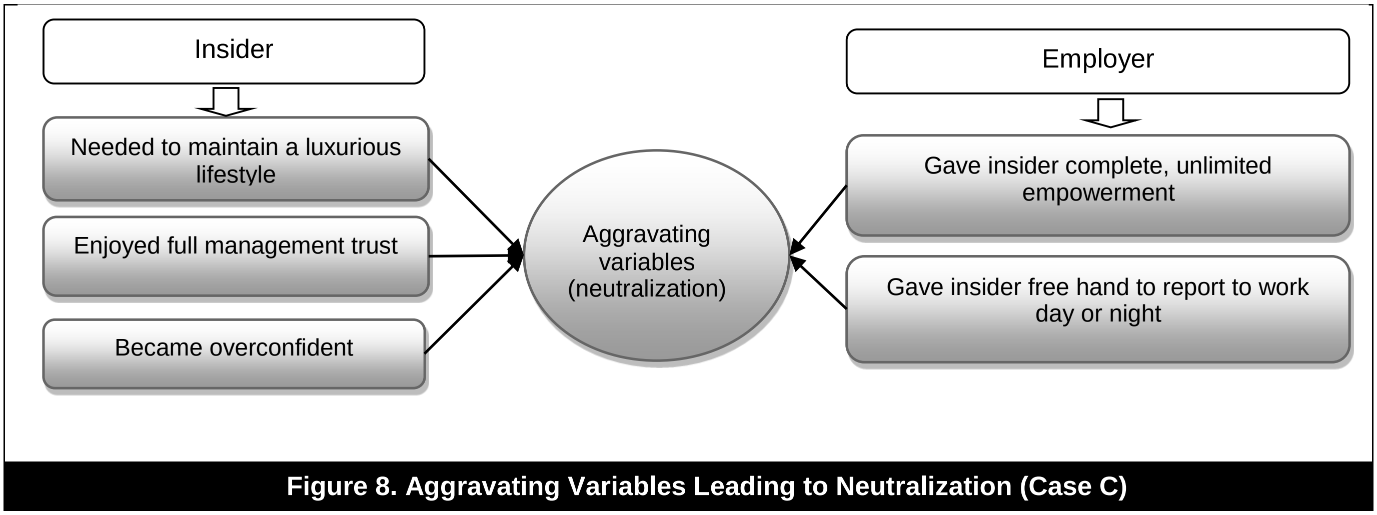

Insider
Needed to maintain a luxurious lifestyle
Enjoyed full management trust
Became overconfident
Aggravating variables (neutralization)
Employer
Gave insider complete, unlimited empowerment
Gave insider free hand to report to work day or night

Figure 8. Aggravating Variables Leading to Neutralization (Case C)

Role of Compliance: Case C

From a compliance perspective, the predominance of non-technical controls should not be overlooked just because the insider was a key IT staff member. While technical controls may prove futile, management-related factors relating to three non-technical controls were overlooked/disregarded.

First, the member of the bank's application support staff "was empowered to access live systems to support the banking application system" (using high privilege access), where "the intention was to keep the banking services running uninterruptedly" since "the bank had a large network of branches and a big client base" (IT strategy manager).

Second, because "he had a free hand to report to work at any time in the morning and work any time", the malicious act was performed at times when most of the bank's staff was off-duty (IT strategy manager).

Third, "due to the criticality of the banking operations, he had been vested with high respect and trust by the IT department and management" (IT strategy manager). While "empowerment" and "trust" are essential elements of a working environment, the absence of proper monitoring mechanisms normally embodied in IT controls that are up to industry standards may facilitate fraudulent activities in financial institutions. This was evident from the respondent's statement that "his work was never supervised or audited as the bank financial transactions were performed without any interruptions or complaints (IT strategy manager). The reason was that he was supporting 24x7 operations of the banking system"(IT strategy manager). When asked what the bank could have done to avoid the breach, the respondent replied that the "developer should not have access to a live environment" and that, if controls had been implemented, the breach would "not have happened". Hence, "nobody suspected that he would do such an act". When asked about the IT controls at the time of the incident, the respondent replied that the bank had implemented ITIL and industry-standard IT controls related to IS security, but not the COBIT framework, nor the ISO 27 K standard.

Figure 9 shows the aggravating variables related to IT control for this case. All these latent variables acted as precursor events that led to the malicious act.

Communication of Policies: Case C

According to the respondent, the bank had meticulously communicated its security policies ("There was not any lapse in any communication"), and the bank also conducted a "continuous training and awareness program" for its IT staff; in addition, IT polices were communicated "appropriately". When further quizzed about any potential lapses in communicating security policies to the insider, the respondent fully defended the bank's communication program at that time. Figure 10 illustrates the aggravating variables of policy communication for this case.

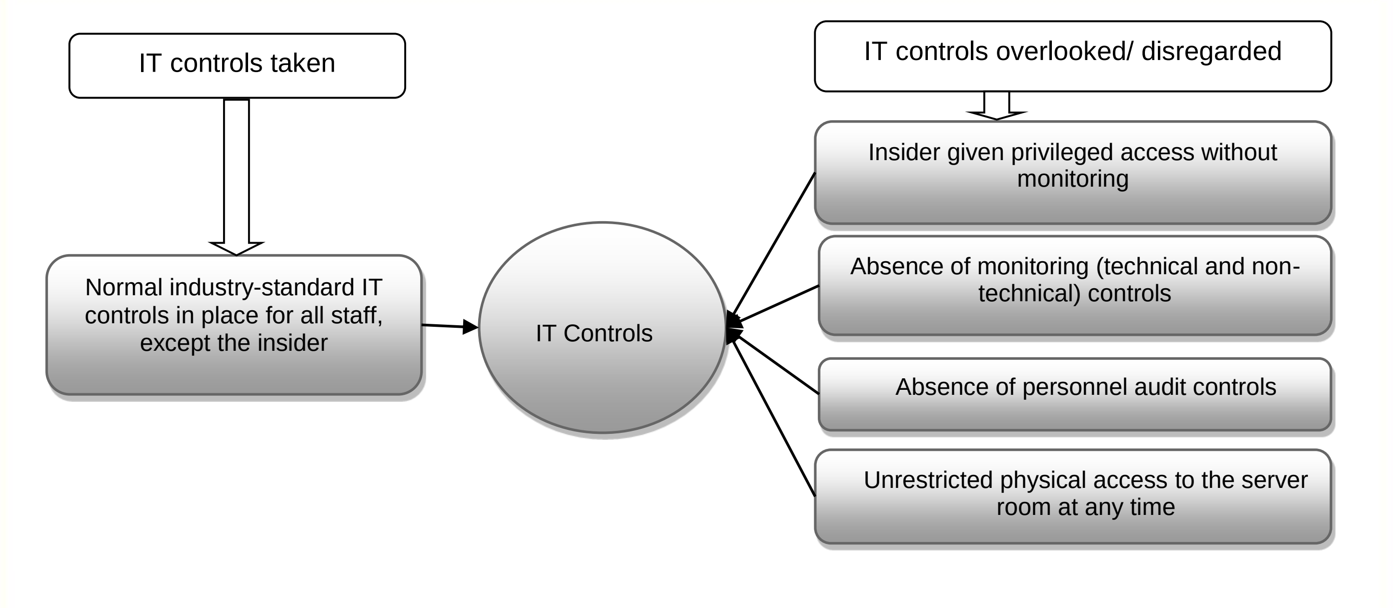

IT controls taken
IT controls overlooked/ disregarded
Insider given privileged access without monitoring
Normal industry-standard IT controls in place for all staff, except the insider
IT Controls
Absence of monitoring (technical and non-technical) controls
Absence of personnel audit controls
Unrestricted physical access to the server room at any time

Figure 9. Aggravating Variables for IT Controls (Case C)

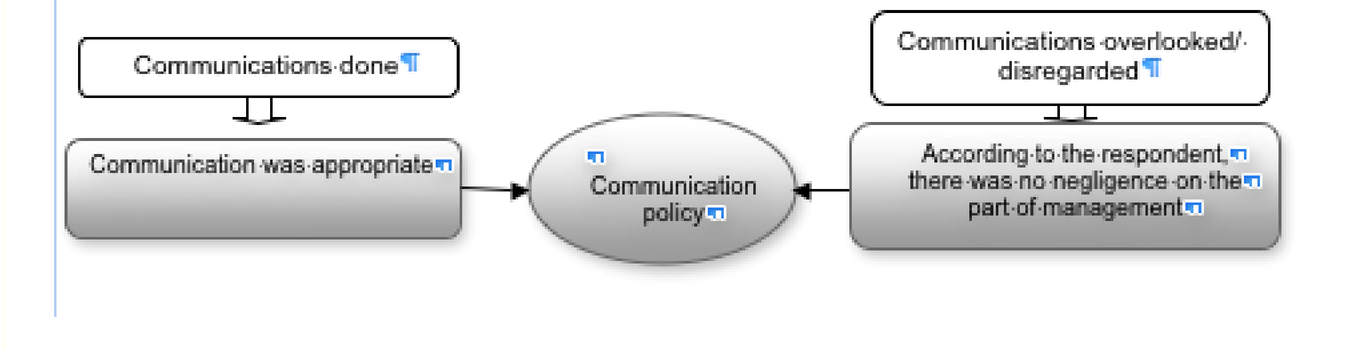

Communications done¶
Communications overlooked/ disregarded¶
Communication was appropriate
Communication policy
According to the respondent, there was no negligence on the part of management

Figure 10. Aggravating Variables for Communication of Policies (Case C)

V. DISCUSSION

While in Section 4 we focus on a multiple case analysis with a reasonable element of interpretation, in this section, we go one step further and identify patterns and assemble the overall structure of the variables into deduced propositions and induced themes to answer the research question. Given that the four propositions corroborate the responses found in the interview transcripts, we derived a prescriptive model, henceforth referred to as the insider threat aggravating variables (ITAV) model. This ITAV model follows a two-tier simple influence diagram that delineates the dependent and independent variables and the relationships among them (Palvia, Midha, & Pinjani, 2006).

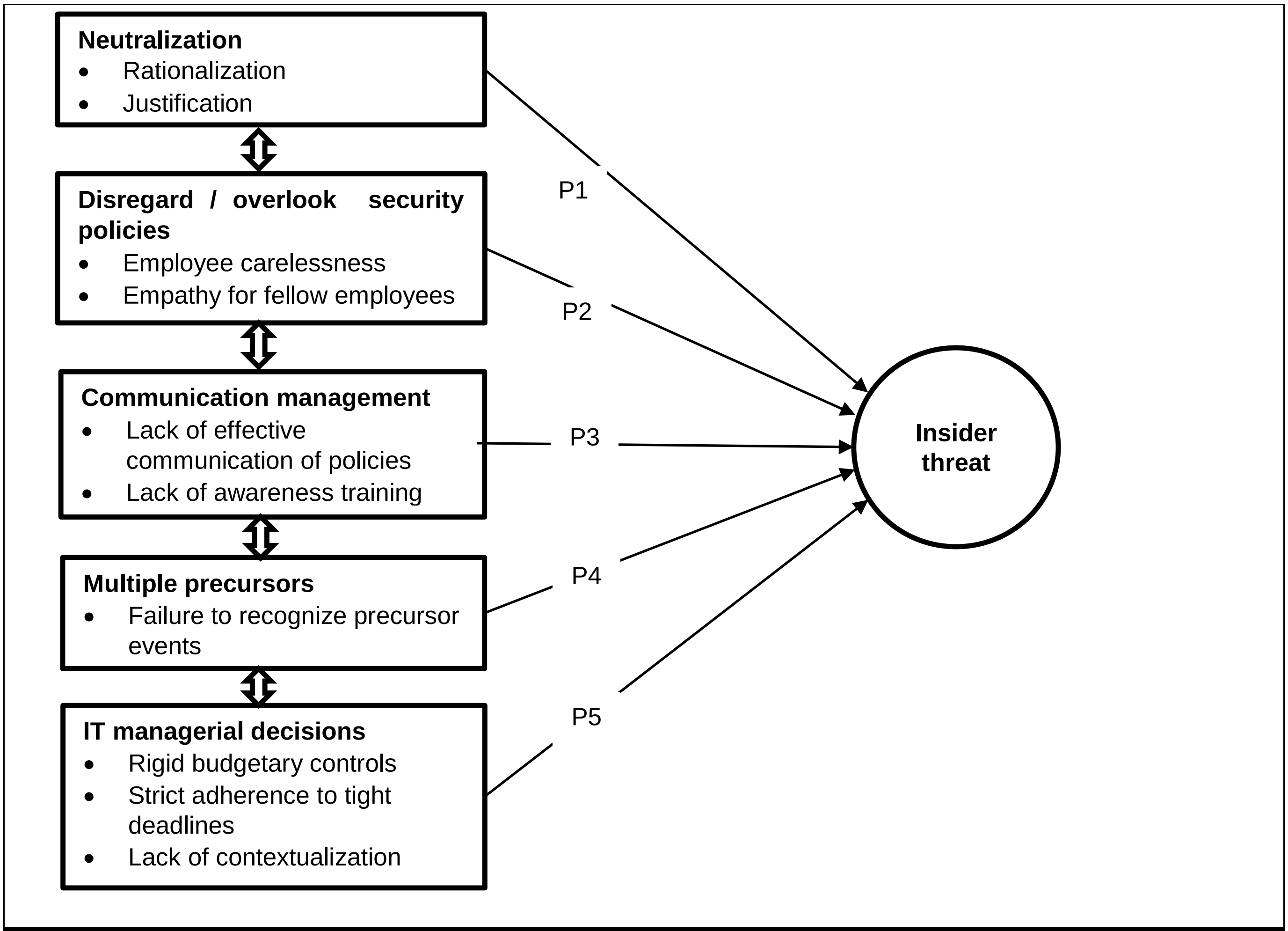
As Figure 11 shows, the ITAV model identifies the five theoretical constructs, the attributes in each construct, the associations, the state space, and the events they cover, (Weber, 2012). The constructs not only support the four propositions but also lead to a fifth proposition:

> **Proposition 5:** IT decisions by management affect the security threat level of organizations.

In particular the above proposition leads to two sub-propositions:

- Economizing the allocation of IT security resources leads to increased security risks.
- Poor contextualization of contingent or emergent security scenarios with relevant IT controls leads to increased security threats.

Our analysis of cases A-C indicates that multiple precursor events triggered a successful data breach by malicious insiders, which justifies the interdependent associations among the constructs. The state space of our model encompasses only those employees with malicious intent, and those employees who have normal and/or privileged access to organizational information systems. Currently, the events in our model cover deliberate modification and disclosure of corporate data.



Neutralization
Rationalization
Justification
Disregard / overlook security policies
Employee carelessness
Empathy for fellow employees
Communication management
Lack of effective communication of policies
Lack of awareness training
Multiple precursors
Failure to recognize precursor events
IT managerial decisions
Rigid budgetary controls
Strict adherence to tight deadlines
Lack of contextualization
P1
P2
P3
P4
P5
Insider threat

Figure 11. The insider Threat Aggravating Variables (ITAV) Model

Proposition 1

Proposition 1 states that insiders use rationalization and neutralization to justify their malicious acts or to bypass IT controls. This proposition was true in all three cases we studied. In addition, two types of aggravating variables are evident in all the three cases: active and latent variables. While active variables are explicit, latent variables are implicit and support the active variables. For example, in the first case, the insider (the outsourced employee) gained the complete confidence of his colleagues (latent variable), and thus no one suspected him of manipulating the program, which prevented the company IT personnel from monitoring him (latent variable on the employees' part). In this regard, Colwill (2009) states that outsourcing can lead to the fragmentation of protection barriers and controls that increases the number of people treated as full-time employees. In all three cases, there were active variables that prompted the insider to breach the IT security perimeter. In the third case, the presence of latent variables, instead of active variables led to the data breach. In this case, the insider had free reign that, coupled with an absence of managerial oversight and/or IT controls, led to the insider attack.

Proposition 2

This proposition states that the overlooking or disregarding technical and non-technical IS security mechanisms is an important contributing factor in aggravating IS security violations. While overlooking/disregarding existing IT controls is an influencing factor, an absence of IT controls can also contribute to data breaches. In the first case study, the company took reasonable (i.e., adequate in terms of industry standards) precautions, but three latent factors that went unnoticed (minimal precautions, no monitoring, no in-house expertise) led to the breach. In this case, however, the aggravating factor was “neutralization” rather than the presence of the three latent factors (minimal IT controls in place, no expertise to monitor insider job, and lack of knowledge of the programs the insider was working on). In the second case, the employee’s termination proved to be the major variable, followed by the lack of IT controls (both active variables). In the third case, the IT personnel’s confidence in the employee (insider) led to them overlooking/disregarding two major IT controls (active variables), which ultimately led to the ongoing data breach. In this respect, Martinez-Moyano et al. (2008) state that an organizational focus on external threats can lead to complacency, which can allow an insider to gain confidence by exploiting known weaknesses in organizational defenses.

Proposition 3

The findings corroborate proposition 3, which states that ineffective communication of IT controls to employees is a factor that can contribute to a data breach. However, as case C reveals, the presence of proper communication concerning IT security policies and procedures cannot by itself safeguard against internal attacks. This finding is in accordance with earlier studies that have found that employee violations of established IS security policies are often due to employees’ negligence or ignorance of these policies (Puhakainen, 2006, cited in Siponen & Vance, 2010; Vroom & von Solms, 2004).

In the first two cases, there was no evidence of ongoing training or orientation on IT controls by the respective organizations/divisions to the outsourced business partner or to their own employees, a situation the respondents confirmed. This finding reflects the need for training IT personnel to think about the different scenarios in which each IT control can be applied or circumvented. Furthermore, IT security and governance controls are inherently generic, which makes it difficult for organizations to come up with controls for each plausible scenario. In this respect, Greitzer, Moore, Cappelli, Andrews, and Carroll (2008) acknowledge that there currently exists a paucity of training, especially innovative training, on insider threats for individuals with different roles and responsibilities in organizations.

Proposition 4

Our study revealed that data breaches by insiders can stem from the cumulative actions of multiple (active and latent) variables, and from insiders’, IT personnels’, and management’s actions/inactions. From the three cases, we suggest that multiple factors can cumulate to trigger an insider attack. Thus, organizations need to take adequate precautions to thwart insider threats because some security layers might be easily penetrated or costly to maintain. Likewise, from a non-technical point of view, it is not economically feasible for all organizations to take all precautions in all aspects of technical and non-technical security while satisfying all employees’ requests, keeping all employees content, implementing all available IT controls, continually communicating polices in an effective manner, and making IT decisions with the greatest diligence and care.

Proposition 5: Management’s IT Decisions

While analyzing and corroborating the interview transcripts with the first three research propositions in Table 3, a fifth category of latent aggravating variables emerged from the empirical data, which we call “IT decisions” (observed explicitly in case A) because these are decisions related to IT made at different management levels. In fact, the existence of two latent variables (cost and time) and the absence of a third variable (contextualization) also contributed to the reported data breaches. In case A, management’s decision to cut costs and not delay their project led to two active variables (rejecting requests for overtime and for additional resources), which, in turn, resulted in the data breach. According to the respondent in case A, the company allocated two experts to go through the entire code line by line to determine the potential malicious code. This endeavor took two months, which calls into question the decision to cut cost and time in the first place.

Contextualization is the process of mapping an emerging or contingent situation with the IT control of a well-drafted policy. We categorized contextualization under “management” since it was management’s responsibility to train employees to map IT controls in different contexts. With regard to contextualization, Koliadis, Desai, Narendra, and Ghose (2010) state that, with increasing legislative and regulatory concerns, the key challenge facing organizations is to understand and communicate high-level compliance policies in natural language, and to interpret them for a particular usage context. These interpreted policies can then be represented in formal language and used to automatically verify compliance of IT/business process executions against the same policies. In this regard, IT personnel should be trained not only in IT controls, but also in interpreting and applying policies in different contexts. This requires training and scenario planning on management’s part.

Cross-Case Analysis

According to Yin (1994), a multiple case design can follow literal replication logic (predicting similar results across cases) or use a theoretical replication strategy (conditions of the case lead to predicting contrasting results but for predictable reasons). Yin (1994) suggests that, initially, three to four cases are satisfactory for a literal replication. In our case, we used literal replication logic to strengthen the robustness and reliability of our findings by constantly comparing and possibly matching the results of one case study with the results of ensuing cases. As Table 6 illustrates, a cross-case analysis shows that, in all three cases, there was an accumulation of multiple events of different magnitude that triggered a data breach, which confirms that no single active or latent variable was sufficient to prompt a successful attack. In addition, since, in most of the cases, the identified patterns associated with insider threats were similar, in the aggregate, we have considerable evidence to support our initial set of propositions (Eisenhardt, 1989). Further, our comparative multiple case approach enabled not only the replication of individual patterns (confirmed by the four propositions), but also the extension of the theoretical constructs by identifying a fifth aggravating variable.

From a threat-prediction perspective, understanding the precursor events provides ample opportunity for management to take proactive actions, which also leads to two important observations. First, our results suggest that no single control can guarantee security in and of itself because each control has its own unique role in a security architecture. As such, a layered defense architecture (Cavusoglu, Cavusoglu, & Raghunathan, 2004) becomes necessary. Secondly, access control and privileges must be properly designed and supervised so that no single person is able to control the system from front to back with unrestricted access (Melara et al., 2003). Through the use of the ITAV model, we illustrate the variables that can help management understand the nature of insider threats and thus guide organizations towards taking proactive steps to eliminate or mitigate the effects of these threats.

Table 6. Cross-Case Analysis Results

Aggregating variable	Case A (hospitality)	Case B (event management)	Case C (financial institution)
Neutralization	Defense of necessity	Defense of necessity/ condemnation of the condemners	Defense of necessity/ Denial of injury
Disregard/overlook security policies	Minimal IT controls in place; overlooking/ disregarding of non-technical IT controls	Technical IT controls used for detection; lack/overlooking/ disregarding of non-technical controls	Overlooking/disregarding of technical as well as non-technical IT controls
Communication management	Lack of re-enforcement of communication; lack of communication to outsourced staff	Lack of communication/training/ enforcement of policies	N/A
Multiple precursors	4 active and 6 latent precursor events	4 active and 2 latent precursor events	10 latent precursor events
IT managerial decisions	Cost and time; lack of contextualization	Lack of contextualization	Lack of contextualization

External Validity

As Yin (1994, pp. 30-32) highlights, the purpose of multiple case study research is not to seek statistical generalization to a larger population—a technique customary in survey research—because individual cases are not sampling units. Rather, the study aspires to theoretical or analytical generalization of "a particular set of results to some broader theory" (Yin, 1994, p. 36) and not to populations. Accordingly, in this multiple case study, we provided analytical generalizations by replicating and expanding the emergent theory of insider attacks variables by deeply analyzing each case and comparing and contrasting the cases with each other. By adopting replication logic and a sequential approach, we were able to progressively acquire convergent patterns about the important mediating factors of insider threats. According to Yin (1994, p 31), in an analytical generalization, a previously developed theory is used as a template with which to cross-check the cases' empirical results and, "if two or more cases are shown to support the same theory, theoretical replication may be claimed". Therefore, it is through this replication logic in our multiple case study design that we strengthen our findings' external validity (Yin, 1994, p. 35).

VI. CONCLUSION AND SUGGESTIONS FOR FUTURE RESEARCH

Drawing on the related literature and by analyzing three case studies concerning organizations from different sectors that experienced insider attacks, we categorized the aggregating variables that led to insider threats into five theoretical constructs; namely, neutralization, disregard/overlook security policies, communication management, multiple precursors, and IT managerial decisions.

Our empirical study contributes to both insider threats research and practice by reducing the gap between these two fields in order to guide managerial actions towards a better understanding of the cues that may announce insider attacks. In particular, through the three case studies examined, we encountered empirical evidence validating the four propositions we identified from previous literature, and also identified a new (fifth) construct that relates to decisions made by IT management that may eventually lead to insider attacks. Our theoretical model explains the “how” (process) and the “why” (reasons) of the insider attack phenomenon; as such, we categorize it under the type 2 theory of explaining and understanding (Gregor, 2006). Our research enabled us to build validated theoretical constructs and propositions from case-based empirical evidence (Eisenhardt, 1989). Accordingly, this contribution provides researchers with real data on insider attacks, which contributes to a better understanding of insider threats’ aggravating variables. This study therefore advances academic research in the area of insider threats by guiding academics towards developing better taxonomies and predictive models for insider attacks. According to Schultz (2002), the most persistent need emanating from research on insider threats is developing predictive models that can assist in preventing insider attacks.

From a practitioner’s perspective, our empirically validated conceptual model for insider threats’ aggravating variables provides practitioners with guidance for developing a more holistic approach for protecting their organizations. Our case study analysis shows that insider attacks can be effectively detected from initial cues, provided that IT personnel are adequately equipped with mechanisms to detect, analyze, and respond to them early on. Hence, our model can guide practitioners to proactively manage insider threats and integrate insider threat mechanisms into the overall risk management process. As Bishop et al. (2008) affirms, if we cannot define the insider threat problem and its underlying factors properly, then we will not be able to come up with a solution. In addition, we can assert that combining insider monitoring mechanisms with overall risk control may increase the probability of detecting insider threats (Yang & Wang, 2011).

A major theme that emerged from our study is the fact that several intertwining factors led to the internal data breaches in our three case studies. In other words, the insiders’ actions alone did not make up a data breach. Rather, it was through additional aggravating variables originating with IT personnel’s and management’s actions/inactions that data breach incidents occurred. In particular, we found that individual behaviors and motives were not the only causal factors behind insider attacks. Put differently, our analysis suggests that insider threats are sometimes the results of circumstances that are outside the realm of those who were directly linked to the threat. A major implication of this finding is the need for organizations to focus their attention beyond the motives behind actual insider attacks and consider other latent technological, managerial, and organizational system defects. Thus, our findings indicate that insider threats are avertable through preventive managerial decisions and actions. Our research also advocates the need for organizations to set up contextually based IT security governance and policies to account for insider data breach risks and minimize them. Such a holistic view of the precursors of insider attacks has not been addressed in the extant literature.

Future research might undertake to further develop the work done here in any of various directions. For instance, although our multiple case study allowed the replication and extension of the results across three different cases among the three individual cases, a more case-based research initiative in different contexts might provide additional literal replications leading to a greater degree of certainty. One of the questions Ifinedo (2009) raises is whether security concerns vary according to socioeconomic contexts. This question might be explored further through an effort to widen empirical research on the five constructs to investigate whether the attributes that define these constructs remain the same or vary across different geographical locations, cultures, and/or sectors. From a similar perspective, since our research focused only on deliberate insider attacks, we would also encourage future empirical studies on internal data breaches that are triggered by unintentional human error. Such studies might then help extend the generalizability of our model to cover the full range of aggregating variables leading to data breaches.

An employee’s attitude is influenced by compliance benefits, compliance cost, and noncompliance cost, which involve beliefs about assessing the consequences of compliance or noncompliance (Bulgurcu et al., 2010). Starting from our second theoretical construct of employees’ actions/inactions with respect to adherence to security policies, further research could identify which of the three compliance factors are dominant in the context of insider threats. In addition, and from an organizational behavior perspective, the motivation factors behind insider attacks could be researched: researchers could examine both the intrinsic and extrinsic moderating factors of these attacks.

Researchers have stated that organizations do not currently place great emphasis on developing aware and responsible information users (Young & Windsor, 2010). In this regard, taking the communication management construct into account, we encourage further research into the optimal communication mix for effectively communicating security policies.

Gupta, Chaturvedi, and Mehta (2011) posit that, if an organization faces external threats from highly skilled perpetrators that trigger severe disciplinary measures, then it would be beneficial for it to increase its budget for disaster-recovery technologies, even if this were to involve reduced investment in security technologies. However, if the attackers demonstrate a low level of skill, then it would be better to increase investment in security technologies instead. Taking the fifth construct (IT managerial decisions) into account, we encourage further research into management budgetary allocation strategies for security technologies from an insider threat perspective.

Finally, while distilling and analyzing the various variables, we did not consider the relative weighting of these variables. Future research might explore their respective roles and ascertain the weighting for active and latent variables in a successful insider attack. The weights assigned as a result may be able to assist practitioners in better quantifying the risk of insider threats and therefore lead to the development of more effective risk management frameworks.

REFERENCES

Editor's Note: The following reference list contains hyperlinks to World Wide Web pages. Readers who have the ability to access the Web directly from their word processor or are reading the paper on the Web, can gain direct access to these linked references. Readers are warned, however, that:

1. These links existed as of the date of publication but are not guaranteed to be working thereafter.
2. The contents of Web pages may change over time. Where version information is provided in the References, different versions may not contain the information or the conclusions referenced.
3. The author(s) of the Web pages, not AIS, is (are) responsible for the accuracy of their content.
4. The author(s) of this article, not AIS, is (are) responsible for the accuracy of the URL and version information.

Abbas, H., Magnusson, C., Yngstrom, L., & Hemani, A. (2011). Addressing dynamic issues in information security management. *Information Management and Computer Security*, *19*(1), 5-24.

Andersen, D., Capelli, D. M., Gonzalez, J. J., Mojtahedzadeh, M., Moore, A. P., Rich, E., Sarriegui, J. M., Shimeall, T. J., Stanton, J. M., Weaver, E. A., & Zagonel, A. (2004). Preliminary system dynamics maps of the insider cyber-threat problem. Paper presented at the 22nd International Conference of the System Dynamics Society.

Bagchi, K., & Udo, G. (2003). An analysis of the growth of computer and internet security breaches. *Communications of the Association for Information Systems*, *12*, 684-700.

Beebe, N. L., & Rao, V. S. (2010). Improving organizational information security strategy via meso-level application of situational crime prevention to the risk management process. *Communications of the Association for Information Systems*, *26*(7), 329-358.

Benbasat, I., & Zmud, R. W. (1999). Empirical research in information systems: The practice of relevance. *MIS Quarterly*, *23*(1), 3-16.

Bishop, M., Gollmann, D., Hunker, J., Probst, C. W. (2008). *Countering insider threats*. Proceedings of the Dagstuhl Seminar (Vol. 8302, p. 18).

Bradford, P., & Hu, N. (2005). *A layered approach to insider threat detection and proactive forensics*. Paper presented at the Proceedings of the Twenty-First Annual Computer Security Applications Conference, Tucson, Arizona.

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

Cavusoglu, H., Cavusoglu, H., & Raghunathan, S. (2004). Economics of IT security management: Four improvements to current security practices. *Communications of the Association for Information Systems*, *14*(3), 65-75.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2005). The value of intrusion detection systems in information technology security architecture. *Information Systems Research*, *16*(1), 28-46.

Chinchani, R., Iyer, A., Ngo, H., & Upadhyaya, S. (2004). *A target-centric formal model for insider threat and more* (Technical Report 2004-16). Department of Computer Science and Engineering, State University of New York at Buffalo, New York.

Choobineh, J., Dhillon, G., Grimaila, M. R., & Rees, J. (2007). Management of information security: Challenges and research directions. *Communications of the Association for Information Systems*, *20*(57), 958-971.

Colwill, C. (2009). Human factors in information security: The insider threat–who can you trust these days? *Information Security Technical Repor*t, *14*(4), 186-196.

Cone, B. D., Irvine, C. E., Thompson, M. F., & Nguyen, T. D. (2007). A video game for cyber security training and awareness. *Computers and Security*, *26*(1), 63-72.

CSI Computer Security Institute. (2011). *CSI Computer Crime and Security Survey 2010/2011*. Computer Security Institute: New York.

Datalossdb. (2013). Data Loss Statistics 2012. Retrieved January 27, 2013, from http://datalossdb.org/statistics?utf8=%E2%9C%93&timeframe=last_year

Dhillon, G., & Moores, S. (2001). Computer crimes: Theorizing about the enemy within. *Computers and Security*, *20*(8), 715-723.

Dubé, L., & Paré, G. (2001). Case research in information systems: Current practices, trends, and recommendations. *Cahier du GReSI*, *1*(12), 1-36.

Durgin, M. (2007). Understanding the importance of and implementing internal security measures. *SANS Institute Reading Room.* Retrieved from https://www2.sans.org/reading_room/whitepapers/policyissues/1901.php

EDPACS. (1973). Computer related fraud. *The EDP Audit, Control, and Security Newsletter*. Retrieved June 11, 2012, from http://dx.doi.org/10.1080/07366987309450059 (current June 11, 2012).

Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of Management Review*, *14*(4), 532-550.

Ernst & Young (2008). *Ernst & Young 2008 global information security survey*. Retrieved from http://faisaldanka.wordpress.com/2008/10/20/ernst-young-2008-global-information-security-survey/

Escamilla, T. (1998). *Intrusion Detection: Network Security Beyond the Firewall*. New York: John Wiley & Sons.

Ganame, A. K., Bourgeois, J., Bidou, R., & Spies, F. (2006). A global security architecture for intrusion detection on computer networks. *Computers and Security*, *27*(1), 30-47.

Garrison, C. P., & Ncube, M. (2011). A longitudinal analysis of data breaches. *Information Management and Computer Security*, *19*(4), 261-230.

George, J. F., Biros, D. P., Burgoon, J. K., Nunamaker, J. F., Jr., Crews, J. M., Cao, J., Marrett, K., Adkins, M., Kruse, J., & Lin, M. (2008). The role of e-training in protecting information assets against deception attacks. *MISQ Executive*, *7*(2), 1-14.

Gordon, L. A., Loeb, M. P., & Sohail, T. (2010). Market value of voluntary disclosures concerning information security. *MIS Quarterly Executive*, *34*(3), 567-594.

Gregor, S. (2006). The nature of theory in information systems. *MIS Quarterly*, *30*(3), 611-642.

Greitzer, F., Moore, A., Cappelli, D., Andrews, D., & Carroll, L. (2008). Combating the insider cyber threat. *IEEE Security and Privacy*, *6*(1), 61-64.

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

Gupta, M., Chaturvedi, A., & Mehta, S. (2011). Economic analysis of tradeoffs between security and disaster recovery. *Communications of the Association for Information Systems*, *28*(1), 1-17.

Hunker, J., & 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), 4-27.

Ifinedo, P. (2009). Information Technology security management concerns in global financial services institutions: Is national culture a differentiator? *Information Management and Computer Security*, *17*(5), 372-387.

IIARF (2002). Systems assurance and control—glossary. *The Institute of Internal Auditors Research Foundation.* Retrieved from http://www.theiia.org/esac/index.cfm?fuseaction=or&page=glos

ITRC. (2013). 2005 to 2012 Breach Analysis. Retrieved October 14, 2013, from http://www.idtheftcenter.org/images/breach/breach_analysis_2005_2012.pdf

Keromytis, D. A. (2008). Hard problems and research challenges concluding remarks. In S. J. Stolfo, S. M. Bellovin, A. D. Keromytis, S. Hershkop, S. W. Smith, & S. Sinclair (Eds.), *Insider attack and cyber security* (pp. 219-222). US: Springer.

Kim, N. Y., Robles, R. J., Sung-Eon, C., Yang-Seon, L., & Tai-Hoon, K. (2008). *SOX Act and IT security governance*. Paper presented at the Proceedings of the International Symposium on Ubiquitous Multimedia Computing, Hobart.

Kjaerland, M. (2006). A taxonomy and comparison of computer security incidents from the commercial and government sectors. *Computers and Security*, *25*(7), 522 – 538.

Koliadis, G., Desai, N. V., Narendra, N. C., & Ghose, A. K. (2010). *Analyst-mediated contextualization of regulatory policies*. Paper presented at the Proceedings of the 2010 IEEE International Conference on Services Computing, Miami.

Kotulic, A. G., & Clark, J. G. (2004). Why there aren't more information security research studies. *Information and Management*, *41*(5), 597-607.

Kruger, H., & Kearney, W. (2006). A prototype for assessing information security awareness. *Computers and Security*, *25*(4), 289-296.

LeCompte, M. D. (2000). Analysing qualitative data. *Theory into Practice*, *39*(3), 146-154.

Lee, J., & Lee, Y. (2002). A holistic model of computer abuse within organizations. *Information Management and Computer Security 10*(2), 57-63.

Lee, S. M., Lee, S. G., & Yoo, S. (2003). An integrative model of computer abuse based on social control and general deterrence theories. *Information and Management, 41*(6), 707-718.

Lehmann, R. L. (1981). Tracking potential security violations. *Security, Audit, and Control Review*, *1*(1), 26-39.

Liu, Q., & Ridley, G. (2005). *IT control in the Australian public sector: An international comparison.* Proceedings of the Thirteenth European Conference on Information Systems.

Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to information systems: Today's reality, yesterday's understanding. *MIS Quarterly*, *16*(2), 173-186.

Mahmoud, A., Siponen, M., Straub, D., Rao, H. R., & Raghu, T. S. (2010). Moving towards black hat research in information systems security: An editorial introduction to the special issue. *MIS Quarterly*, *34*(3), 431-433.

Martin, N., & Rice, J. (2011). Cybercrime: Understanding and addressing the concerns of stakeholders. *Computers and Security*, *30*(8), 803-814.

Martinez-Moyano, I. J., Rich, E., Conrad, S., Andersen, D. F., & Stewart, T. R. (2008). A behavioral theory of insider-threat risks: A system dynamics approach. *ACM Transactions on Modeling and Computer Simulation*, *18*(2), 7.1-7.27.

McLean, K. (1992). *Information security awareness—selling the cause*. Proceedings of the IFIP TC11, Eighth International Conference on Information Security: IT Security: The Need for International Cooperation.

Melara, C., Sarriegui, J. M., Gonzalez, J. J., Sawicka, A., & Cooke, D. L. (2003). *A system dynamics model of an insider attack on an information system*. Proceedings of the 21st International Conference of the System Dynamics Society.

Myers, M. (1997). Qualitative research in information systems. *MIS Quarterly*, *21*(2), 241 - 241.

Paans, I. R., & Herschberg, I. S. (1987). Computer security: The long road ahead. *Computers and Security*, *6*(5), 403-416.

Palvia, P., Midha, V., & Pinjani, P. (2006). Research models in information systems. *Communications of the Association for Information Systems*, *17*(47), 1041 - 1059.

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

Pathak, J. (2003). Internal audit and e-commerce controls. *Internal Auditing*, *18*(2), 30-34.

Pfleeger, S. L., & Stolfo, S. J. (2009). Addressing the insider threat. *IEEE Security & Privacy*, *7*(6), 10-13.

Pfleeger, C. P. (2008). Reflections on the insider threat. In S. J. Stolfo, S. M. Bellovin, S. Hershkop, A. Keromytis, S. Sinclair, & S. W. Smith (Eds.), *Insider attack and cyber security* (pp. 5-16). US: Springer.

Ponnemon Institute. (2011). *The true cost of compliance: Benchmark study of multinational organizations*. Retrieved January 5, 2011, from http://www.ponemon.org/library/the-true-cost-of-compliance-a-benchmark-study-of-multinational-organizations

Post, G. V., & Kievit, K. A. (1991). Accessibility vs. security: A look at the demand for computer security. *Computers and Security*, *10*(4), 331-344.

Privacy Rights Clearing House. (2013). *Chronology of data breaches*. Retrieved January 12, 2013, from https://www.privacyrights.org/data-breach

Puhakainen, P. (2006). *A design theory for information security awareness*, Oulu, Finland: University of Oulu.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly*, *34*(4), 757-778.

Richards, T. C. (1984). A computer fraud survey. *acm sigsac review*, *3*(1), 17-23.

Richardson, R. (2008). CSI computer crime and security survey. *Computer Security Institute*, *1*, 1-30.

Russell, D., & Gangemi, G. T. (1992) *Computer security basics*. Sebastopol, CA: O'Reilly & Associates.

Santos, E., Nguyen, H., Yu, F., Kim, K. J., Li, D., Wilkinson, J. T., Olson, A., Russell, J., & Clark, B. (2012). Intelligence analyses and the insider threat. *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans*, *42*(2), 331-347.

Schultz, E. (2002). A framework for understanding and predicting insider attacks. *Computers and Security*, *21*(6), 526-531.

Schultz, E. (2005). The human factor in security. *Computers and Security*, *24*(6), 425-426.

Siponen, M., Pahnila, S., & Mahmood, A. (2007). Employees' adherence to information security policies: An empirical study. *New Approaches for Security, Privacy and Trust in Complex Environments: IFIP International Federation for Information Processing*, *232*, 133-144.

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

Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *MIS Quarterly*, *34*(3), 503-522.

Stake, R. E. (2003). Qualitative case studies. In N. K. Denzin & Y. S. Lincoln (Eds.), *The Sage handbook of qualitative research* (pp. 443-466). California: Sage.

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

Straub, D., & Welke, R. (1998). Coping with systems risk: Security planning models for management decision-making. *MIS Quarterly*, *22*(4), 441-469.

Straub, D. W., & Nance, W. D. (1990). Discovering and disciplining computer abuse in organizations: A field study. *MIS Quarterly*, *14*(1), 45-60.

Sykes, G. M., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American Sociological Review*, *22*(6), 664-670.

Thomson, M., & von Solms, R. (1998). Information security awareness: Educating your users effectively. *Information Management and Computer Security*, *6*(4), 167-173.

Trček, D. (2003). An integral framework for information systems security management. *Computers and Security*, *22*(4), 337-360.

Tsiakis, T., & Stephanides, G. (2005). The economic approach of information security. *Computers and Security*, *24*(2), 105-108.

Verizon. (2008). 2008 Data Breach Investigations Report. Retrieved April 16, 2012, from http://www.wired.com/images_blogs/threatlevel/2011/04/Verizon-2011-DBIR_04-13-11.pdf

von Solms, R., van de Haar, H., von Solms, S. H., & Caelli, W. J. (1994). A framework for information security evaluation. *Information and Management*, *26*(3), 143-153.

Vroom, C., & von Solms, R. (2004). Towards information security behavioural compliance. *Computers and Security*, *23*(3), 191-198.

Weber, R. (2012). Evaluating and developing theories in the information systems discipline. *Journal of the Association for Information Systems*, *13*(1), 1-30.

Yadav, S. B. (2010). A six-view perspective framework for system security: Issues risks and requirements. *International Journal of Information Security and Privacy*, *4*(1), 61-92.

Yang, S. C., & Wang, Y. L. (2011). System dynamics based insider threats modeling. *International Journal of Network Security and its Applications*, *3*(3), 1-14.

Yin, R. (1994). Case study research: Design and methods (2nd edn.) Thousand Oaks, CA: Sage.

Yin, R. (2009) Case study research: Design and methods (4th edn.) Thousand Oaks, CA: Sage.

Young, R. F., & Windsor, J. (2010). Empirical evaluation of information security planning and integration. *Communications of the Association for Information Systems*, *26*(13), 245-266.

ABOUT THE AUTHORS

Mathew Nicho is a lecturer in the School of Computing and Digital Media at Robert Gordon University in United Kingdom. He holds a Master's degree in Information Systems, and a doctorate from the School of Computing and Mathematical Sciences of Auckland University of Technology, New Zealand. His current research interests are in the areas of information systems (IS) security management, IS vulnerabilities and mitigation, advanced persistent threats, information security governance, and information technology governance frameworks namely COBIT, ITIL, and PCI DSS. His research outputs has appeared in international journals and conference proceedings.

Faouzi Kamoun is an Associate Professor in the College of Technological Innovation at Zayed University. He received his PhD in Electrical and Computer Engineering from Concordia University and an MBA from McGill University. He was the recipient of an IBM Faculty Award in 2008 and Nortel Networks CEO Top Talent Awards in 2000 and 2001. His research interests are in the areas of technology and security management, next-generation networks, and IT innovations. His research outputs has appeared in international journals and conference proceedings.

Communications of the Association for Information Systems

ISSN: 1529-3181