Review of IS Security Policy Compliance: Toward the Building Blocks of an IS Security Theory

Puzant Balozian
Lebanese American University

Dorothy Leidner
Baylor University and Lund University

Abstract

An understanding of insider threats in information systems (IS) is important to help address one of the dangers lurking within organizations. This article provides a review of the literature on insider compliance (and failure of compliance) with information systems' policies in order to understand the status of IS research regarding negligent and malicious insiders. We begin by defining the terms, developing a new taxonomy of insiders, and then providing a comprehensive review of articles on IS policy compliance for the past 26 years. Grounding the analysis in the literature, we inductively identify four themes to foster Information Security policy compliance among employees. The themes are: 1) IS management philosophy, 2) procedural countermeasures, 3) technical countermeasures, and 4) environmental countermeasures. We propose that future research can draw upon these themes and use them as the building blocks of an indigenous IS security theory.

Keywords: Insider Threat; Information Systems Security; Review; Compliance; Noncompliance; Information Systems Security Policy

Introduction

Ashley Madison is a dating website for married couples who wish to cheat on their spouses. On July 20, 2015, Ashley Madison site's customer data was stolen, the systems were compromised, large quantities of supposedly confidential data were appropriated, and a small percentage of user account secret affairs data with matching credit card transactions were exposed to the public (BBC News, 2015). The hackers planned to post more data online until the website closed. Security experts indicated that the company's negligent insider(s) might have clicked on a phishing email and thus unintentionally assisted the hackers (BBC News, 2015). This incident cost the mother company $370,000 (as a reward money to catch the hackers), the CEO his job (who resigned), and two people their lives who committed suicide after the hackers exposed their infidelity (Sharp, 2015; Zetter, 2015).

Despite the press coverage, the Ashley Madison hack was not an isolated case nor was the action a new trend. Throughout the years, studies have consistently indicated that current employees are responsible for over 50 percent of reported security breaches (PWC, 2015) and that carelessness or lack of awareness accounts for nearly 40 percent of insider security incidents (Young, 2014). A CSI/FBI report (Richardson, 2011) showed that internal actors

were responsible for no less than half of significant cyber security breaches. These figures intensify the constant mandate to decrease the risk of negligent — as well as opportunistic and malicious — insiders in organizations. According to the same CSI study, 66.1 percent of the respondents reported that up to 20 percent of total company losses are attributed to nonmalicious insiders, and 87.1 percent of the respondents reported that up to another 20 percent of losses are attributed to malicious insiders (Richardson, 2011).

Furthermore, 29 percent of data breaches occur through social engineering tactics (Verizon, 2013), similar to the phishing email example in Ashley Madison's case. Social engineering can be successful only if and when employees are unaware and ill-equipped to handle such techniques used by hackers. There are a number of insider threat examples to draw upon:

- Just before her company downsized, a disgruntled employee used her expertise to encrypt her company's database, only to offer her services to decipher it for $10,000 afterward, with the promise of no legal action. She regarded the fee as compensation for her job termination (Shaw et al., 1998).
- Tse Thow Sun sold trade secrets to a competitor of his current employer, a software company, in exchange for $3 million. He pled guilty in April 2003 to theft of proprietary information (Hunter, 2003).
- An employee tried to beat her organization's time-consuming, work-impeding security system in a newly implemented Enterprise Resource Planning (ERP). She asked her colleague to replicate an action on her desktop's keyboard, preventing a log out while she was away from her office. Ironically, instead of enhancing security, the ERP system contributed to an increase in security risk (Boudreau & Robey, 2005).

Insider threat risk has not been diminishing over time. According to a survey of 671 IT and IT security practitioners, information systems security risks are generally on the rise and negligent insider threat risk still remains high (Ponemon Institute, 2012). The same institute found that practitioners and IT managers are witnessing the greatest rise of potential IT security risk within their work environment in both the negligent dimension (according to 43 percent of the respondents) and in the malicious dimension (according to 16 percent of the respondents) (Ponemon Institute, 2012).

Thus, organizational information systems security is directly linked to the effectiveness of the implementations of IS policies inside organizations (Straub & Welke, 1998). The effectiveness of IS policies is directly tied to employee compliance. This paper addresses IS policy compliance, a cornerstone in ensuring IS security in organizations.

Research in IS security in organizations seeks to uncover how to best fortify the organization against outside hackers. In order to be effective in this, the IT department's security experts need to transform every employee in the organization into an unbreakable link in the security chain. For that reason, and since the majority of employees are not very knowledgeable about security issues, employees need specific and understandable guidelines known as IS security policies. The IT department expects employees to abide by these laws, that is, to comply with IS security policies. A lack of compliance from even one employee weakens the chain, creating a vulnerability in the impenetrable wall from which a hacker can breach IS security. The lack of compliance (i.e., noncompliance or violations of policies) from an employee is termed as an "insider threat" to IS security in the organization. IT management uses IS security policy compliance as a means of diminishing insider threats. Since noncompliance creates a state of insider threat, for simplicity, both terms (insider threat and compliance) are used interchangeably in this study.

Several reasons moved us to embark on this research. First, the literature of IS security policy compliance dates from the early 1990s, which means there is a need to make sense of an extensive amount of research from more than two decades. Second, although there are excellent IS security reviews, these are intended to provide a broad coverage of the IS security topic and hence do not expressly focus on IS security policy compliance. For example, an excellent general security meta-analysis of both technical and socio-technical articles is available from Siponen and Oinas-Kukkonen (2007), but it barely touches on policy compliance. Another IS security review specifically examines articles that employ general deterrence theory (GDT) to questions of IS security (D'Arcy & Herath, 2011). A broader review of security compliance would need to include many other theories. In this article, we go beyond covering GDT and incorporate the empirical articles that include all the approaches, methodologies, theories, philosophies, and countermeasures tested in IS research for a period of 26 years to deter insider threats and ensure IS security policy compliance on the employee level in organizations. Recently, Guo (2013) provided a broad review of the IS security literature including a taxonomy. Although the taxonomy we develop is consistent with Guo's taxonomy in considering intention (malicious vs.

nonmalicious), willingness to comply (willing vs. unwilling), and level of ability to comply or not (high ability vs. low ability), it is different in focus and contribution. Whereas Guo focuses on understanding the dependent variable (e.g., security behavior), our review focuses on the antecedents of compliance or the independent variables. After examining hundreds of independent variables, we come up with four overarching themes: Philosophy of IS management (development or deterrence), Procedural countermeasures, Technical countermeasures, and Environmental countermeasures. We found that these are the potential building blocks of an indigenous IS security theory, based on the past 26 years of IS security research.

The paper is organized as follows: in the first section, we present the boundaries of our study, the relationship between the compliance research and insider threats, a definition of insider threats, and a new comprehensive taxonomy. The next section provides a concise overview of the research methodology used to accomplish this review. The literature review follows the methodology section, treating each theme (developed inductively) simultaneously on both negligent and malicious insider levels. The paper concludes with the theoretical contributions and suggests the use of the abstract themes developed in the study as the building blocks of a potential indigenous IS security theory.

The Concept of Insider Threat

In the context of IS, the term "insiders" refers to "employees who are authorized to use a particular system or facility" (Neumann, 1999). Our review is on the compliance of insiders, but in our article inclusion decisions, we accepted those articles that use several different keywords or terms related to compliance. We found many terms regarding insider threats in the IS security literature, for example, "computer crime," "computer abuse," "IS misuse," "policy compliance," and so on. Although these terms include outside threats, such as data breaches from outside hackers, they necessarily encompass both outside and insider threats. Hence we include these terms in our insider threat security research. We argue that each of these terms is related to IS security policy noncompliance. Every breach, every misuse, every crime, and all cyberloafing, goes back to an employee who is not abiding by (or not complying with) the IS security policies in place (assuming there are policies in place). Regardless of the security problem, the question at hand is a compliance failure. These are two sides of the same coin. For example, Straub (1990) uses the keyword "computer crime" in his article, nevertheless, he is clearly dealing with insider compliance and noncompliance in his discussion section. The following quotations from his seminal article clearly equate the terms "computer crime" (in the author's keywords section) with "compliance/noncompliance" (in his discussion section): the "follow up of all identified violations will deter potential abusers and encourage ***compliance*** with security directives" (1990, p. 272) and "an active security staff and a commitment to data security are effective controls, as are activities in which security staff inform users about unacceptable system use and penalties for ***noncompliance***" (p. 274). Another example occurs in the seminal work of Harrington (1996). In the keywords section of her article, she uses the words "abuse and crime" and "computer crime" among others, along with using the word "compliance" in her hypothesis development: "the existence of a code of ethics and the affidavit of ***compliance*** often signed by the employee suggest sanctions will occur should the code be broken" (p. 259). Her use of the terms "abuse and crime" and "compliance" in the main body of the article proves that these terms are the two faces of the same coin. Therefore: 1) our inclusion of the broader literature (e.g. computer abuse, computer crime...) and not just strictly compliance literature is appropriate, 2) our defined topic is compliance (or the lack thereof) inside organizations (regardless of the motivation: malicious, opportunistic, or negligent), and 3) our free use of the terms is not coincidental but intentional, since all of the terms, "computer crime," "misuse," "breach," "cyberloafing," etc., are directly related to a failure of compliance.

In this paragraph, we discuss the motivation behind creating a new taxonomy of insider threats. First, the structure of our review follows a taxonomy that we developed for this study. We reviewed employee compliance, which requires understanding who the employees are: whether they are a homogenous or a diverse group. Another reason for writing this section is the need for improving or upgrading the existing taxonomies in the literature because of some of their shortcomings. The taxonomy by Stanton, Stam, Mastrangelo, and Jolton (2005) is a two-factor organization of security behaviors based on expertise (high-low) and intentions (malicious, neutral, and beneficial). Our taxonomy (Table 1) adds another dimension to Stanton et al.'s taxonomy: the willingness to comply. Opportunistic employees are unwilling to comply, although they have nonmalicious intentions. It seems best to describe these types of employees as opportunistic rather than neutral, since they are willingly and knowingly noncompliant and their acts may lead to unanticipated damages. Another taxonomy is that of Willison and Warkentin (2013), where the authors expand Loch, Carr, and Warkentin's (1992) IS security threat vector

taxonomy, and divide the internal human threat into a continuum of three types: 1) passive, non-volitional noncompliance; 2) volitional (but not malicious) noncompliance; and 3) intentional, malicious (harmful) computer abuse. Our taxonomy adds an ability dimension, which is the skillfulnes of the employee to either protect or hack the system.

Table 1 presents our taxonomy of insiders based upon our reading of the literature. The table divides the types of insiders among three groups: compliant users (quadrant 1), negligent users (naïve and opportunistic, quadrants 2 and 3, respectively), and malicious users (quadrant 5). These three groups (four quadrants) are discussed at length in the IS literature. Potential opportunistic or potential malicious insiders (quadrants 4 and 6, respectively) are virtually nonexistent in the literature (and thus out of the scope of this review). We believe that the study of potential negligent and malicious insiders are absent from the literature because researchers lack theoretical explanations to accurately predict and identify the employees who may turn out to be opportunistic or malicious insiders in the future. We note that there is a rising interest among IS researchers to develop theories and models to understand potential opportunistic or potential malicious insiders (see Willison & Warkentin, 2013). However, since there is a dearth of empirical articles that study these types of insiders, we have not included these two categories of insiders here. What follows is a description of the well-researched categories of insiders, the second and third groups mentioned above (negligent and malicious insiders), with a passing note on the first group.

The first group, the compliant insiders, are IS users who comply with IS policies. This group is not treated independently in the scope of the present manuscript, mainly because IS security literature does not treat them independently. The literature tends to ask why people do not comply and what can be done about it. It does not seek to understand the characteristics of individuals who comply nor understand why they comply. Furthermore, compliant insiders are the byproduct of implementing countermeasures that force and/or encourage a user to comply. In this study, we outline these countermeasures and we assume that their end result will be compliant IS users in organizations. The same reasons, countermeasures, or motives (verbal praise, fear appeal, technical monitoring, etc.) that may motivate the potential noncompliant employees will also motivate the compliant employees. Thus, the compliant quandrant is indirectly covered in our study.

The second group, the negligent insiders, are the IS users who do not comply with their organizations' IS policies, albeit for nonmalicious reasons. This group consists of two subcategories: negligent naïve and negligent opportunistic. An employee who carelessly plugs his personal USB flash drive (regularly used on his personal laptop) into his work computer (without scanning it first) can be an example of a naïve negligent insider. He did not know that some types of worms (malware programs) are able to detect passwords and send them back to outside hackers. The right clicks on the wrong websites on his personal laptop may unleash the worm, which embeds itself in the USB flash drive. If the flash drive is not scanned first by powerful antivirus software and is plugged into the desktop of a work computer in an organization, it registers the computer's password and sends it to the hacker automatically via the Internet. Thus, an outside hacker gains access to a computer inside the organization because of a negligent naïve employee (quadrant 2 in Table 1).

An employee who knows how to update his desktop's security software but neglects to do so because he has deadlines to meet is a good example of the second subcategory of the negligent insider, the "opportunistic" user (quadrant 3 in Table 1). Another expression for negligent opportunistic is "abusive insider," which describes the noncomplying employee who neglects IS policies knowingly, thereby abusing the system. Henceforth, we will use the notation of "opportunistic insider" instead of abusive insider, in order to depart from the negative nuance that the word "abusive" may have. Opportunistic insiders do not intend to harm the company; they just want to circumvent policies for nonmalicious reasons. Both types of negligent insiders (naïve and opportunistic) pose indirect threats to the IS security of the organization for which they work.

Therefore, logically, negligent insiders can be categorized into two subcategories according to their ability and willingness: some IS users are willing to comply but are not able (naïve acts caused by lack of awareness or training), while others are able to comply but are not willing (opportunistic acts caused by negative motivation). The absence of malicious intent to harm the company is what differentiates these two negligent subcategories from malicious insiders. Hence naïve acts and opportunistic acts are surveyed under the same category of negligent insiders.

Table 1. Insider Types - Matrix

Intent	Nonmalicious Intent		Malicious Intent
Willingness / Ability	**Willing to Comply**	**Unwilling to Comply**	**Unwilling to Comply**
High Expertise	I) Compliant	*III) Negligent (opportunistic acts)*	*V) Malicious*
Low Expertise	*II) Negligent (naïve acts)*	IV) Negligent (opportunistic acts) – potential	VI) Malicious - potential

The third group, the malicious insiders (quadrant 5 in Table 1), are the IS users who do not comply with the organization's IS policies for malicious reasons. They are deliberately noncompliant in order to harm the company. They may try to alter or destroy information by curbing or destroying existing security countermeasures. A disgruntled employee who plants a logic bomb (a software program that once planted in a system may erase data in a specified day/time) in the organization's main server before the deadline of his employment termination is a good example of a malicious insider.

Having described our version of different types of insiders as presented in the taxonomy in Table 1, we will next describe the research methodology used to identify the articles for our review.

Research Methodology

In order to be as inclusive as possible, our approach towards the literature search followed a twofold process. First, we sought to survey all the articles on IS policy compliance in the top 25 IS journals depicted in the worldwide ranking in Lowry et al. (2004), available on the official AIS website. Since one was in the German language, 24 journals were included. Furthermore, one extra journal was added (the *Journal of Information Technology*) because it is included in the senior scholars' basket, but is not in the Lowry et al. ranking. Thus, the number of surveyed journals remained at 25.

We used the following databases to initiate the search process: *ABI/Inform*, *ScienceDirect*, and *Business Source Complete*, as well as the AIS website. These databases are known for their inclusion of business, management, computer science, and information systems journals (and include our 25 IS journals). We used the following keyword searches in both titles and author-supplied keywords: security, policy, compliance, and noncompliance. We placed heavy emphasis on the word "security" in the searches because of the fact that the majority of the papers prior to 2005 use the keyword "security" rather than "compliance," even if they treat compliance in the paper. Reading and analysis of the literature began in early 2013. Therefore, the initial search incorporated peer reviewed articles from 1990 to 2012 inclusive. We subsequently conducted a post-hoc search for articles published in the years 2013-2015 to bring the review up-to-date prior to publication. We scanned the articles' titles and abstracts to identify relevant articles on compliance with IS security policies and insider threats to IS security.

We also scanned all the references of the identified key articles to double-check the inclusion of relevant studies. We only included empirical studies at the user/employee unit of the analysis. Conceptual articles and those pertaining to other levels of analysis were discarded to keep our study focused and manageable. A total of 67 articles were identified and selected (Appendix A; also see Appendix B for the distribution of papers among the journals). All the articles were thoroughly studied to confirm that they dealt with insider threats to IS security and/or IS security policy compliance/noncompliance. Furthermore, the references of a meta-analysis of security research (Siponen & Oinas, 2007) were consulted to ensure the inclusion of all the relevant articles prior to 2007.

In order to emphasize the lack of studies of purely malicious insiders, we categorized each identified article in Appendix A into 1) purely malicious, 2) malicious and negligent (including the latter's subcategories of naïve or opportunistic), or 3) purely negligent (with both subcategories). Some of the articles were difficult to classify because the authors did not provide any indications (phrases, author supplied keywords, clear wording in the questionnaires, etc.) that clearly identified the paper as dealing with certain types of insiders. They seemed to deal with insiders in a general manner.

Thus, these articles remained uncategorized, but were nevertheless incorporated into the overall analysis.

Since not all articles in our sample differentiate between different types of insiders, the researchers inferred the type of threat. These inferences were made by carefully examining the research model, survey items, and/or the scenarios used by the study. The following constructs used in the models guided the researchers to classify the respective articles as dealing with negligent threats: self-efficacy; resource availability; safety/vulnerability (of work files from outside attacks); security education, training, and awareness (SETA) or training programs; response efficacy; response cost; and work impediment. These constructs imply that employees are technically able to comply with IS policies; that they have the company resources, including the technical means, to protect their files from outsider threats; that they are educated, trained, and aware of security measures; that the security software used in the organization is effective in blocking external attacks; and that the security measures are perceived as counter-productive.

Survey items and scenario cases similar to the following implied that the article also dealt with negligent threats: “It is ok to share passwords with colleagues” or “It is ok to violate the company information security policy if no damage is done to the company.” Finally, articles with keywords that included “Security Awareness Training,” “Security Policy Compliance,” “IS Misuse,” and “Compliance and Information Security Awareness” indicated that the article dealt with negligent threats, since these procedures are not usually applied to malicious insiders. The articles on malicious insider threats were identified based on keywords, including “Computer Crime” or “Abuse and Crime,” or wording and expressions in the text like “revenge,” “disgruntled employees,” “criminal activities,” “criminal behavior,” and “crime and anti-social acts.” All the articles were thoroughly studied to confirm their classification as negligent, malicious, or both. When an article included both, it was classified as both “malicious and negligent” in Appendix A.

See Appendix A for a list of the articles reviewed in this paper and a summary of the different categorizations by chronological date of publication. The chronological mapping provides the following insight: the research on negligent insiders is continuous, whereas the research on malicious insiders is sporadic. This finding in 2016 is still consistent with what the editorial article observed in 2009 (Warkentin & Willison, 2009).

Literature Review

In this section, the main themes that emerged from the review are identified and analyzed. Each theme begins with its treatment under negligent threats, followed by its treatment under malicious threats. We believe that these themes can serve as the building blocks for the development of an indigenous IS security theory. The section concludes with suggestions for future research.

The literature review section is organized as follows: the conceptual themes are introduced first, along with the analysis of the 67 articles. Table 2 gives a concise outline of the review. The literature review section is summarized by an overview of negligent and malicious insider threats. Then an overview of the theories used in IS policy compliance and insider threat research is presented, followed by an overview of the methodologies used in all of the articles.

The Conceptual Themes

The themes are the abstractions of the constructs, independent variables, and measurement items used in the sample papers. For example, constructs, such as policies or training and awareness programs tested and analyzed in the research, are categorized as procedural countermeasures (Theme 2); software monitoring and access control as technical countermeasures (Theme 3). In the following section, each theme will be defined and discussed in terms of both the negligent and malicious categories. The panoramic view of the current status of IS literature on this topic can be found in Table 3 (a-b) found at the end of this section. We identified 28 studies that can be used against both negligent and malicious insiders, 37 purely negligent insider studies, and two uncategorized.

The process through which IS management tries to strengthen the links in the security chain of the organization is by making every employee abide or comply with the IS policies. In this section, we describe the countermeasures that IS management uses in order to make employees comply with IS policies by force or, in other words, to counteract noncompliance and the state of insider threat created by noncompliance. Alternatively, management may take a more positive philosophy by encouraging employees to follow the rules. In this study, the philosophies of countermeasures were either negative (by deterrence) or positive (by development). We identified four overarching themes depicting countermeasures for addressing insider threats to IS security: (1) implementing different philosophies of countermeasures (of deterrence and development), (2) applying

procedural countermeasures, (3) applying technical countermeasures, and (4) enhancing environmental countermeasures. Next, we define each of these themes and, in a section for each, describe them in a more comprehensive way.

In this study, the philosophy of countermeasure is defined as the philosophical approach IS management uses to ensure compliance or to decrease noncompliance among employees. There are two main philosophies regarding approaches to ensure compliance. One approach is a positive developmental one, with an emphasis on encouragement to comply, referred to here as the development philosophy. The second is a more negative one, referred to here as the deterrence philosophy, with an emphasis on creating fear in the case of failure to comply. An example of the development philosophy is explaining why compliance is beneficial for the employees (for example, because it may provide a sense of personal satisfaction). An example of the deterrence philosophy is informing employees that those who do not comply with the newly established policies will be penalized financially.

Procedural countermeasures are managerial measures taken by IS management to deter noncompliance or encourage compliance with IS security policies. This may include forming policies and training employees on security awareness. The definitions for the procedural and technical countermeasures can be found in the literature (Guo & Yuan, 2012; Straub, 1990). The rest of the definitions are formulated for this study.

Technical countermeasures are the technical means employed by IS management to deter noncompliance or encourage compliance with IS security policies. This may include software monitoring and reviewing computer logs.

Environmental countermeasures are the social measures used by IS management to deter noncompliance or to encourage compliance with IS security policies. This may include creating a fear culture toward security by encouraging supervisors to keep tabs on employee compliance, thereby creating a heightened sense of subjective norms (the expectations of significant people, like the employee's supervisors and colleagues) or creating a more positive culture toward security by hiring those potential employees that have shown high standards of commitment and loyalty to the organization they serve.

We have introduced the themes, and defined and described them by giving examples. In the following sections we study the literature along the lines of these themes in detail. We turn to look closely at each of the four themes, describing the studies of negligent insiders in each theme first and then describing the studies of malicious insiders.

Table 2. Outline of the Review

Theme 1: Implementing a Philosophy of Deterrence and a Philosophy of Development Regarding Countermeasures
Deterrence Philosophy (negligent threat)
Deterrence Philosophy (malicious threat)
Development Philosophy (negligent threat)
Development Philosophy (malicious threat)
Theme 2: Applying Procedural Countermeasures
Forming Policies (negligent and malicious threat)
Informing Employees (negligent threat)
Informing Employees (malicious threat)
Theme 3: Applying Technical Countermeasures
Technical Countermeasures (negligent and malicious threat)
Theme 4: Enhancing the Environmental Countermeasures
External Environment (negligent threat)
External Environment (malicious threat)
Internal Environment (negligent threat)
Internal Environment (malicious threat)

Theme 1: Implementing a Philosophy of Deterrence or a Philosophy of Development Regarding Countermeasures

Seventy percent of the studies of negligent insiders (26 papers out of 37) and 93 percent of the studies of malicious insiders (26 papers out of 28) cover compliance philosophies. The literature presents two main philosophies regarding approaches to ensure compliance. The two approaches correspond to the extrinsic model, which is command and control, and the intrinsic model, which is self-regulatory (see Tyler & Blader, 2005). These can be understood as deterrence and development philosophies. The deterrence philosophy threatens employees with sanctions to force them to follow IS policies. The development philosophy motivates policy compliance by offering a reward or by informing IS users of the intrinsic benefits and overall safe work environment they will experience (safety from outside hacking attacks) if they comply with IS policies.

Researchers aiming to test and prove the effectiveness of sanctions on malicious insiders heavily relied upon the deterrence philosophy. We believe this is the case because of the long proven history of the deterrence approach; its effectiveness

has been shown in dealing with criminal acts not just in IS research, but also in governmental and legal actions throughout thousands of years of recorded human history. Specifically, General Deterrence Theory (GDT) was adopted, adapted, and contextualized in IS research in the early 1990s. There are other possible reasons why deterrence theory is widespread in IS security research: IS security lacks indigenous theories on security, and there are still not enough good robust developmental theories (with the exception of Protection Motivation Theory, PMT) that have been adopted, adapted, and contextualized in IS security research. Given enough time and a good direction from IS security editors and reviewers, our research community will adopt and contextualize more of the developmental theories to change potential malicious insiders into complying employees.

GDT focuses on the indirect (or general) prevention of crime by making examples of specific perpetrators, using the instrument of quickly inflicting a severe and particular sanction on the perpetrator. It is not surprising to see the influence of this approach in IS theory and practice, especially pertaining to malicious insiders. How this philosophy of deterrence is studied and tested in IS research is more fully explained in the following section.

Deterrence Philosophy (Negligent Threat)

To determine the effectiveness of deterrence philosophy on negligent insiders, the severity and certainty of sanctions have been tested, but sanction certainty lacked significance: severity had a greater impact than certainty in deterring IS misuse intentions (D'Arcy et al. 2009). The severity of sanctions is the severity of the punishment that may be inflicted on noncompliant employees. The certainty of sanctions is the likelihood of being caught and reprimanded or punished, regardless of punishment severity. The researchers explain the insignificance of sanction certainty by introducing the awareness of policies in a post-hoc analysis. Apparently, the certainty of sanction awareness is more significant than sanction certainty alone (ibid). Since the sanctions are in and of themselves insufficient for enforcing compliance, they must be communicated to IS users during security training, and the employees must be well informed about the penalties of breaching security (Straub & Welke, 1998).

The fear of sanctions has a deterrent effect, and since deterrence increases actual compliance (Siponen et al., 2010; Guo & Yuan, 2012), one of the means of maximizing IS security is to introduce the threat of being fired upon failure of compliance (Dhillon & Torkzadeh, 2006). The existence of codes of ethics has little deterring value if used alone, and therefore punishment is an enforcer of policies (Harrington, 1996). Sanctions affect the perceived cost of noncompliance toward IS policies, and therefore compliance intention (Bulgurcu et al., 2010). Moreover, moral reasoning seems to have a moderating effect on sanctions. Pre-conventional moral reasoning exists when a person is abiding by ethical codes because of fear of punishment. This reasoning is the only significant moral reasoning that deters noncompliance (Myyry et al., 2009). The social conformity that makes the employee abide by the policies is called "conventional moral reasoning." The firm beliefs and principles that make the employee abide by the policies are defined as "post-conventional moral reasoning." Nevertheless, the effectiveness of the deterrence approach is only *partly* dependent on the moral reasoning factor in individuals (ibid). This suggests that the perception of severity and certainty of sanctions will work best only on employees who fear punishment.

The philosophy of deterrence has other techniques besides the enforcement of severity and certainty of sanctions. The detailed formulation or specification of security policies and the periodic evaluation of the employees' behaviors based on these specified IS policies are positively associated with the individual's perception of compliance mandatoriness (see Kirsch & Boss, 2007). Thus, when employees notice that management is investing time in developing detailed IS policy documents, they will perceive the gravity and the seriousness of policy compliance.

Deterrence Philosophy (Malicious Threat)

Regarding malicious threats, early IS literature on insider threats (Straub, 1990; Straub & Nance, 1990) found that the severity and certainty of sanctions deter computer abuse. Severe punishment could be executed on a malicious insider such that he would be a living example to other potential perpetrators. In the case of the absence of a malicious incident, punishment threats should be regularly communicated to employees.

Hu et al. (2011) added another dimension, "the celerity of sanctions" to the already tested severity and certainty of sanctions and found that the deterrence increases the perceptions of informal and formal risks. The celerity dimension explains how fast a breach, or misuse, will be detected and punished.

The deterrence research on malicious insiders is inconsistent in its results: deterrence certainty and severity had no influence on compliance behavior in one of the articles (Son, 2011) in contrast to the

other articles that found that the severity and certainty of sanctions significantly decreased IS misuse. Perhaps the fact that Son's (2011) sample comes from China could be the cause behind the differing worldviews regarding compliance (Leidner & Kayworth, 2006). For example, the deterrence effect of certain security countermeasures varies between U.S. and Korean cultures (Hovav & D'Arcy, 2012).

In summary, based on the research of many scholars, deterring IS misuse using the severity, certainty, and celerity of sanctions is a proven technique available to IS management to enforce compliance on the company's negligent as well as malicious insiders. Interestingly, the security studies did not differentiate among the types of insiders in their abilities and intentions (naïve, opportunistic, and malicious) when they tested the deterrence approach. Their samples consisted of general users and not specific malicious, opportunistic, or naïve employees. This could be remedied in future IS security research.

Development Philosophy (Negligent Threat)

The rise of insider security incidents moved some scholars to argue that the deterrence model is not effective enough. Thus, they started advocating for another approach, the development philosophy, which uses encouragement to motivate employees to comply with IS policies. Although convincing at first glance, the argument of rising incidents cannot be firmly attributed to the ineffectiveness of the deterrence philosophy. The rising incidents could be easily ascribed to the poor implementation and appropriation of the deterrence philosophy or to the rising number of IT users. Furthermore, punishment cannot be abandoned altogether. People who follow rules to avoid punishment and people with low self-control are deterred better by punishment than by ethical training (Workman & Gathegi, 2007). Perhaps the explanation of the incentive to shift the focus of some research from the deterrence approach to the development approach is of a philosophical nature: punishment in deterrence models embodies a negative approach, and any negative approach is frowned upon in a society driven by political correctness and eager to explore positive approaches to societal problems. Siponen and Oinas-Kukkonen (2007), among others, encourage researchers to explore motivational approaches to ensure IS compliance. Thus, IS researchers have recently started to explore a more positive dimension to compliance. Although this is a relatively new research focus, with most of the studies having been published from 2007-2015, roughly the same percentage of researchers are investigating the development philosophy (43 percent; 16 out of 37 papers) as the deterrence philosophy (48 percent; 18 out of 37 papers) to mitigate negligent threats. The percentages depict the number of articles testing the specific approach divided by the total number of articles using any approach in the negligent insider table.

Bulgurcu et al. (2010) found that the perceived benefit of compliance positively influences compliance intention. In their study, the benefit of compliance was comprised of intrinsic benefit (a sense of accomplishment and satisfaction), the safety of the resources (working files being safe from virus attacks), and rewards (financial and promotional). Furthermore, the increasing awareness of the intrinsic cost of noncompliance (guilt, stress, and embarrassment) was found to positively affect intention to comply. The intrinsic cost is not a component of a deterrence approach because it is self-inflicted; it is not initiated by the organization as formal or informal sanctions are. The intrinsic cost is solely dependent on the individual character of the insider and his or her emotional makeup. Hence we do not group this construct under the deterrence approach. The organization encourages users to comply by directing them to count the cost of potential technical and psychological harm resulting from hackers destroying work files (extrinsic) or feelings of guilt (intrinsic) upon failure of compliance.

Some studies (Kirsch & Boss, 2007; Pahnila et al., 2007; Siponen et al., 2010) reached different conclusions than Bulgurcu et al. (2010) regarding rewards, which may take the form of a pay raise, bonuses, or verbally praising IS policy compliant employees in front of other colleagues. According to these studies, rewards are not related to the enhancement of compliance. Others found only weak correlations between rewards and good practices related to password creation, storage, and change (Stanton et al., 2005). This discrepancy in the results could be the natural consequence of the absence of reward systems in current IS departments. Since IS departments do not typically use rewards as an incentive for IS policy compliance, the survey questions might have been regarded as irrelevant by the respondents, thus lead to the discrepancy of the results in the above-mentioned studies.

Several authors (Johnston & Warkentin, 2010; Vance et al., 2012) tested the fear appeal, which is not induced by punishment, but is generated from an outside threat. The fear appeal concept is an instrinsic part of protection motivation theory and is used in several studies (Boss et al., 2015; Chen & Zahedi, 2016; Herath et al., 2014). The authors

found that management should uncover the severity of an attack coming from a hacker, depicting the damage it can do to the work files of employees. This step will motivate IS users to abide by the security policies and protect their work files, thus indirectly protecting the overall organizational security. If the work files are compromised, organizational security is jeopardized. Fearing outside attacks, the employee will seek help by others or the IT department in his endeavor to comply with the IS policies (Chen & Zahedi, 2016) or will be more inclined to adopt an email authentication technical service (Herath et al., 2014).

Not just the severity of an attack, but also the efficacy of the security software in place and the self-efficacy of employees in applying the security software should be emphasized. Along these same lines, research has found that as long as employees understand the damage of an outside threat to the company and perceive the company's security countermeasures as effective, their attitudes toward the policies will be positive and they will abide by them (Herath & Rao, 2009a; Workman et al., 2008).

Development Philosophy (Malicious Threat)

Although the encouragment approach has experienced a resurgence in the case of negligent insider threats, it has yet to be explored thoroughly in terms of malicious insider threats, perhaps for a good reason: it seems counterintuitive to use a positive approach to deter abuse or criminal acts. One of the articles (Lee et al., 2004) measured both negligent and malicious intents by using the self-defense intention (SDI) construct and found that a physical security system (i.e., locks on server room doors) increases SDI, which in the study is composed of the intention to implement access control and intrusion protection software. Although the article failed to show SDI's impact on insider abuse, it does indicate that at least there was an attempt to measure a development approach (raising the self-defense intention). Nevertheless, the article was not clear whether it was testing the case of negligent or malicious insiders.

Practice shows that malicious insiders desire either monetary compensation from competitors who reward espionage, or revenge following a salary cut or demotion (Shaw et al., 1998; Hunter, 2003). If this is the case, rewarding compliance financially (Dhillon & Torkzadeh, 2006) could be a promising construct to solve the problem of espionage, but it has not yet been tested empirically. It seems that deterring vengeance (sabotage) is harder than quenching materially felt needs (espionage) using a development philosophy. Whatever the rewards of the development philosophy are, they need to be equal to or greater than the benefits of noncompliance perceived by opportunistic or malicious insiders. For example, using the organization's Internet access for non-work-related activities is lucrative (convenience, saving personal time and money), and this lucrativeness negatively impacts compliance (Li et al., 2010).

There is only one study in our sample (Peace et al., 2003) that directly dealt with the theft of software and intellectual property (software piracy or copying), which is a form of espionage. Other than punishment certainty and severity, which are beneficial, a new solution was discovered: decreasing software costs will lead to lowering the incidents of espionage or software copying. This could be a positive solution to deterrence, but it is restricted in scope and limited to software copyrights, rather than addressing overall security in organizations.

Finally, a recent article (Johnston et al., 2015) tested both GDT (deterrence approach) and PMT (development approach) in the same study. What we learn from the recurrence of these two theories in IS security research as recently as in 2015, is that these two theories are the most succesfully appropriated theories in IS security research. Apart from these two, there is a clear paucity of IS security theories with high explanatory power.

In summary, two major subcategories have been studied to date within development philosophy, especially in studies of negligent insiders: 1) informing employees of the direct benefits of compliance (e.g. intrinsic and financial) and 2) informing them about the indirect benefits of compliance (e.g. the security of their files). The indirect benefits include not having to undergo the re-creation of important work files upon losing them to successful outside virus attacks. We use the terms "direct" and "indirect," since the direct category of benefits is known and experienced daily by the employees. The indirect category is known by the employees only upon the condition of an attack and the unsuccessful mitigation of it.

Overall, deterrence and development philosophies are of little value if they are not written down and communicated to IS users. These two concepts, forming policies (writing down) and informing employees (communication) are discussed next under procedural countermeasures.

Theme 2: Applying Procedural Countermeasures

Procedural countermeasures are managerial practices that include forming policies, informing employees about them, and training employees on behavioral and technical skills to ensure that they

are well aware of the threats and the ways to comply with IS policies, and thereby how to mitigate the threats. In this section, we will describe forming policies and informing employees, first the studies of negligent insider threats, followed by that of malicious insider threats.

Forming policies is not in and of itself a countermeasure mitigating noncompliance. But compliance cannot be assured unless there are written policies. Therefore, procedural countermeasures (having procedural policies) are the backdrop based on which the policies can be enforced or encouraged, and eventually followed or broken. Policies have two subcategories: First, the actual technical rules that increase the security of information systems (e.g. not having organizational data on personal mobile devices like laptops, smartphones, iPads) and describe the punishments (or incentives) when a rule is broken (or kept). The second one constitutes the actual countermeasure or deterrence to noncompliance. Since both are important and the first is a prerequisite for the second, both are described under the theme of forming policies.

Sixty-five percent of the articles (42 out of 65) deal with forming IS policies or codes of ethics along with communicating them to the IS users, making this one of the most commonly addressed countermeasure against insider threats in the IS literature. The IS policies that include the costs of noncompliance (sanctions) are imperative to deter IS misuse (D'Arcy et al., 2009), and when they include the benefits of compliance (rewards), they become useful in encouraging compliance intentions (Bulgurcu et al., 2010). Thus, policies can serve both deterrence and encouragment approaches and will be described as such in the following section.

Forming Policies (Negligent and Malicious Threats)

Among the earliest responses of IS departments to insider threats was the establishment of appropriate IS policies and codes of ethics. A security policy defines the rules and guidelines for the proper use of organizational IS resources (Straub & Nance, 1990). Yet the effects of codes of ethics have been found to be infrequent and negligible on computer abuse intention (Harrington, 1996). The same can be said of policies. Motivating compliance requires more than just framing and communicating policy to an organization's employees (Lim et al., 2002). Of course, we are not suggesting the abolition of written codes of ethics. Their importance lies in their legal functions, based on which organizations may take action if a violation occurs (Siponen & Vance, 2010).

User participation in policy formation directly raises the perception of improvements of security controls, which in turn increases the employees' policy compliance (Spears & Barki, 2010). When IS management makes employees aware of security risks and invites user participation in policy formation, employees realize that they have a valuable role in enhancing organization security. Thus they will be more apt to comply with the policies they have contributed in creating. Other forms of user participation are whistle-blowing policies. When the users are empowered and encouraged to report computer abuse in the workplace and the system or reporting procedure is anonymous, there is an increase in the willingness to report the abuse or noncompliance, and therefore the overall efficiency of security is enhanced (Lowry et al., 2013).

A small number of studies considered the implications of policy characteristics on compliance. Characteristics may include things like policy age, frequency of update, and clarity. Two studies showed that the degree of specificity of IS policies (detailed explanations) may increase the employees' perception of the mandatoriness of compliance (Boss et al., 2009; Kirsch & Boss, 2007). Another study found that information security policies' existence, longevity, updates, scope, and adoption of best practices have no significant impact on the existence and severity of security breaches (Doherty & Fulford, 2005). We think national differences could be at the root of this discrepancy. The first two studies were conducted in the U.S., but the second in the U.K. Americans put a greater emphasis on punctuality than their U.K. peers (Fullbright Commission, 2015), which may explain why American employees are more positively affected by IS policy age, updates, and clarity than their peers in the U.K. This raises the question of whether the same countermeasures are equally valid in different cultural contexts. Future research may shed light on the universality of the effectiveness of countermeasures as well as on the different philosophies of deterrence and development. Another explanation of this discrepancy may be the finding that U.K. policies (at least, of the healthcare sector) do not promote understanding and are not clear enough (Stahl et al., 2012).

A number of articles tested policies or codes of ethics to see their impact on IS malicious misuse. For example, guidelines and policies for acceptable system use and the dissemination of information about sanctions decrease computer abuse (Straub, 1990; Straub & Nance, 1990; Straub & Welke, 1998). Similar to the negligent insider case, these policies may lose effect if they are not effectively

communicated to employees (Straub & Welke, 1998) and followed by the enforcement of sanctions in case of a breach (Straub & Nance, 1990).

In summary, IS policies are the backbone of countermeasures to deter negligent as well as malicious threats, but only the *awareness* of IS policies, not the mere existence of them, decreases IS misuse intention (D'Arcy & Hovav, 2007). Although awareness was described superficially in Theme 1 (related to the awareness of sanctions), in the next section it will be described in an extensive way, encompassing not just the awareness of sanctions but also the awareness of what to do and how to do it, in relation to policy compliance.

Informing Employees (Negligent Threat)

This subtheme speaks about the communication of both managerial policies and technical information to users. Knowledge of managerial policies is helpful to both types of insiders but technical knowledge is specifically helpful to negligent IS users. After all, no IS department wants to send a potential malicious or abusive employee to advanced training to gain additional technical knowledge of the systems.

Informing and educating users can take many forms other than technical education or communication of managerial policies. For example, informing employees about basic security practices may make them conscious enough to not share confidential data with others on public forums (see Smith et al., 2012) or on social media. In our study, this type of education is labeled raising behavioral knowledge. Thus, communicating behavioral knowledge may include raising *awareness* of IS policies and their related sanctions and incentives as well as good security practices at work. Communicating technical knowledge may include raising users' perceptions of self-efficacy, reducing response costs, and increasing response efficacy. These two dimensions are discussed next.

Behavioral Knowledge: Security, Education, Training, and Awareness (SETA) programs can decrease IS misuse intention among negligent insiders (D'Arcy et al., 2007, 2009) [SETA programs are named "cues to action" in Ng et al. (2009)]. Bulgurcu et al. (2010) confirmed the role of IS policy awareness in increasing the perceived costs of noncompliance and the benefits of compliance. Informing employees about IS policies through SETA programs is not the only channel for raising awareness among employees. Other channels include requiring users to participate in security risk management (SRM), which raises employee awareness of IS security risks (Spears & Barki, 2010).

Awareness campaigns do not have to include awareness about policies and procedures only; they may also include educational materials for employees on how to notice suspicious employees doing suspicious activities (Dhillon & Torkzadeh, 2006) as well as on how to be aware of social engineering techniques employed by outsiders or malicious insiders. Clicking on phishing links or responding to an email allegedly coming from the IT department requesting the username and password are well known hackers' social engineering techniques to breach security. Building a robust behavioral knowledge among the employees may mitigate these types of threats.

Technical Knowledge: Self-efficacy, response costs, and response efficacy comprise the technical dimension of awareness. These are technical "know-hows" that are different from the behavioral policies. Security compliance self-efficacy is an employee's perception of his or her technical ability to abide by the policy (Warkentin et al., 2011). The second subtheme, response costs, refers to the employee perception of how policy compliance (ex: software update) is time-consuming and impedes daily work, and the last (response efficacy) is employees' perception of software effectiveness in preserving security.

Self-efficacy positively impacts IS policy compliance (Boss et al., 2009; Bulgurcu et al., 2010; Herath & Rao, 2009a; Johnston & Warkentin, 2010; Warkentin et al., 2011; Workman et al., 2008). If an employee has been trained to skillfully respond to any policy demand (e.g. training on password behaviors, Stanton et al., 2005), he or she will be apt to comply with the policy more than the employee who is poorly trained. "Resource availability" is a similar term advanced by Herath and Rao (2009a) and refers to the robust training of employees who subsequently tend to perceive themselves as more competent to comply with IS policies than the poorly trained employees.

The second technical measure negatively affecting compliance, response cost, is the employees' perception of IS solutions as being too cumbersome for daily activities. In other words, the response to comply may impede employees from giving their best to their projects. "Perceived response cost work impediment" and "perceived cost of compliance" are the terms used for this dimension of technical awareness. These constructs significantly affect attitudes toward solutions and intentions to comply (Herath & Rao, 2009a; Bulgurcu at al., 2010). Therefore, management needs to design solutions that make IS policy compliance as least cumbersome as possible. Solutions can include less complex yet still powerful security countermeasures

and incorporating updates during working hours as part of job descriptions (Bulgurcu et al., 2010).

"Response efficacy" explains the effectiveness of IS policies or packages to protect information (Johnston & Warkentin, 2010). A higher perception of response efficacy is associated with the intention to comply (Johnston & Warkentin, 2010) and a decrease in noncompliance (Workman et al., 2008). Adopting and disseminating awareness about powerful security tools in IS departments seems to be promising in encouraging IS policy compliance.

Informing Employees (Malicious Threat)

Pertaining to malicious threats, all the research dealing with IS policies also deal with IS policy awareness, which includes communicating information about sanctions upon failure to abide by IS policies (Straub, 1990; Straub & Nance, 1990; Straub & Welke, 1998). SETA programs dominate a good number of the papers categorized as dealing with negligent insiders, but the literature is silent on how SETA programs help the potential malicious insiders to devise their cunning plans. If IS management cannot differentiate between potential negligent and potential malicious employees, and IS provides training for all, does this training make the potential malicious insiders more knowledgeable or more capable of breaching the security? We found one study (Cronan et al., 2006) that may shed light on this subject. The students who were aware of the university policies were more prone to circumvent these policies than the students who were unaware of the policies. Furthermore, tech savvy students had a greater tendency to commit computer misuse than regular students (Cronan et al., 2006). However, it is not known if student behavior holds true among organizational employees.

This study raises a question: why do "the informed and the trained" in organizations comply and "the informed and the trained" in universities not comply? If the difference in the two settings is the presence (or absence) of forces such as accountability (its presence in organizations and its absence in universities), this then raises the question of whether the reality of compliance in organizations is due to the increase in awareness and the increase in self-efficacy or whether it is due to the presence of accountability. Since awareness of consequences (e.g. punishment) significantly impacts attitude on ethical decision making (Leonard et al., 2004), this could mean that awareness and training may help only in the presence of deterrence measures.

Training is important, but equally important is the method, the context, and the situational conditions of the training. In Puhakainen and Siponen's (2010) action research (one of the two action research studies, the other being that of Tsohou et al., 2015) they found that the integration of IS security training with the companies' normal daily business communication was crucial in enhancing users' motivation to comply with the IS security policies. In the same study, the authors found that continuous training, rather than a one-time training effort, increases compliance.

Another study found that early communication of upcoming implementation of IS policies (the steps that the employees need to take and how to take them) is found to be a significant antecedent in decreasing negative employee reaction and computer abuse (Lowry et al., 2015). The "what to do" and the "how to do" are termed "explanation adequacy." What could be a more promising antecedent though is the measuring of what we term "justification adequacy" and its impact on minimizing security policy violations. In other words the "why to comply" rather than just the "what" and the "how" is a promising construct for future research.

In summary, since SETA programs may include ethics training, it is important for organizations to understand that ethics training is beneficial only with the employees who follow the rules out of social conformity and those who exhibit high levels of self-control (Workman & Gathegi, 2007). Although the "E" (education) in SETA programs does not ensure 100 percent compliance, it does significantly affect a section of the employees who have certain individual characteristics. Stated differently, forming policies, communicating them, and educating employees are like putting "do not enter" signs on roads. These signs are sufficient for most citizens but not enough for some: some need physical barriers blocking the entrance of the road or hidden cameras watched by police officers to monitor movement. The notion of barriers and monitoring is the dimension depicted by our next theme: technical countermeasures that control access to systems and monitor the traffic on the networks.

Theme 3: Applying Technical Countermeasures

This is one of the least studied themes regarding insider threats in the information systems literature, probably because the computer science journals may have been attracting all the technical studies and experiements. Only 29 percent of the articles (19 out of 65) tested technical countermeasures in the negligent threat category. Nevertheless, the socio-technical aspect of technical countermeasures needs more attention by IS security research because of its importance.

For example, the mere presence (or absence) of technical countermeasures (e.g. software monitoring) depicts the deterrence (or development) philosophy adopted by IS management (Theme 1). Monitoring the IPs of employee computers to know who failed to update the security software is a good example of a strict deterrence approach. The absence of such a strict measure could signify in the user's perception that IS management is less serious about deterring noncompliance or at least less serious in using technical means to achieve deterrence. Another example is the impact of advance notice of technical monitoring: it seems the advance notice not only enhances deterrence but also cultivates trust between the employee and the organization. The advance notice of Internet usage monitoring has been shown to build trust between employees and organizations (Alder et al., 2006). We suggest that the studies on the socio-technical dimension of compliance need not be neglected nor left to the computer science field.

Technical Countermeasures (Negligent and Malicious Threats)

An important factor of enhancing technical countermeasures to deter IS misuse among negligent insiders is user participation in the design, creation, and implementation of technical preventives and access control (Dhillon & Torkzadeh, 2006; Spears & Barki, 2010) in the security risk management planning process. This technique positively influences the performance of technical security controls among users.

A second technique to increase the compliance of negligent insiders is the employment of technical interfaces (software applications that identify which projects an employee is working on and what databases he or she is accessing) which in turn increases online identifiability in the department, expectations of evaluation, awareness of monitoring, and the social presence of peers. All of these factors may increase the perceived accountability of the user, diminishing his or her intention to violate organizational access policies (Vance et al., 2015). It is true that technical controls are somehow used to deter negligent threat, but using them to deter *malicious* threat is even more emphasized in IS security literature.

In the case of malicious insider threats, 39 percent (11 out of 28) of the studies of malicious insiders consider technical countermeasures. These studies examine computer monitoring, access control, and auditing logs as ways to technically control and secure the systems. Tracking down questionable activities on the network and the subsequent punishment of perpetrators are the direct value of preventive countermeasures (Straub & Nance, 1990; Straub & Welke, 1998).

Technical preventives do not just block an employee from accessing an unauthorized database; they also deter all employees from accessing unauthorized databases if, for example, the system generates a monthly report on each and every employee's accessed files and databases and sends copies of the report each month to the respective employees and to their supervisors. The key issue here is that IS users should be aware of such countermeasures (Straub & Welke, 1998) (through the report, in this example) for this channel to have a deterring effect. If and when the employees learn that the IT department is using technical means to monitor their computer behaviors, they will be more likely to sense that the management is following a deterrence philosophy. For example, the presence of a monitoring system is usually communicated to employees by directly informing them about the presence of such a system (D'Arcy et al., 2009; Straub, 1990).

A more specific monitoring system is the community anomaly detection system (CADS), which extracts relational patterns in the patient records' access logs among work team members. Based on relational patterns, it detects a deviation from the pattern and sends a notice to security analysts to investigate the access logs of the user in question (Chen et al., 2012a).

Some compliance policies are subject to implementation by force through employing technical means. For example, enforcing the creation of complex secure passwords using a specific length of characters, capital and small letters, numbers, and punctuation are only possible through automated technical software. It is interesting to see how technical countermeasures enhance compliance in some dimensions, but at the same time, degrade it in other dimensions. Looking at the same case, password composition (numbers, punctuation, etc.) is significantly related to writing the password down (Zviran & Haga, 1999), and writing the password down is prohibited in the IS policies of organizations (see, for example, Renaud, 2012). IS management has yet to come up with solutions that ensure both the use of strong passwords and the prevention of writing the passwords down on paper or registering them in unencrypted unsecured smartphones. Since reusing passwords across sites is strongly discouraged, the users need tools to remember their ever increasing number of complex passwords. A solution could be the adoption or creation of password storage and management software solutions by IS departments. To the best of our knowledge, current IS departments are still fearful of

recommending the available third party solutions (e.g. LastPass). We suggest that each organization develop its own password storage website for its employees to use. Thus the organizational user passwords could remain inside the secure firewalls instead of being written on papers, saved on unsecured smartphones prone to be lost or stolen, or saved on third party cloud computing outsourced servers.

Although the significance of increasing the awareness of technical countermeasures as a deterrence measure has been proven in the literature, we argue that past research dealt with this countermeasure in a one-sided manner. There could be side effects of making employees aware of the types of technical countermeasures used. Potential opportunistic or malicious insiders could take advantage of such information and devise their acts accordingly. Therefore we propose two layers of technical countermeasures: declared and undeclared. The declared ones may deter the majority of employees from thinking about circumventing policies, and the undeclared ones may catch those who attempted to circumvent the known countermeasure by other ways.

In summary, applying technical countermeasures provides another layer of protection. This theme is in need of further IS research in order to more extensively cover the socio-technical side of it. The journals in the computer science and engineering disciplines contain extensive research on technical countermeasures, including access control, password mechanisms, and firewalls (Siponen & Oinas-Kukkonen, 2007). Future IS research should study the socio-technical effects of these technical countermeasures on insider behavior. We argue that this is an IS issue (socio-technical) rather than just a computer science issue (technical), because as we saw in the case of password change, employees may devise ways to circumvent technical countermeasures.

Finally, we conclude the procedural and technical countermeasures with the following observation: evident in these reviews of the literature is the assumption implicit in most empirical IS security research that IS security is de facto "good", that the more IS security, the better, and that motivating employees to comply with IS security is a highly desirable objective for IS departments. Moreover, the literature takes a distinct negative attitude towards employees who circumvent their organization's IS security policies. However, recent IS security (ISsec) research is starting to challenge this assumption. In an attempt to explain the high percentage of unexplained variance (50-70 percent) in employee IS security violations, D'Arcy et al. (2014) introduce the notion of stress related to the need to oblige IS security policies. Labeled technostress, this negative outcome experienced by employees trying to adhere to IS security policies reflects a downside of ISsec policies. We suggest that future research in IS security compliance needs to more comprehensively investigate the phenomenon of the downsides of IS security compliance efforts.

Theme 4: Enhancing the Environmental Countermeasures

Environmental countermeasures constitute the fourth and final theme of this study. The social environment plays a role in channelling deterring or encouraging messages to IS users. For example, negligent employees may experience shame inflicted on them by other more compliant employees. This social embarrassment channels a deterring message to other potential negligent insiders. This overarching theme of environment includes not just shame (which is part of subjective norms), but also organizational commitment and ethical climate, among others. Although this theme that comprises IT ethics is complex and intertwined on both individual and organizational levels (Chatterjee et al., 2015), we try to categorize the articles under separate groups: external and internal environments, corresponding to the organizational and individual levels respectively.

This theme is well studied, with 71 percent of the articles (46 out of 65) measuring some aspect of the environment dimension, and can be grouped into two sections: external and internal. The external environment depicts the organizational characteristics, including subjective and descriptive norms, and the overall social and moral environment within the organization. The internal environment depicts the individual characteristics of the employee, including his or her moral character.

External Environment (Negligent Threat)

Pertaining to negligent threats, ethical, professional, legal, and societal environments and climates in an organization could increase or decrease IS security policy compliance intentions (Banerjee et al., 1998; Leonard et al., 2004; Posey et al., 2011). The three major expressions of the external environment of organizations are subjective norms, descriptive norms, and organizational justice pertaining to IS security.

IS Security Subjective Norms: These norms refer to the perception of the IS user regarding whether his or her immediate significant environment (managers, colleagues, etc.) expects him or her to perform a

certain behavior (Herath & Rao, 2009a). Subjective norms are the same as normative beliefs, which increase ethical behavior intention regarding IS use (Leonard & Cronan, 2001; Pahnila et al., 2007; Siponen et al., 2010). If a manager has high expectations of his or her subordinates, it is likely that this will impact the behavior of the majority of the manager's employees. Johnston and Warkentin (2010) named this construct "social influence" and found, like Herath and Rao (2009a), that social influence impacts behavioral intentions. Along the same lines, Banerjee et al. (1998) found that situational characteristics (conventional beliefs and high expectations of managers) increased ethical behavior intention. In an opposite result, Siponen and Vance (2010) found that the impact of shame is nonsignificant when measured in the same model along with neutralization techniques used by employees. This means that the countermeasure results are not solely dependent on the message communicated from outside the person but also on the individual characteristics from within that person, which will be elaborated more fully in the internal environment section below.

Although neutralization is a cognitive technique, there are other noncognitive forces that may neutralize shame and the effect of the organizational security culture on the employees. For example, virtual status is the level and degree of business activities that an employee implements from different remote locations compared to within the organization itself (D'Arcy & Devaraj, 2012). These researchers found that virtual status increases technology misuse intention. We argue that this misuse is due to the absence of or decrease in the effect of organizational security culture on the employees (shame or subjective norms are neutralized in this case).

Descriptive norms refer to the perception of an IS user as to whether his or her colleagues are abiding by the IS policies or not. Herath and Rao (2009a) found that descriptive norms positively affect intention to comply. Banerjee et al. (1998) included role models in their description of situational characteristics. Apparently, good role models impact the ethical climate of the organization and channel a message of encouraging compliance.

Organizational Justice: Two studies investigated the organizational focus of justice in relation to IS policies and the expectations of IS management. They found that positive perception of organizational justice significantly decreases the intentional noncompliance of employees. The organizational justice theme regarding fair communication of sanctions and just distribution of sanctions among perpetrators is first investigated by Willison and Warkentin (2013) who proposed that the organizational injustice may increase the disgruntlement and subsequently the intentional computer abusive behaviors by the employees. The propositions advanced by Willison and Warkentin (2013) were tested by Li et al. (2014) who found that the increase in procedural justice and the distributive justice is positively related to IS policy compliance intentions.

External Environment (Malicious Threat)

Pertaining to malicious threats, subjective norms have no significance impact on malicious intentions. In contrast negative descriptive norms (bad role models) increase malicious predisposition among colleagues. One of the major predictors of computer crime is associating with friends who engage in the activity (Skinner & Fream, 1997). In other words, learning computer crime is primarily peer driven, which could be an echo of descriptive norms. Regarding subjective norms, Hu et al. (2011) found that shame had no impact on malicious insiders, unlike their negligent counterparts. This may be attributable to the criminal mindset that had already accounted for the cost of losing social credibility; therefore, shame may not have its full impact.

In summary, developing and sustaining an ethical environment maximizes IS security (Dhillon & Torkzadeh, 2006). In our survey, the external environment described organizational justice, as well as organizational subjective and descriptive norms in their positive and negative dimensions (reasonable expectations, role model and social pressure, differential association, respectively). We now turn attention to the internal environment section. Whereas the external environment deals with the issues outside and around the individual, the internal environment deals with the issues within him or her.

Internal Environment (Negligent Threat)

The internal environment is the personal individual moral convictions of each employee, including ethics, morality, organizational commitment, apathy, denial of responsibility, neutralization techniques, individual propensity, and locus of control. For example, individuals who have an internal locus of control take responsibility for their own actions, and therefore may be less inclined to omit IS security precautions at work (Workman et al., 2008). Some employees may be predisposed toward higher self-control. This predisposition increases an individual's intentions to comply with IS policies (Hu et al., 2015). In the same way, Lowry and Moody (2015) found that reactance proneness (another personal

characteristic that makes a person inclined to react to rules) may lead to security violation intention.

On the negligent level, Banerjee et al. (1998) talked about individual *ethical* characteristics that influence behavioral intent and high moral commitment that decreases IS misuse intention (D'Arcy et al., 2009). Gattiker and Kelley (1999) applied different levels of morality to the IT environment: personal (preferences and tastes), conventional (societal norms that dictate the perception of non-harmful but nevertheless unacceptable behaviors), and moral (social norms that dictate the perception of harmful acts). The latter study not only found that users differ from each other within the domains of morality, but also that young male employees are more vulnerable to err in the moral domain. Cronan et al. (2006) agreed, finding that males committed more IS misuse than females. Loch and Conger's (1996) findings may hint at a solution for the gender issue. The findings suggest that men make ethical decisions in computing acts based more on their attitude toward the ethical scenario rather than on the social norms, while woman intend to act ethically or unethically based more on the social norms, rather than on their attitude. This study tells us that men and women do not respond in the same way to the same countermeasures to the same degree. IT professionals probably need to work on the attitudes of men toward compliance, while the expectations and pressures of the socio-organizational environment will drive women toward compliance. Social norms do not seem to significantly affect the disposition of men toward ethical computing acts (Loch & Conger, 1996). This finding suggests two things: first, that the internal environment is a moderator of the relationship between procedural/technical countermeasures and employee compliance, and second, that there is no one-size-fits-all strategy toward the different types of insiders but rather that strategies should be customized based on individual characteristics.

Siponen and Vance (2010) studied neutralization techniques and found that all employees with high usage of these techniques were more inclined to violate IS policies. The scenario examples of their study include the following items: "It is not as wrong to violate a company information security policy that is not reasonable" and "It is all right to violate a company information security policy if you get your work done." This echoes what Harrington (1996) found to be true in one of her IS ethical hypotheses: "employees with high responsibility *denial* have a propensity to enact computer abuse."

Along the same lines, organizational commitment was found to significantly increase intentions to comply (Herath & Rao, 2009a), and apathy was found to decrease precautions taken to secure systems (Kirsch & Boss, 2007). Therefore, IS management should build the moral reasoning and the organizational commitment of employees by working on improving the internal and external ethical climates. Education has been a proven method in shaping the acceptable moral reasoning of individuals (Davis, 1987; Rest, 1979; Thoma & Davison, 1983). Another promising way to increase compliance is through legislation. Governmental regulations on IS policies increase individual beliefs in IS compliance (Cannoy & Salam, 2010). Thus organizations can push governments to legislate IS security policies. This will help increase compliance in organizations.

Nevertheless, there are some signs of new emerging dimensions being studied in the internal environment theme. These dimensions include the adoption of electrocognitive testing devices in measuring ISsec behaviors and the study of employees who attempt to enhance the security in their organizations above and beyond their basic duties. These two trends are described in the following paragraphs.

Security research started using electro-encephalography (EEG) measures which are neurophysiological lab experiments that analyze the trends of the brain waves that might be responsible for different security related behaviors (Vance et al., 2014). This type of IS research found that only those employees who have neurocognitive evidence of having higher self-control (neurons of the brain related to self-control are for some reason more developed) need to be trusted with and assigned to more sensitive digital assets (Hu et al., 2015). Nevertheless, schools of law assert that this type of neurological research, although interesting, is of little practical value because of ethical sensitivity and legal regulations governing practices such as employee job assignments that are the results of psychological screening (London & Bray, 1980).

Research on employees who attempt to enhance the security in their organizations above and beyond their expected basic duties was the focus of Hsu et al. (2015). They found out that organizational commitment, involvement and attachment significantly increase this "extra-role" security compliance. Although the antecedents of organizational commitment are not novel, nevertheless the dependent variable is somewhat novel. This type of new compliance behaviors are more distinct than the "traditional" dependent variables of security violation or compliance intention and may deserve separate considerations and explanations in the future (see Guo, 2013).

Internal Environment (Malicious Threat)

Regarding malicious insiders, an interesting insight comes from the canonical correlation analysis done by Shropshire (2009), when he analyzed documented stories of malicious and opportunistic insiders who were legally prosecuted in the past. The independent variables of this study were financial changes, relationship strains, substance abuse, and job changes; the dependent variables were IT sabotage (i.e., destroying data) and IT espionage (i.e., selling data). The results showed that only financial changes in the life of an employee correlated with IT espionage: financial crises moved employees to sell information to competitors. Relationship strains, substance abuse, and job changes correlated with IT sabotage. These findings may give IS management insights on the importance of scanning, profiling, and keeping a supervising eye on the changes in the lives of employees. The application of these findings is not unique to IS employees; nevertheless, IS management needs to apply these proactive methods to keep malicious insiders at bay. One of the major predictors of computer crime is associating with friends who engage in the activity. Learning computer crime is primarily peer-driven (Skinner & Fream, 1997), and peer behavior positively influences policy compliance intention (Herath & Rao, 2009b). Therefore, IS management should take heed to cultivate an IS department with the highest standards of moral and ethical behavior. This does not necessarily mean that IS departments should be saturated with the uncomfortable tension of shame, especially since shame and informal social sanctions are not promising constructs in deterring the misuse intentions of malicious insiders (Hu et al., 2011). However, attracting and keeping a large base of ethical employees and encouraging them to expect the highest standards of IS policy compliance from their peers should deter potential malicious insiders from acting on their schemes.

A third insight of securing the environment is found in Son (2011). The congruence between employees' intrinsic values and organizational values will encourage employees to abide by IS policies. Therefore, IS management should survey potential employees and only accept those whose moral values coincide with those of the organization. Nevertheless, this might not be realistic in the cases of outsourcing the service where IS management has no control over the employees of the provider. Future research should investigate the best ways to implement this congruence.

We have already noticed how neutralization techniques nullify the impact of formal and informal sanctions in the case of negligent insiders (Siponen & Vance, 2010). In the case of malicious insiders, this relationship may also hold true. Investigating new techniques to profile and identify malicious insiders or perhaps to empirically test the situational and behavioral characteristics or criminological settings (Banerjee et al., 1998; Willison & Backhouse, 2006) are some areas for studying malicious employees in the future.

In summary, the internal environment captures the ethical dimension, morality, organizational commitment, apathy, and neutralization strategies, all initiated within and related to the individual characteristics of the IS user. Promising countermeasures on the level of the internal environment are pre-employment screening, profiling, and training. Overall, the theme of environmental countermeasures covers the external (organizational climate) and internal (individual characteristics) dimensions that affect IS compliance. Lately, some authors (Chen et al., 2012b; Hu et al., 2012) have started using the term "security culture" in organizations, which is along the same lines of what we called environmental countermeasures.

Thus far, we described the four overarching themes emerging from the literature treating each theme simultaneously on both negligent and malicious insider levels. We now proceed to give brief summary overviews of negligent and malicious insider threats.

Summary Overview of Negligent and Malicious Insider Threats

As shown in Tables 3a and 3b, we found a less diversified research stream on malicious insider threats (3a) than on negligent insider threats (3b). The table is divided into two subcategories: articles dealing purely with malicious threats and articles dealing with both malicious and negligent threats. Table 3a suggests that the malicious category, an important but sensitive one, is not drawing much attention from researchers (only 22 different primary authors vs. 31 for negligent threats), although acts of espionage and sabotage are among the first five extremely significant overall threats (and the first three insider threats) to information security (Whitman, 2004). The uncategorized column (in Table 3b) incorporates the papers that were not clearly identified by the authors, either because of the absence or the vagueness of the instrument. Tables 3a and 3b are the secondary contributions of this study, providing an overview of IS security research.

Table 3a. Malicious Threats: Summary of Investigated Issues

Authors	Date	Philosophy of		Procedural Countermeasures		Technical Countermeasures	Environmental Countermeasures
		Deterrence	Development	Forming Policies	Informing Employees		
Purely Malicious (4 studies)							
Hu et al.	2011	+					+
Skinner & Fream	1997	+					+
Chen et al.	2012a	+				+	
Willison & Warkentin	2013	+					+
Malicious and Negligent Intertwined (24 studies)							
Boss et al.	2015		+		+		
Chatterjee et al.	2015	+	+	+	+	+	+
Chen et al.	2012b	+		+		+	
Chen & Zahedi	2016		+		+		
D'Arcy et al.	2014	+		+		+	
Dhillon & Torkzadeh	2006	+	+	+	+	+	+
Herath et al.	2014		+			+	
Hsu et al.	2015		+	+			+
Hu et al.	2015						+
Johnston et al.	2015	+	+	+	+		
Kankanhalli et al.	2003	+				+	
Lee et al.	2004	+		+	+		+
Li et al.	2014	+	+	+	+		+
Lowry et al.	2015	+	+	+	+		+
Lowry & Moody	2015	+		+			+
Shropshire	2009						+
Son	2011	+					+
Stahl et al.	2012	+		+			
Straub	1990	+		+	+	+	+
Straub & Nance	1990	+		+	+	+	
Straub & Welke	1998	+		+	+	+	
Tsohou et al.	2015		+	+	+		
Vance et al.	2014		+				+
Vance et al.	2015	+			+	+	+

Table 3b. Negligent Threats: Summary of Investigated Issues

Authors	Date	Philosophy of		Procedural Countermeasures		Technical Countermeasures	Environmental Countermeasures
		Deterrence	Development	Forming Policies	Informing Employees		
Purely Negligent (37 studies)							
Alder et al.	2006					+	
Banerjee	1998						+
Boss et al.	2009	+	+	+	+		+
Bulgurcu et al.	2010	+	+		+		+
Cannoy & Salam	2010			+	+		+
Cronan et al.	2006			+	+		+
D'Arcy & Devaraj	2012	+		+			+
D'Arcy et al.	2009	+		+	+	+	+
D'Arcy & Hovav	2007			+	+	+	
Gattiker & Kelley	1999						+
Guo & Yuan	2012	+		+			+
Guo et al.	2011	+	+				+
Harrington	1996	+		+	+		+
Herath & Rao	2009a	+	+	+	+	+	+
Herath & Rao	2009b	+	+	+			+
Hovav & D'Arcy	2012	+		+		+	+
Hu et al.	2012		+	+			+
Johnston & Warkentin	2010		+		+		+
Kirsch & Boss	2007	+	+	+			+
Leonard	2001						+
Leonard et al.	2004				+		+
Li et al.	2010	+					+
Loch & Conger	1996						+
Myyry et al.	2009	+					+
Ng et al.	2009		+		+		+
Pahnila & Siponen	2007	+	+				+
Peace et al.	2003	+					+
Puhaikenen & Siponen	2010		+	+	+		
Siponen et al.	2010	+	+		+		+
Siponen & Vance	2010	+					+
Smith et al.	2012	+		+	+		
Spears & Barki	2010			+	+	+	
Stanton et al.	2005		+		+	+	
Vance et al.	2012		+		+		+
Warkentin et al.	2011		+		+		+
Workman et al.	2008		+				+
Zviran & Haga	1999					+	
Uncategorized (2 studies)							
Doherty & Fulford	2005			+			
Workman & Gathegi	2007	+			+		+

Upon first glance of Table 3b, we find a well-diversified research stream on negligent insider threats. The research was spread over an inclusive timeframe of 1996 to 2015. Articles incorporating one or more of the identified themes and subthemes are marked with a plus sign in the relative theme and subtheme columns. We found a spike in studying negligent insiders in the more recent years (78 percent of the insider articles, 36 out of 46 papers, were from 2007-2015 inclusive).

Table 4 summarizes our findings (the themes, the interaction between the different philosophies on one hand and the different countermeasures on the other) and highlights the study areas to which future research may turn its attention. This table is considered one of the main contributions of this study. We identified two philosophies of IS management (philosophy of deterrence and philosophy of development) and three countermeasures (procedural, technical, and environmental). The interaction and relation between philosophies and countermeasures, what we know about them and what we still lack knowledge of, are discussed in the next paragraphs.

The literature informs us that coercive procedures, like tough punishments (i.e., sanctions), in the case of noncompliance are emphasized under IS department philosophy of deterrence. Nevertheless, we do not know if these sanctions would be implemented in an organization where the philosophy of development is stressed. Thus, the cell in the first row and column of Table 4 mentions a "high emphasis" on sanctions, and the cell in the first row and second column mentions "future research." Since the literature does not cover the existence of deterrent procedural measures in organizations that adopt an encouraging developmental philosophy, we leave the case open for future research.

Based on our review findings, we posit that empowering procedural measures (e.g. training, rewards) and empowering environmental measures (e.g. praising good role models) are highly employed in organizations where a developmental IS philosophy of management is dominant. We provide examples and proofs of this in the conceptual themes section. Along the same lines, coercive technical measures (e.g. computer monitoring) and coercive environmental measures (e.g. subjective norms) could be implemented in organizations where a deterrence IS philosophy of management is dominant (see the conceptual themes section). Based on the extant literature, what is still unknown is whether *developmental* countermeasures (procedural, technical, or environmental) are employed or made use of in organizations that have a *deterrence* philosophy, and if they are: 1) what is the nature of such countermeaures, 2) are they beneficial or not, and most importantly, 3) what is the nature of interaction between the coercive and empowering countermeasures (i.e., does an empowering countermeasure neutralize the deterrent effect of a coercive countermeasure?). The same questions could be asked about coercive countermeasures implemented in organizations where a developmental IS philosophy is implemented. The probable use of developmental countermeasures in organizations that have a deterrence philosophy and the probable use of deterrent countermeasures in organizations that have a development philosophy could be labeled strange bedfellows. These countermeasures and philosophies may interact. The interactions are still largely unknown for IS security research, therefore we categorize them under "future research." We find an insight and a pointer to such an interaction in economics. Both punishments and rewards are tested together in the same experimental model and the results are different than when punishment is tested alone apart from the rewards, or the latter apart from the former (Andreoni et al., 2003). In Andreoni et al., the authors had the participants play a simple proposer-responder game. In the first stage, a participant (called the proposer) chooses what portion of $2.40 he or she needs to transfer to the responder. The main difference among the four treatments is in the responder's capacity to punish or reward during the second stage. Four treatments are available: 1) neither punish nor reward, 2) punish or reward by decreasing or increasing the proposer's earnings by 5 cents at a cost of 1 cent, 3) only punish, and 4) only reward. The study found that using both punishments and rewards in the same treatment had a significant strong effect. Even though generous offers were not punished, such generosity only occurred when the threat of punishments existed. The same, similar, or different interactions may also be present in IS security. For example, it may be true that IS security developmental and encouraging endeavors will show maximum impact on IS compliance intentions only if and when there is a threat of punishment.

Overview of Theories

The major theories used in IS policy compliance and insider threat issues in both their forms (negligent and malicious) are depicted in Table 5a. Thirty one percent of the articles (21 out of 67) used a theory that drew upon the GDT of criminology. The second most-used theory is the theory of planned behavior (TPB) (18 percent; 12 papers), followed by the theory of reasoned action (TRA) (13 percent; nine papers), and protection motivation theory (13 percent; nine papers).

Table 4. The Research Findings and Suggestions for Future Research

Countermeasures		IS Management Security Philosophy	
		Deterrence	**Development**
Procedural	Coercive Procedural	High Emphasis (ex: sanctions)	*Future Research*
	Empowering Procedural	*Future Research*	High Emphasis (ex: rewards, training)
Technical	Coercive Technical	High Emphasis	*Future Research*
	Empowering Technical	*Future Research*	*Future Research*
Environmental	Coercive Environmental	High Emphasis (ex: subjective norms)	*Future Research*
	Empowering Environmental	*Future Research*	High Emphasis (ex: role models)

Table 5a. Major Theories Used in IS Policy Compliance

General Deterrence Theory (32%)*	Theory of Planned Behavior (18%)	Theory of Reasoned Action (14%)	Protection Motivation Theory (14%)
Boss et al. (2009); Chen et al. (2012b); D'Arcy et al. (2009); D'Arcy & Devaraj (2012); Guo et al. (2011); Guo & Yuan (2012); Harrington (1996); Herath & Rao (2009a); Hu et al. (2011); Kankanhalli et al. (2003); Lee et al. (2004); Li et al. (2014); Pahnila et al. (2007); Peace et al., (2003); Siponen et al. (2010); Siponen & Vance (2010); Son (2011); Straub (1990); Straub & Nance (1990); Straub & Welke (1998); Workman & Gathegi (2007)	Banerjee et al. (1998); Boss et al. (2009); Bulgurcu et al. (2010); Cronan et al. (2006); Herath & Rao (2009a); Hu et al. (2012); Johnston & Warkentin (2010); Lee et al. (2004); Leonard et al. (2004); Ng et al. (2009); Peace et al. (2003); Workman & Gathegi (2007)	Banerjee et al. (1998); Cannoy & Salam (2010); Guo et al. (2011); Johnston & Warkentin (2010); Lee et al. (2004); Leonard et al. (2004); Loch & Conger (1996); Pahnila et al. (2007); Siponen et al. (2010)	Boss et al. (2015); Herath & Rao (2009a); Chen & Zahedi (2016); Johnston & Warkentin (2010); Johnston et al. (2015); Pahnila et al. (2007); Siponen et al. (2010); Vance et al. (2012); Workman et al. (2008)

*Percentage of articles using the theory (exclusively or partly).

Seventy six percent of the articles (51 out of 67) incorporated at least one of these four theories. Only 33 articles (49 percent) did not use any of these major four theories. The first three theories are heavily used because of the vast similarities between regular criminology and cybercriminology (GDT), the explanatory power of human behavior in management (TPB and TRA), and because some key highly successful pioneer articles were based on GDT (namely Straub, 1990 and Straub & Nance, 1990), which triggered a wave of adaptations of the same theory.

Future research is advised to depart from GDT and PMT by incorporating other theories from criminology (e.g., rehabilitation theory, incapacitation theory, and retribution theory) or theories from other reference disciplines of psychology and management. Table 5b depicts other theories used in IS compliance research to date. In Siponen and Oinas-Kukkonen's (2007) security review article, they underlined the fact that since deterrence criminology strategies are used extensively, researchers should investigate non-deterrence motivational and ethical strategies as well, based on psychology and philosophy, respectively. Comparing Tables 5a and 5b, it appears that over the last decade (2007 and on), researchers have investigated more non-deterrence strategies as opposed to previous years. Nevertheless, GDT and PMT still occupy prominent places among the preferred theories among IS security researchers.

Overview of Methodologies

Figure 1 depicts the methodologies used in the sample articles of this review paper. Seventy-six percent of the articles (51 out of 67) incorporated surveys in their research methodology, and 72 percent used surveys solely as their instrument (11 percent for lab experiments, 6 percent for interviews, 5 percent mixed methods; 3 percent for action research, and 1.5 percent for direct observation of logs and archival analysis each).

Table 5b. Other Theories Used in IS Policy Compliance

Theory	Source
Accountability Theory	Vance et al. (2015)
Action-Network Theory	Tsohou et al. (2015)
Agency Theory	Boss et al. (2009); Herath & Rao (2009b);
Buy-in Theory of Participation	Spears & Barki (2010)
Causal Reasoning Theory	Posey et al. (2011)
Cognitive Learning Theory	Lowry et al. (2013)
Contextualism Theory	Tsohou et al. (2015)
Coping Theory	D'Arcy et al. (2014)
Domain Theory of Moral Development	Gattiker & Kelley (1999)
Emergent Interactions Theory	Spears & Barki (2010)
Ethical Theory	Chatterjee et al. (2015)
Expectancy Theory	Lowry et al. (2013)
Expected Utility Theory	Peace et al. (2003)
Extended Parallel Process Model	Johnston & Warkentin (2010)
Fairness Theory	Lowry et al. (2015)
Fear Appeal Theory	Johnston & Warkentin (2010)
Fishbein and Ajzens Theory	Leonard & Cronan (2001)
Habit Theory	Vance et al. (2012)
Innovation Diffusion Theory	Siponen et al. (2010)
Kohlberg Cognitive Moral Development Theory	Leonard & Cronan (2001); Myyry et al. (2009)
Moral Disengagement Theory	D'Arcy et al. (2014)
Neutralization Theory	Siponen & Vance (2010)
Organismic Integration Theory	Boss et al. (2009)
Organizational Control Theory	Boss et al. (2009); Kirsch & Boss (2007); Lowry & Moody (2015)
Organizational Justice Theory	Li et al. (2014)
Rational Choice Theory	Bulgurcu et al. (2010); Hu et al. (2011); Li et al. (2010);
Reactance Theory	Lowry & Moody (2015); Lowry et al. (2015)
Self-Control Theory	Hu et al. (2015)
Social Cognitive Theory	Workman et al. (2008)
Social Control Theory	Hsu et al. (2015); Hu et al. (2011); Lee et al. (2004)
Theory (cont.)	**Source**
Social Influence Theory	Boss et al. (2009)
Social Learning Theory	Skinner & Fream (1997); Warkentin et al. (2011)
Structuration Theory	Tsohou et al. (2015)
System Quality Theory	Spears & Barki (2010)
Technology Acceptance Theory (TAM)	Herath et al. (2014)
Technology Threat Avoidance Theory	Herath et al. (2014)
Theory of Motivational Types of Values	Myyry et al. (2009)
Universal Constructive Instructional Theory	Puhaikenen & Siponen (2010)

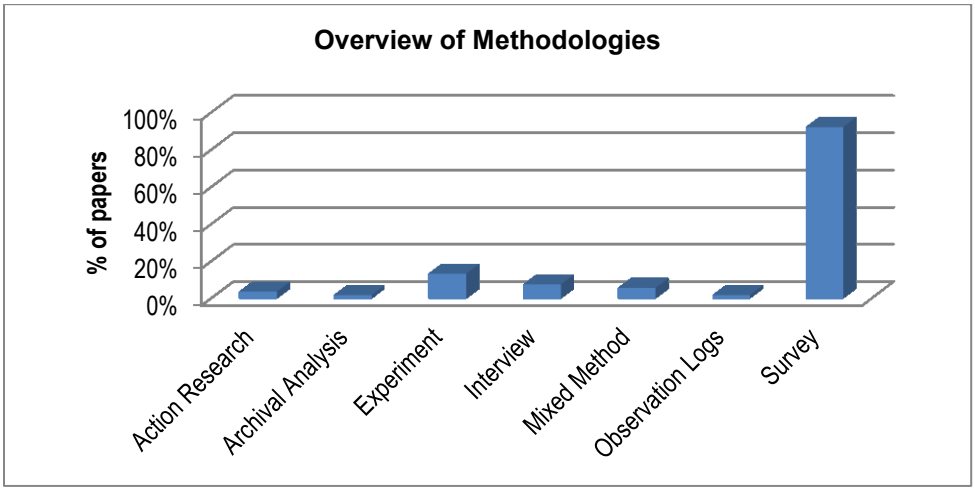

Figure 1: The Distribution of Papers across Methodologies

Furthermore, these 88 percent of the survey articles have some measure of common-method variance risk, since the studies asked the same employees about the countermeasures as well as their intention to comply. Along the same lines, Workman et al. (2008) found that there is some discrepancy between subjective and objective compliance measures. The first is related to the survey measuring self-reported subjective compliance and the second to the observation of computer logs measuring actual objective compliance (computer logs of password changes, security patch updates, and backups). Future research should, where possible, rely less on subjective measurements (surveys) and more on objective methods to measure compliance (observation of logs, lab experiments, triangulation of surveys, etc.). Nevertheless, we acknowledge the difficulty of measuring actual compliance in organizations or requesting and accessing computer logs from IT departments. In the case of the latter, these logs are highly vulnerable data that few organizations are willing to disclose. Even more difficult is the collection of data about malicious noncompliance, since actual malicious behavior is typically only noticed after the fact, and then the IT department is even more protective of the information about the incidents in order to protect the organization from a poor reputation and bankruptcy. Lab experiment simulations, archival document analysis, and interviewing convicted IT criminals may be promising instruments in research on malicious insiders and may alleviate the paucity and difficulty of gathering data on malicious threats.

Contributions and Conclusion

This paper has presented a review of the literature on IS security policy compliance in organizations. Since the literature does not explicitly differentiate malicious from nonmalicious threats (Guo et al., 2011), we endeavored to divide the articles in our sample into those dealing with malicious employees and those dealing with negligent employees. This is one of the contributions of this study (Appendix A). Appendix A shows that the majority of researchers lumped all insider types (naïve, opportunistic, and malicious) into one camp and tried to measure and test their models accordingly. This has the inherent weakness of not knowing how each insider type behaves. Future research may try to test models with each insider type and find out if there is a difference among the direction, significance, and power of the relationships between each countermeasure and philosophy on one hand and policy compliance or compliance intention on the other.

The second contribution is the all-inclusive Insider Types - Matrix (Table 1), which does not have the weaknesses of traditional taxonomies (Stanton et al., 2005; Willison & Warkentin, 2013). Traditional taxonomies, although they do have the insiders' malicious or negligent intention component, either lack the willingness to comply or the ability components, or in the case of Guo (2013) does not come up with insider or IS user names or types. Our taxonomy divides IS users based on all three dimensions of intention, ability, and willingness as well as names the types of insiders (negligent naïve, negligent opportunistic, and malicious insider).

The third and a major contribution of this article is the identification of the building blocks for a potential indigenous IS security theory. Grounding the analysis in the literature, we inductively identified four themes to foster Information Security policy compliance among employees. The four themes are: 1) IS management philosophies of deterrence and

development, 2) procedural countermeasures, 3) technical countermeasures, and 4) environmental countermeasures. We propose that future research can draw upon these themes, find the relationships among them, and use them as the building blocks of a potential indigenous IS security theory.

The fourth contribution consists of a list of potential research areas regarding the interactions between different philosophies in one hand and different countermeasures on the other (Table 4). The four contributions mentioned above are on the academic theoretical level.

On the professional level, our review identifies and summarizes the antecedents to IS policy compliance. In the case of negligent insiders, these mainly include employing a deterrence or encouraging approach, forming policies, imparting behavioral and technical knowledge to employees, making use of technical countermeasures, and enhancing the environment by clarifying the subjective norms, encouraging positive descriptive norms, improving organizational justice, and developing inner ethical convictions among users. In the case of malicious insiders, these antecedents mainly include employing a deterrence approach, forming policies, informing employees about these policies, intensively making use of technical countermeasures, and enhancing the environment by clarifying the subjective norms, decreasing negative descriptive norms, and noticing personal struggles in the lives of employees. Specific managerial practicial insights were given in the body of the text whenever the relevancy demanded.

Future research should carefully trace security incidents to negligent, opportunistic, or malicious reasons. Dividing the target audience into the types of insiders (Crossler et al., 2013) and devising a specific approach for each type (Straub & Widon, 1984) and a weighted amount of procedural versus technical countermeasures may yield the most promising results. At a minimum level, if the papers explicitly define which type of incidents they are measuring, it will be clear that the measured variables would be significantly related to that specific type of insider or incident and perhaps researchers will find that some countermeasures are more or less successful toward decreasing other types of incidents.

Although practitioner-based journals and magazines cover security standards and best practices extensively (Ma & Pearson, 2005), the need for peer-reviewed academic theory-based and empirically tested research on IS policy compliance remains large. Moving toward the development of a theory of security, and specifically, a theory of insider threat mitigation is in order. We believe that the review presented in this paper provides the building blocks of such a potential future theory.

References

Alder, G. S., Noel, T. W., and Ambrose, M. L. (2006). "Clarifying the Effects of Internet Monitoring on Job Attitudes: The Mediating Role of Employee Trust." *Information & Management*, Vol. 43, No. 7: pp. 894-903.

Andreoni, J., Harbaugh, W., and Vesterlund, L. (2003). "The Carrot or the Stick: Rewards, Punishments, and Cooperation." *American Economic Review*, Vol. 93, No. 3: pp. 893–902.

Banerjee, D., Cronan, T. P., and Jones, T. W. (1998). "Modeling IT Ethics: A Study in Situational Ethics." *MIS Quarterly*, Vol. 22, No. 1: pp. 31–60.

BBC News (2015, July 20). "Ashley Madison Infidelity Site's Customer Data Stolen." Retrieved April 9, 2016, from http://www.bbc.com/news/technology-33592594

Boss, S., Kirsch, L., Angermeier, I., Shingler, R., and Boss, R. (2009). "If Someone Is Watching, I'll Do What I'm Asked: Mandatoriness, Control, and Information Security." *European Journal of Information Systems*, Vol. 18, No. 2: pp. 151-164.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., and Polak, P. (2015). "What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors." *MIS Quarterly,* Vol. 39, No. 4: pp. 837-864.

Boudreau, M.C. and Robey, D. (2005). "Enacting Integrated Information Technology: A Human Agency Perspective." *Organization Science*, Vol. 16, No. 1: pp. 3-18.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. (2010). "Information Security Policy Compliance: An Empirical Study of Rationality-based Beliefs and Information Security Awareness." *MIS Quarterly*, Vol. 34, No. 3: pp. 523-548.

Cannoy, S. D. and Salam, A. F. (2010). "A Framework for Health Care Information Assurance Policy and Compliance." *Communications of the ACM*, Vol. 53, No. 3: pp. 126-131.

Chatterjee, S., Sarker, S., and Valacich, J. S. (2015). "The Behavioral Roots of Information Systems Security: Exploring Key Factors Related to Unethical IT Use." *Journal of Management Information Systems*, Vol. 31, No. 4: pp. 49-87.

Chen, Y., Nyemba, S., and Malin, B. (2012a). "Detecting Anomalous Insiders in Collaborative Information Systems." *IEEE Transactions on Dependable and Secure* Computing, Vol. 9, No. 3: pp. 332-344.

Chen, Y. R., Ramamurthy, K. and Wen, K.-W. (2012b). "Organizations' Information Security Policy Compliance: Stick or Carrot approach?" *Journal of Management Information Systems,* Vol. 29, No. 3: pp. 157-188.

Chen, Y. and Zahedi, F. M. (2016). "Individuals' Internet Security Perceptions and Behaviors: Polycontextual Contrasts Between the United States and China." *MIS Quarterly,* Vol. 40, No. 1: pp. 205-222.

Cronan, T. P., Foltz, C. B., and Jones, T. W. (2006). "Piracy, Computer Crime, and IS Misuse at the University." *Communications of the ACM*, Vol. 49, No. 6: pp. 85-90.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M. and Baskerville, R. (2013). "Future Directions for Behavioral Information Security Research." *Computers & Security*, Vol. 32, pp. 90-101.

D'Arcy, J. and Devaraj, S. (2012). "Employee Misuse of Information Technology Resources: Testing a Contemporary Deterrence Model." *Decision Sciences,* Vol. 43, No. 6: pp. 1091-1124.

D'Arcy, J. and Herath, T. (2011). "A Review and Analysis of Deterrence Theory in the IS Security Literature: Making Sense of the Disparate Findings." *European Journal of Information Systems*, Vol. 20, No. 6: pp. 643-658.

D'Arcy, J. and Hovav, A. (2007). "Deterring Internal Information Systems Misuse." *Communications of the ACM*, Vol. 50, No. 10: pp. 113-117.

D'Arcy, J., Hovav, A., and Galletta, D. (2009). "User Awareness of Security Countermeasures and its Impact on Information Systems Misuse: A Deterrence Approach." *Information Systems Research*, Vol. 20, No. 1: pp. 79-98.

D'Arcy, J., Herath, T., and Shoss, M. K. (2014). Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective." *Journal of Management Information Systems,* Vol. 31, No. 2: pp. 285-318.

Davis, L. F. (1987). *Moral Judgment Development of Graduate Management Students in Two Cultures: Minnesota and Singapore* (Unpublished Doctoral Dissertation). University of Minnesota, Minneapolis, MN.

Dhillon, G. and Torkzadeh, G. (2006). "Value-focused Assessment of Information System Security in Organizations." *Information Systems Journal*, Vol. 16: pp. 293-314.

Doherty, N. F. and Fulford, H. (2005). "Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis." *Information Resources Management Journal,* Vol. 18, No. 4: pp. 21-39.

Fullbright Commission. (2015). "Cultural Differences." Retrieved August 24, 2015, from http://www.fulbright.org.uk/pre-departure/us-culture/cultural-differences

Gattiker, U. E. and Kelley, H. (1999). "Morality and Computers: Attitudes and Differences in Moral Judgments." *Information Systems Research*, Vol. 10, No: 3: pp. 233–254.

Guo, K. H. (2013). "Security-related Behavior in Using Information Systems in the Workplace: A Review and Synthesis." *Computers & Security,* Vol. 32: pp. 242-251.

Guo, K. H., and Yuan, Y. (2012). "The Effects of Multilevel Sanctions on Information Security Violations: A Mediating Model." *Information & Management*, Vol. 49, No. 6: pp. 320-326.

Guo, K., Yufei, Y., Archer, N., and Connelly, C. (2011). "Understanding Non-malicious Security Violations in the Workplace: A Composite Behavior Model." *Journal of Management Information Systems*, Vol. 28, No. 2: pp. 203-236.

Harrington, S. J. (1996). "The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions." *MIS Quarterly*, Vol. 20, No. 3: pp. 257-278.

Herath, T. and Rao, H. (2009a). "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations." *European Journal of Information Systems*, Vol. 18, No. 2: pp. 106-125.

Herath, T., and Rao, H. (2009b). "Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effecrtiveness." *Decision Support Systems,* Vol. 47, No. 2: pp. 154-165.

Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., and Rao, H. R. (2014). "Security Services as Coping Mechanisms: An Investigation into User Intention to Adopt an Email Authentication Service." *Information Systems Journal,* Vol. 24, No. 1: pp. 61-84.

Hovav, A. and D'Arcy, J. (2012). "Applying an Extended Model of Deterrence across Cultures: An Investigation of Information Systems Misuse in the U.S. and South Korea." *Information & Management,* Vol. 49, No. 2: pp. 99–110.

Hu, Q., Xu, Z., Dinev, T., and Ling, H. (2011), "Does Deterrence Work in Reducing Information Security Policy Abuse by Employees?" *Communications of the ACM*, Vol. 54, No. 6: pp. 54-60.

Hu, Q., Dinev, T., Hart, P., and Cooke, D. (2012). "Managing Employee Compliance with Information Security Policy: The Critical Role of Top Management and Organizational Culture." *Decision Sciences,* Vol. 43, No. 4: pp. 615-659.

Hu, Q., West, R., and Smarandescu, L. (2015). "The Role of Self-control in Information Security Violations: Insights from a Cognitive Neuroscience Perspective." *Journal of Management Information Systems*, Vol. 31, No. 4: pp. 6-48.

Hui, K. L., Teo, H. H., and Lee, S. Y. T. (2007). "The Value of Privacy Assurance: An Exploratory Field Experiment." *MIS Quarterly,* Vol. 31, No. 1: pp. 19-33.

Hunter, P. (2003). "Computer Espionage." *Computer Fraud & Security*, Vol. 7: pp. 16.

Hsu, J. S. C., Shih, S. P., Hung, Y. W., and Lowry, P. B. (2015). "The Role of Extra-role Behaviors and Social Controls in Information Security Policy Effectiveness." *Information Systems Research,* Vol. 26, No. 2: pp. 282-300.

Johnston, A. C., and Warkentin, M. (2010). "Fear Appeals and Information Security Behaviors: An Empirical Study." *MIS Quarterly*, Vol. 34, No. 3: pp. 549-566.

Johnston, A. C., Warkentin, M., and Siponen, M. T. (2015). "An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset Through Sanctioning Rhetoric." *MIS Quarterly,* Vol. 39, No. 1: pp. 113-134.

Kankanhalli, A., Teo, H., Tan, B. C. Y., and Wei, K. (2003). "An Integrative Study of Information Systems Security Effectiveness." *International Journal of Information Management*, Vol. 23, No. 2: pp. 139-154.

Kirsch, L. and Boss, S. (2007). "The Last Line of Defense: Motivating Employees to Follow Corporate Security Guidelines." *ICIS 2007 Proceedings*. Paper 103. http://aisel.aisnet.org/icis2007/103

Lee, S. M., Lee, S. G., and Yoo, S. (2004). "An Integrative Model of Computer Abuse Based on Social Control and General Deterrence Theories." *Information & Management,* Vol. 41, No. 6: pp. 707-718.

Leidner, D. and Kayworth, T. (2006). "Review: A Review of Culture in Information Systems Research: Toward a Theory of Information Technology Culture Conflict." *MIS Quarterly*, Vol. 30, No. 2: pp. 357-399.

Leonard, L. N. K., Cronan, T. P., and Kreie, J. (2004). "What Influences IT Ethical Behavior Intentions - Planned Behavior, Reasoned Action, Perceived Importance, or Individual Characteristics?" *Information & Management*, Vol. 42, No. 1: pp. 143-158.

Leonard, L. N. K. and Cronan, T.P. (2001). "Illegal, Inappropriate, and Unethical Behavior in an Information Technology Context: A Study to Explain Influences." *Journal of the Association of Information Systems*, Vol. 1, No. 12: pp. 1–31.

Li, H., Zhang, J., and Sarathy, R. (2010). "Understanding Compliance with Internet Use Policy from the Perspective of Rational Choice Theory." *Decision Support Systems*, Vol. 48, No. 4: pp. 635–645.

Li, H., Sarathy, R., Zhang, J., and Luo, X. (2014). "Exploring the Effects of Organizational Justice, Personal Ethics and Sanction on Internet Use Policy Compliance." *Information Systems Journal,* Vol. 24, No. 6: pp. 479-502.

Lim, V. K. G., Teo, T. S. H., and Loo, G. L. (2002). "How Do I Loaf Here? Let me Count the Ways." *Communications of the ACM*, Vol. 45, No. 1: pp. 66-70.

Loch, K., Carr, H., and Warkentin, M. (1992). "Threats to Information Systems: Today's Reality, Yesterday's Understanding." *MIS Quarterly*, Vol. 16, No. 2: pp. 173-186.

Loch, K. D., and Conger, S. (1996). "Evaluating Ethical Decision Making and Computer Use." *Communications of the ACM*, Vol. 39, No. 7: pp. 74-83.

London, M. and Bray, D. W. (1980). "Ethical Issues in Testing and Evaluation for Personnel Decisions." *American Psychologist,* Vol. 35, No. 10: pp. 890–901.

Lowry, P. B., Moody, G. D., Galetta, D. F., and Vance, A. (2013). "The Drivers in the Use of Online Whistle-Blowing Reporting Systems." *Journal of Management Information Systems,* Vol. 30, No. 1: pp. 153-189.

Lowry, P. B., Romans D., and Curtis A. (2004). "Global Journal Prestige and Supporting Disciplines: A Scientometric Study of Information Systems Journals." *Journal of the Association for Information Systems*, Vol. 5, No. 2: pp. 29-77.

Lowry, P. B. and Moody, G. D. (2015). "Proposing the Control-Reactance Compliance Model (CRCM) to Explain Opposing Motivations to Comply with Organisational Information Security Policies*." Information Systems Journal*, Vol. 25, No. 5: pp. 433-463.

Lowry, P. B., Posey, C., Bennett, R. B. J., and Roberts, T. L. (2015). "Leveraging Fairness and Reactance Theories to Deter Reactive Computer Abuse Following Enhanced Organisational Information Security Policies: An Empirical Study of the Influence of Counterfactual Reasoning and Organisational Trust." *Information Systems Journal,* Vol. 25, No. 3: pp. 193-273.

Ma, Q. and Pearson, J. M. (2005). "ISO 17799: "Best Practices" in Information Security Management?" *Communications of the AIS*, Vol. 15, No. 1: pp. 577-591.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., and Vance, A. (2009). “What Levels of Moral Reasoning and Values Explain Adherence to Information Security Rules? An Empirical Study.” *European Journal of Information Systems*, Vol. 18, No. 2: pp. 126-139.

Neumann, P. G. (1999). “Risks of Insiders.” *Comunications of the ACM,* Vol. 42, No. 12: pp. 160.

Ng, B.-Y., Kankanhalli, A., and Xu, Y. C. (2009). “Studying Users' Computer Security Behavior: A Health Belief Perspective.” *Decision Support Systems,* Vol. 46, No. 4: pp. 815-825.

Pahnila, S., Siponen, M., and Mahmood, A. (2007). “Employees’ Behavior Towards IS Security Policy Compliance,” in 40th *Hawaii International Conference on System Sciences* (HICSS 07). Hawaii, USA.

Peace, A. G., Galletta, D., and Thong, J. Y. L. (2003). “Software Privacy in the Workplace: A Model and Empirical Test,” *Journal of Management Information Systems*, Vol. 20, No. 1: pp. 153-177.

Ponemon Institute (2012). *2013 State of the Endpoint*. Traverse City, MI. Available at http://www.ponemon.org/blog/2013-state-of-the-endpoint

Posey, C., Bennett, R. J., and Roberts, T. L. (2011). “Understanding the Mindset of the Abusive Insider: An Examination of Insiders’ Causal Reasoning Following Internal Security Changes.” *Computers & Security,* Vol. 30, No. 6: pp. 486-497.

Puhakainen, P. and Siponen, M. (2010). “Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study.” *MIS Quarterly,* Vol. 34, No. 4: pp. 757-778.

PWC, PricewaterhouseCoopers. (2015). *Managing Cyber Risks in an Interconnected World: Key Findings from the Global State of Information Security Survey 2015*. Retrieved from http://www.pwc.com/gsiss2015

Renaud, K. (2012). “Blaming Noncompliance Is Too Convenient: What Really Causes Information Breaches?” *Security & Privacy*, Vol. 10, No. 3: pp. 57-63.

Rest, J. R. (1979). *Development in Judging Moral Issues*. Minneapolis, MN: University of Minnesota Press.

Richardson R. (2011). “15th Annual 2010/2011 Computer Crime and Security Survey.” *Computer Security Institute*. Available at http://reports.informationweek.com/abstract/21/7377/Security/research-2010-2011-csi-survey.html

Sharp, A. (2015, Aug 24). “Two People May Have Committed Suicide After Ashley Madison Hack: Police.” Retrieved April 9, 2016, from http://www.wired.com/2015/08/ashley-madison-ceo-resigns-wake-hack-news-affairs/

Shaw, E., Ruby, K. G., and Post, J. M. (1998). “The Insider Threat to Information Systems” [pdf]. *Security Awareness Bulletin*, Vol. 2, No. 98: pp. 1. Available online at www.pol-psych.com/sab.pdf

Shropshire, J. (2009). “A Canonical Analysis of Intentional Information Security Breaches by Insiders.” *Information Management and Computer Security*, Vol. 17, No. 4: pp. 221-234.

Siponen, M. T. and Oinas-Kukkonen, H. (2007). “A Review of Information Security Issues and Respective Research Contributions.” *The DATABASE for Advances in Information Systems*, Vol. 38, No. 1: pp. 60-80.

Siponen, M., Pahnila, S., and Mahmood, M.A. (2010). “Compliance with Information Security Policies: An Empirical Investigation.” *Computer*, Vol. 43, No. 2: pp. 64-71.

Siponen, M. and Vance, A. (2010). “Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations.” *MIS Quarterly*, Vol. 34, No. 3: pp. 487-512.

Skinner, W. F. and Fream, A. M. (1997). “A Social Learning Theory Analysis of Computer Crime Among College Students.” *Journal of Research on Crime and Delinquency*, Vol. 34, No. 4: pp. 495-518.

Smith, A. L., Baxter, R. J., Boss, S. R., and Hunton, J. E. (2012). “The Dark Side of Online Knowledge Sharing.” *Journal of Information Systems*, Vol. 26, No. 2: pp. 71-91.

Son, J. Y. (2011). “Out of Fear or Desire? Toward a Better Understanding of Employees’ Motivation to Follow IS Security Policies.” *Information & Management*, Vol. 48, No. 7: pp. 296-302.

Spears, J. and Barki, H. (2010). “User Participation in Information Systems Security Risk Management.” *MIS Quarterly*, Vol. 34, No. 3: pp. 503-522.

Stahl, B. C., Doherty, N. F., and Shaw, M. (2012). “Information Security Policies in the U.K. Healthcare Sector: A Critical Evaluation.” *Information Systems Journal*, Vol. 22, No. 1: pp. 77-94.

Stanton, J. M., Stam, K. R., Mastrangelo, P., and Jolton, J. (2005). “Analysis of End User Security Behaviors.” *Computers & Security*, Vol. 24, No. 2: pp. 124-133.

Straub, D. W. (1990). “Effective IS Security: An Empirical Study.” *Information Systems Research*, Vol. 1, No. 3: pp. 255-276.

Straub, D. W. and Nance, W. D. (1990). “Discovering and Disciplining Computer Abuse in Organizations: A Field Study.” *MIS Quarterly*, Vol. 14, No. 1: pp. 45-60.

Straub, D. W. and Welke, R. J. (1998). “Coping with Systems Risk: Security Planning Models for Management Decision Making.” *MIS Quarterly*, Vol. 22, No. 4: pp. 441-469.

Straub, D. W. and Widon, C. S. (1984). “Deviancy by Bits and Bytes: Computer Abusers and Control Measures,” in *Computer Security: A Global Challenge*. J. Finch & E. Dougall (Eds.). Amsterdam: Elsevier Science Publishers B.V, (North-Holland) and IFIP, pp. 431-442.

Thoma, S. J. and Davison, M. L. (1983). “Moral Reasoning Development and Graduate Education.” *Journal of Applied Developmental Psychology*, Vol. 4, No. 3: pp. 227-238.

Tsai, J. Y., Egelman, S., Cranor, L., and Acquisti, A. (2011). “The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study.” *Information Systems Research,* Vol. 22, No. 2: pp. 254–268.

Tsohou, A., Karyda, M., Kokolakis, S., and Kiountouzis, E. (2015). “Managing the Introduction of Information Security Awareness Programmes in Organisations.” *European Journal of Information Systems,* Vol. 24, No. 1: pp. 38-58.

Tyler, R. T. and Blader, S. L. (2005). “Can Businesses Effectively Regulate Employee Conduct? The Antecedents of Rule Following in Work Settings.” *The Academy of Management Journal*, Vol. 48, No. 6: pp. 1143-1158.

Vance, A., Siponen, M., and Pahnila, S. (2012). “Motivating IS Security Compliance: Insights from Habit and Protection Motivation Theory.” *Information & Management,* Vol. 49, No. 3: pp. 190-198.

Vance, A., Anderson, B. B., Kirwan, C. B., and Eargle, D. (2014). “Using Measures of Risk Perception to Predict Information Security Behavior: Insights from Electroencephalography (EEG).” *Journal of the Association for Information Systems*, Vol. 15, No. 10: pp. 679-722.

Vance, A., Lowry, P. B., and Eggett, D. L. (2015). “Increasing Accountability Through User-interface Design Artifacts: A New Approach to Addressing the Problem of Access-Policy Violations.” *MIS Quarterly,* Vol. 39, No. 2: pp. 345-366.

Verizon. (2013). “Data Breach Investigations Report.” *Verizon Enterprise.* Available at http://www.verizonenterprise.com/DBIR/2013/

Warkentin, M., Johnston, A. C., and Shropshire, J. (2011). “The Influence of the Informal Social Learning Environment on Information Privacy Policy Compliance Efficacy and Intention.” *European Journal of Information Systems,* Vol. 20: pp. 267-284.

Warkentin, M. and Willison, R. (2009). “Behavioral and Policy Issues in Information Systems Security: The Insider Threat.” *European Journal of Information Systems*, Vol. 18, No. 2: pp. 101-105.

Whitman, M. (2004). “In Defense of the Realm: Understanding the Threats to Information Security.” *International Journal of Information Management*, Vol. 24: pp. 43-57.

Willison, R. and Backhouse, J. (2006). “Opportunities for Computer Crime: Considering Systems Risk from a Criminological Perspective.” *European Journal of Information Systems,* Vol. 15, No. 4: pp. 403-414.

Willison, R. and Warkentin, M. (2013). “Beyond Deterrence: An Expanded View of Employee Computer Abuse.” *MIS Quarterly*, Vol. 37, No. 1: pp. 1-20.

Workman, M. and Gathegi, J. (2007). “Punishment and Ethics Deterrents: A Study of Insider Security Contravention.” *Journal of the American Society for Information Science and Technology*, Vol. 58, No. 2: pp. 212-222.

Workman, M., Bommer, W. H., and Straub, D. (2008). “Security Lapses and the Omission of Information Security Measures: A Threat Control Model and Empirical Test.” *Computers in Human Behavior*, Vol. 24: pp. 2799-2816.

Young, E. (2014). “Get Ahead of Cybercrime.” Ernst & Young’s 2014 Global Information Security Survey.

Zetter, K. (2015, Aug 28). “Ashley Madison CEO Resigns in Wake of Hack, News of Affair.” Retrieved April 9, 2016, from http://www.wired.com/2015/08/ashley-madisons-business-growing-company-says/

Zviran, M., and Haga, W. J. (1999). “Password Security: An Empirical Study.” *Journal of Management Information Systems*, Vol. 15, No. 4: pp. 161-185.

About the Authors

Puzant Y. Balozian, Ph.D., is an assistant professor of Information Technology. He received his Ph.D. in Information Systems from Baylor University, Waco, Texas, along with a distinguished dissertation award. He also has an M.B.A. with an emphasis in information systems and a B.S. in Information Systems Management from LAU AKSOB. His research, focused primarily on the impacts of organizational factors on individual user behaviors in the context of information security and privacy, addresses security policy compliance/violation and has appeared or been accepted in recognized journals and conferences, including the *Journal of Computer Information Systems*, *International Conference on Information Systems*, and *Americas Conference on Information Systems*. Puzant is an active member in the international body of AIS and the Lebanese AIS. He serves as a reviewer in security and privacy in prominent journals.

Dorothy E. Leidner, Ph.D., is the Ferguson Professor of Information Systems at Baylor University and the Director of the Ph.D. program in Information Systems. She is a visiting professor at the University of Lund, Sweden and during the summers, she serves as a visiting professor at the University of Mannheim in Germany. Dorothy received her B.A., M.B.A., and Ph.D. from the University of Texas at Austin. She has more than 50 refereed publications in such journals as *MIS Quarterly*, *Information Systems Research*, *Organization Science*, *Journal of Management Information Systems*, *Decision Sciences Journal*, *Journal of Strategic Information Systems*, and *MIS Quarterly Executive*, among others. She has received numerous best paper awards, including the *MIS Quarterly* Best Paper Award (1995), the Senior Scholar's Best Publication Award (2007), the *Journal of Strategic Information Systems* Best Paper Honorable Mention Award (2009 and 2010), the *Decision Sciences Journal* Best Article Finalist (2008), the Academy of Management OCIS division best paper award (2000), and a best track paper (1993) and runner-up best track paper (1999) from the HICCS conference. Dorothy has previously served as AE and SE for *MIS Quarterly*. She currently serves as editor-in-chief for *MIS Quarterly Executive* and as SE for *JAIS* and *ISR*.

Appendix A: Partition of Papers Among Insider Types

Authors	Date	Insiders' Cases			
		Purely Malicious	Malicious and Negligent (naïve and opportunistic acts)	Purely Negligent (naïve and opportunistic acts)	Uncategorized
Straub	1990		X		
Straub & Nance	1990		X		
Harrington	1996			X	
Loch & Conger	1996			X	
Skinner & Fream	1997	X			
Banerjee, Cronan & Jones	1998			X	
Straub & Welke	1998		X		
Gattiker & Kelley	1999			X	
Zviran & Haga	1999				
Leonard & Cronan	2001			X	
Kankanhalli et al.	2003		X		
Peace et al.	2003			X	
Lee, Lee & Yoo	2004		X		
Leonard, Cronan & Kreie	2004			X	
Doherty & Fulford	2005				X
Stanton et al.	2005			X	
Alder, Noel & Ambrose	2006			X	
Cronan, Foltz & Jones	2006			X	
Dhillon & Torkzadeh	2006		X		
D'Arcy & Hovav	2007			X	
Kirsch & Boss	2007			X	
Pahnila, Siponen & Mahmood	2007			X	
Workman & Gathegi	2007				X
Workman, Bommer & Straub	2008			X	
Boss S.R., Kirsch, Angermier, Shingler & Boss R.W	2009			X	
D'Arcy, Hovav & Galletta	2009			X	
Herath & Rao	2009a			X	
Herath & Rao	2009b			X	
Myyry,Siponen, Pahnila, Vartiainen & Vance	2009			X	
Ng et al.	2009			X	
Shropshire	2009		X		
Bulgurcu, Cavusoglu & Benbasat	2010			X	
Cannoy & Salam	2010			X	

Authors	Date	Insiders' Cases			
		Purely Malicious	Malicious and Negligent (naïve and opportunistic acts)	Purely Negligent (naïve and opportunistic acts)	Uncategorized
Johnston & Warkentin	2010			X	
Li et al.	2010			X	
Puhaikenen & Siponen	2010			X	
Siponen, Pahnila & Mahmood	2010			X	
Siponen & Vance	2010			X	
Spears & Barki	2010			X	
Guo et al.	2011			X	
Hu, Xu, Dinev & Ling	2011	X			
Son	2011		X		
Warkentin et al.	2011			X	
Chen, Nyemba & Malin	2012	X			
Chen, Ramamurthi & Wen	2012		X		
D'Arcy & Devaraj	2012			X	
Guo & Yan	2012			X	
Hovav & D'Arcy	2012			X	
Hu et al.	2012			X	
Smith et al.	2012			X	
Stahl et al.	2012		X		
Vance et al.	2012			X	
Willison & Warkentin	2013	X			
D'Arcy, Herath & Shoss	2014			X	
Herath, Chen, Wang, Banjara, Wilbur & Rao	2014			X	
Li, Sarathy, Zhang & Luo	2014		X		
Vance, Anderson, Kirwan & Eargle	2014			X	
Boss, Galletta, Lowry, Moody & Polak	2015			X	
Chatterjee, Sarker & Valacich	2015		X		
Hsu, Shih, Hung & Lowry	2015			X	
Hu, West & Smarandescu	2015			X	
Johsnton, Warkentin & Siponen	2015		X		
Lowry & Moody	2015			X	
Lowry, Posey, Bennett & Roberts	2015		X		
Tsohou, Karyda & Evangelos	2015			X	
Vance, Lowry & Eggett	2015		X		
Chen & Zahedi	2016			X	

Appendix B: The Distribution of Papers Across Journals

Journal Name	# of Articles from Sample
Top 25 journals	**87% of surveyed papers**
Communications of the ACM	5
Decision Support Systems	3
Decision Sciences	2
European Journal of Information Systems	5
IEEE Computer Security	1
IEEE Transactions on Dependable and Secure Computing	1
Information and Management	8
Information Systems Journal	6
Information Systems Research	4
Journal of the Association for Information Systems	1
Journal of Management Information Systems	7
Journal of Information Systems	1
MIS Quarterly	14
Other journals and Publications	**13% of surveyed papers**
Computers & Security	1
Computers in Human Behavior	1
Information Management & Computer Security	1
Information Resources Management Journal	1
Hawaii International Conference on System Sciences	1
International Conference on Information Systems	1
International Journal of Information Management	1
Journal of Research in Crime and Delinquency	1
Journal of the American Society for Information Science and Technology	1
TOTAL	**67**