MIS Quarterly

RESEARCH ARTICLE

SEEING THE FOREST *AND* THE TREES: A META-ANALYSIS OF THE ANTECEDENTS TO INFORMATION SECURITY POLICY COMPLIANCE[1]

W. Alec Cram
Bentley University, 175 Forest Street,
Waltham, MA 02452 U.S.A. {wcram@bentley.edu}

John D'Arcy
Department of Accounting and MIS, University of Delaware, 356 Purnell Hall
Newark, DE 19716 U.S.A. {jdarcy@udel.edu}

Jeffrey G. Proudfoot
Bentley University, 175 Forest Street,
Waltham, MA 02452 U.S.A. {jproudfoot@bentley.edu}

A rich stream of research has identified numerous antecedents to employee compliance (and noncompliance) with information security policies. However, the number of competing theoretical perspectives and inconsistencies in the reported findings have hampered efforts to attain a clear understanding of what truly drives this behavior. To address this theoretical stalemate and build toward a consensus on the key antecedents of employees' security policy compliance in different contexts, we conducted a meta-analysis of the relevant literature. Drawing on 95 empirical papers, we classified 401 independent variables into 17 distinct categories and analyzed each category's relationship with security policy compliance, including an analysis for possible domain-specific moderators. A meta-analytic relative weight analysis determined the relative importance of each category in predicting security policy compliance, while adding robustness to our findings. At a broad level, our results suggest that much of the security policy compliance literature is plagued by suboptimal theoretical framing. Our findings can facilitate more refined theory-building efforts in this research domain and serve as a guide for practitioners to manage security policy compliance initiatives.

Keywords: Information security, cybersecurity, information security policies, compliance, meta-analysis, relative weight analysis

Introduction

The effective use of information systems is essential for the long-term success of any organization operating in today's global and digitally driven economy, while securing these systems and their accompanying data continues to be a specific area of paramount importance. One tactic that companies use to protect their systems and data is the creation, deployment, and enforcement of information security policies (hereafter called security policies). At the operational level, security policies are defined as

> a set of formalized procedures, guidelines, roles and responsibilities to which employees are required to

[1]Jason Thatcher was the accepting senior editor for this paper. Anthony Vance served as the associate editor.

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

DOI: 10.25300/MISQ/2019/15117

> adhere to safeguard and use properly the information and technology resources of their organizations (Lowry and Moody 2015, p. 434).

Organizations have put strong reliance on such policies, given the recurring findings that employees account for a large percentage of data breaches and other security incidents (Kaspersky Lab 2017; Ponemon Institute 2016; PwC 2016).

A wealth of research has been conducted on the factors that drive, inhibit, or modify employee compliance with security policies.[2] Research in this realm has drawn from theories of criminology, morality/ethics, psychology, sociology, and others in promoting a variety of antecedents to security policy compliance (see Appendix A, as well as Balozian and Leidner 2017; Cram et al. 2017; Hui et al. 2016; Moody et al. 2018). Collectively, the results have contributed to both the scholarly and practical advancement of information security management, particularly in terms of behavioral compliance issues. At the same time, the number of competing theoretical perspectives and inconsistencies in the reported findings have yielded certain unresolved conflicts.

For example, several models of security policy compliance are built upon the attitude–intention linkage that is integral to the theory of reasoned action (TRA), theory of planned behavior (TPB), and other behavioral theories. Empirical tests of these models support attitude as a strong antecedent of security policy compliance (e.g., Bauer and Bernroider 2017; Bulgurcu et al. 2010; Foth 2016; Ifinedo 2012; Siponen et al. 2014); however, Moody et al. (2018) recently advanced a unified model of security policy compliance, based on an extensive empirical assessment of constructs from several behavioral theories, and attitude was not retained as a construct in their model. Interestingly, the Moody et al. model was also devoid of standalone constructs for social norms and moral considerations, whereas other studies suggest that social and moral influences are key predictors of security policy compliance (e.g., Bulgurcu et al. 2010; Herath and Rao 2009b; Li et al. 2014; Li et al. 2010; Siponen et al. 2014; Yazdanmehr and Wang 2016).

Similar equivocality exists regarding the constructs of deterrence theory (DT). DT provides a foundation for several studies that posit the influences of formal and informal sanctions on security compliance decisions (D'Arcy and Herath 2011). The results of this research have been mixed and at times contradictory. For example, some studies support the influence of formal and/or informal sanctions, while other studies support only certain dimensions of sanction constructs, and still others show that these same constructs are nonsignificant (e.g., Bulgurcu et al. 2010; Foth 2016; Herath and Rao 2009a, 2009b; Johnston et al. 2015; Li et al. 2014; Li et al. 2010; Lowry and Moody 2015).

Yet another example of divergent findings involves the constructs of protection motivation theory (PMT). Adapted from the health domain, PMT has been used to explain employees' willingness to comply with security policies based on their assessments of security threats and their abilities to cope with these threats. Empirical results have generally supported PMT in this context, but there are inconsistencies in terms of the predictive strength of its constructs, whether the full PMT nomology is needed, and whether certain PMT-based relationships hold under different circumstances (e.g., specific versus general security threats; threats directed at employees versus the organization) (e.g., Boss et al. 2015; Herath and Rao 2009b; Ifinedo 2012; Johnston et al. 2015; Siponen et al. 2014; Sommestad et al. 2015).

The preceding examples epitomize a broader state of affairs in the security policy compliance literature: there is a lack of consensus regarding the key drivers of security policy compliance and uncertainty regarding if/how these drivers perform under different conditions. Consistent with the metaphor that one "can't see the forest for the trees," the security policy compliance literature has been preoccupied with finding the best individual predictors of security policy compliance in a piecemeal fashion (as the disparate constructs and theories in Appendix A show), as opposed to a holistic theoretical understanding based on comprehensive themes. This situation is problematic because it hinders theoretical advancement. Indeed, scholars working toward more robust models of security policy compliance face a dilemma in terms of which theoretical frameworks to build upon and which specific constructs to utilize. From a methodological perspective, scholars face difficulties regarding contextual factors that may unknowingly alter the explanatory power of their research models and thus impact their findings.

Against this backdrop, the purpose of the current study is to holistically investigate, via a meta-analytic approach, the findings of prior research on employees' security policy compliance to help further illuminate this problem space and promote theoretical advancement. Our broad objective is to *clarify the relative importance of the antecedents to security policy compliance, as well as the moderators of these relationships*. While methodological factors (e.g., sampling error, measurement error) are plausible explanations for some inconsistent findings within any body of literature, we concentrate on a set of contextual moderators that are particularly germane to the security policy compliance research domain:

[2]We recognize that past studies have examined factors associated with security policy compliance, as well as policy noncompliance, violation, misuse, and abuse. Taken together, we refer to this body of research inclusively as security policy compliance research.

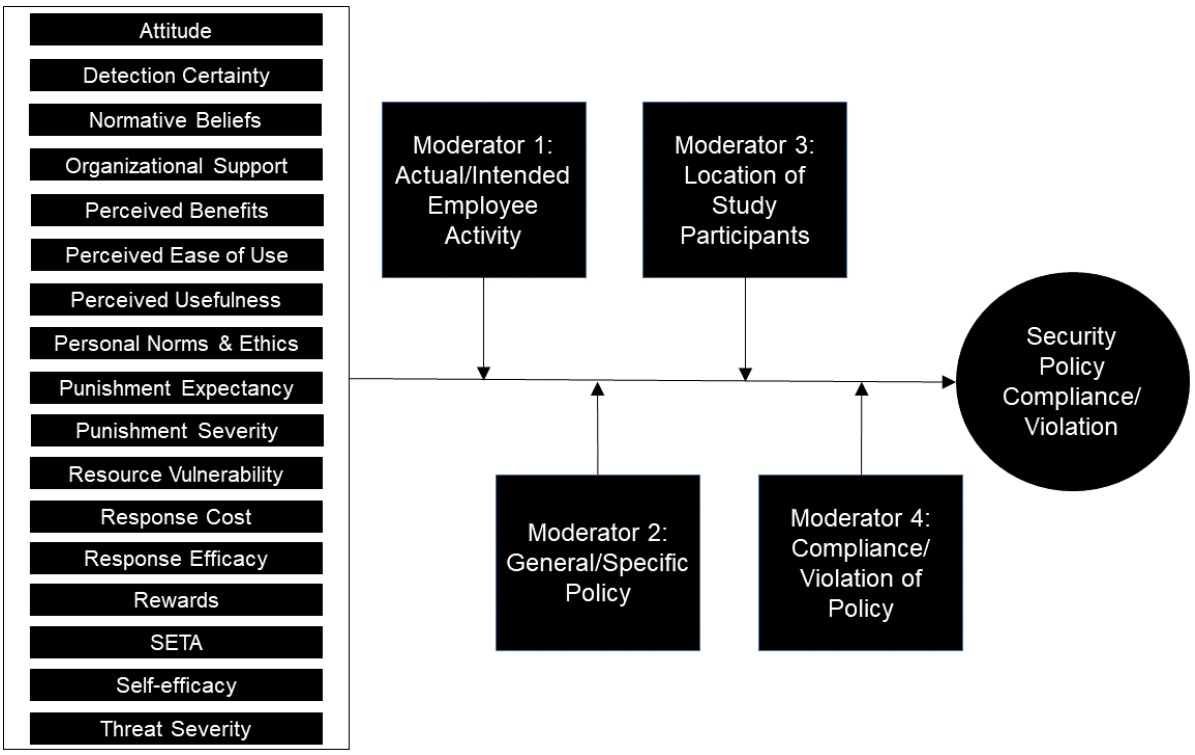

Figure 1. Research Model

the dependent variable focus on security policy compliance versus security policy violation; actual versus intended compliance with security policies; general versus specific security policy; and the national (country) location of the study's respondents. In doing so, we aim to facilitate more refined theorizing that explains security policy compliance in consideration of these contextual differences. Figure 1 depicts our overall research model, which we later elaborate.

While we are not the first to meta-analyze research on employees' security policy compliance (Sommestad and Hallberg 2013; Sommestad et al. 2014; Sommestad et al. 2015), our study diverges from past meta-analyses in important ways. Most notably, we include a much larger and more contemporary body of literature, which lends stronger credibility to our synthesized findings. Our results provide a current perspective on the cumulative work of the field, which can provide clear, novel, and actionable contributions to both research and practice. Most importantly, we help to identify the areas that have yielded consistently strong or weak associations with security policy compliance, as well as those where the results are more varied. Through a relative weight analysis, we are able to demonstrate the *relative* importance of the predictors of security policy compliance; this as compared to prior meta-analyses, which are limited to assessments of each predictor's effect size in isolation (i.e., a single association at a time). Based on our results and analysis, we propose several future paths of study that build on research opportunities in the area of security policy compliance.

The remainder of this paper is organized as follows. First, we present an overview of the security policy compliance literature, along with reasoning for our selected moderator variables. Second, the methodology used to identify relevant literature and conduct our meta-analysis is discussed. Next, the results of this meta-analysis are presented. Finally, we discuss the results, including implications for research and practice, and outline directions for future research.

Overview of Security Policy Compliance Research

Although security policy compliance has garnered increasing scholarly attention in recent years, the topic has a rich history in information systems (IS) security research. Dating back to early works by Straub (1986, 1990), it has been widely recognized that factors such as management support for security activities, clear communication with users on policies, and

noncompliance sanctions can be influential in encouraging employees to behave securely. Roughly 20 years ago, Harrington (1996) investigated the effectiveness of different types of security policies using a vignette-oriented methodology and Parker (1998) proposed that organizations include security accountability as a specific objective in every job description in order to improve security compliance. In a similar vein, Thomson and von Solms (1998) argued that utilizing techniques such as social learning, persuasion, and attribution can improve employee attitudes toward security, which in turn leads to increased compliance behavior. Around the same time, Siponen (2000) promoted behavioral models from social psychology as useful toward understanding the factors that influence employees' intentions to comply with security policies and procedures.

Taking cues from this earlier work, much of the contemporary empirical research on security policy compliance is rooted in theories of human behavior that span the disciplines of criminology, psychology, and sociology (Balozian and Leidner 2017; Cram et al. 2017; Hui et al. 2016; Moody et al. 2018). As described, these studies incorporate constructs from the TRA, TPB, DT, and PMT. Additional studies incorporate elements from rational choice theory (RCT) and theories of moral reasoning and development, along with various individual differences and situational characteristics of the workplace, as antecedents of employees' security policy compliance behavior (see Appendix A).

Inevitably, as this body of work has grown, the empirical results have become scattered, and in some cases contradictory, leading to unanswered questions. Beyond the divergent findings described in the "Introduction," many others abound. For example, some studies (e.g., D'Arcy and Greene 2014; Jenkins et al. 2010; Shropshire et al. 2015) found a negative or very small relationship between forms of organizational support and employee compliance with security policies, while other studies (e.g., Goo et al. 2014; Herath and Rao 2009b) found that a strong relationship exists. Similarly, some publications (e.g., Herath and Rao 2009b; Johnston et al. 2015) found a negative link between perceptions of resource vulnerability and security policy compliance, while others (e.g., Bulgurcu et al. 2010; Ifinedo 2012) found a strong positive link.

What is troubling is that we know little of the relative importance of the various predictors of security policy compliance, as the results differ across studies and research contexts. Finite security budgets push organizations to be selective in undertaking compliance activities, but the uncertain benefits of one activity compared to another creates difficulties for managers in choosing the most effective techniques. Today's managers may need to choose between rewards and punishment or between training and organizational support in seeking to enhance security policy compliance, but no clear answers exist that build on the full body of current research literature. Compounding the challenge for researchers is the variability in the techniques used to study security policy compliance. Our research seeks to address these challenges by clarifying the relative importance of the antecedents to security policy compliance, as well as the moderators of these relationships, through the use of meta-analysis. Before delving into the specifics of our meta-analysis, we first discuss our moderator variables.

Moderators for Security Policy Compliance Studies

Beyond the typical methodological issues that explain varied findings within any body of literature, there are factors specific to the security policy compliance research domain that plausibly explain some of the inconsistencies within this literature. We focus on four such factors as moderators for our meta-analysis (see definitions in Table 1). Each moderator is commonly referenced in the security policy compliance literature, but confusion remains in interpreting their impact.

First, our study considers the differences associated with the nature of the dependent variable. Some past studies measure the extent that employees *comply* with security policies, while other studies focus on the extent that employees *violate* security policies. IS security researchers are divided on whether compliance and violation actually measure the same construct in opposite ways (e.g., Moody et al. 2018) or if, in fact, compliance and violation are different constructs altogether (D'Arcy and Herath 2011; Guo 2013). This latter view is akin to the distinction between trust and distrust in the IS literature (Dimoka 2010).

Arguments for compliance and violation being on opposite ends of a single continuum are based on the limited empirical evidence that supports several of the same antecedents for the two behaviors (Sommestad et al. 2014) and studies that have applied a single theory equally across the two behaviors (e.g., DT as applied to both security policy compliance and violations). However, some IS security scholars have asserted that it may be too simplistic to treat security policy compliance and violations as mere opposites of each other (D'Arcy and Herath 2011; Guo 2013). The rationale for a distinction is that violations are more active, deliberate, and premeditated than compliance, and as such, the antecedents of each type of behavior may be quite different (Guo 2013). Mixing the two behaviors together in a single study, therefore, may lead to inaccurate and unreliable results. Our moderator analysis seeks to uncover potential differences stemming from

Table 1. Moderator Definitions

Moderator	Definition
Nature of the Dependent Variable	
Security Policy Compliance	The extent that an employee fulfills the requirements outlined in a security policy.
Security Policy Violation	The extent that an employee violates the requirements outlined in a security policy or fails to comply with a security policy.
Nature of Policy Compliance	
Actual Policy Compliance	A study's measurement instrument focuses on gauging an employee's actual compliance with a security policy, by posing questions such as "I comply with the information security policy."
Intended Policy Compliance	A study's measurement instrument focuses on gauging an employee's intended compliance with a security policy, by posing questions such as "I plan to comply with the information security policy in the future."
Type of Security Policy	
General Security Policy	Employees are expected to comply with a broad, all-encompassing, generic security policy.
Specific Security Policy	Employees are expected to comply with a specific type of security policy, such as anti-virus software, internet use, backups, and passwords.
Location of Respondents	
Asia-Pacific	Data are collected from respondents located in the Asia-Pacific region (e.g., Australia, China, South Korea).
Europe	Data are collected from respondents located in Europe (e.g., Finland, Germany, Sweden).
North America	Data are collected from respondents located in North America (e.g., U.S.A, Canada).

the study of policy compliance versus policy violation. Achieving clarity on this issue is crucial to behavioral IS security research because it may lead to entirely different theories and constructs being used to study each of the behaviors.

Second, we consider differences stemming from the nature of policy compliance. That is, some studies measure *actual* security policy compliance (e.g., "I currently comply with the policy"), while others focus on *intended* policy compliance (e.g., "I plan to comply with the policy in the future"). While some studies have noted a strong link between the two variables (e.g., Pahnila et al. 2013; Siponen et al. 2014), other studies (e.g., Jenkins and Durcikova 2013; Vance et al. 2014) have raised questions on the accuracy of using the intention to comply as a proxy for actual policy compliance.[3] Our moderator analysis aims to determine if this can help explain differences in security policy compliance effect sizes.

[3]With few exceptions (e.g., Workman et al. 2008), extant security policy compliance studies have measured actual policy compliance using self-reported responses, just as for intended compliance. The use of self-reports is due to both the difficulties of observing useful security policy compliance behaviors in the workplace and organizations' reluctance to provide researchers with access to such information (Crossler et al. 2013; Kotulic and Clark 2004).

Considering the actual versus intended behavior distinction is particularly relevant in the information security context because employees often view security policy requirements as a barrier to productivity (Posey et al. 2014; Puhakainen and Siponen 2010). In this vein, Lowry et al. (2017) asserted the following with respect to security policy compliance:

> it is easy to "intend" positive behavior, but actual compliance can take substantial effort, which can undermine one's work productivity or create other costly nuisances (p. 16).

Hence, in comparison to other more desirable behaviors (e.g., using a new software program that facilitates a work practice), employees may be more likely to divert from their stated intentions when it comes to adhering to security policies. This intention–behavior gap is also plausible because security policies can be complex and difficult to understand, especially for employees with limited technical knowledge (D'Arcy et al. 2014). In such cases, even well-meaning employees who intend to comply with security policies may fail to enact those intentions due to uncertainty regarding specified technical requirements. For example, Puhakainen and Siponen (2010) described a situation wherein some employees failed to comply with a secure email usage policy because they could not decide when the use of email encryption was necessary.

The third moderator concerns differences associated with the type of security policy in place. Some studies evaluate compliance with *general* security policies (i.e., a broad, all-encompassing, generic security policy), while other studies focus on compliance with a *specific* type of security policy (e.g., anti-virus software, internet use, data backups, passwords). There are differing perspectives on this issue. One view is that focusing on compliance with specific policies provides a more accurate assessment of compliance intentions and behaviors. Inherent in this view is that employees interpret the two types of policies differently, and thus researchers should account for differences in employees' willingness to comply with different types of security policies (Siponen and Vance 2014). A second perspective is that evaluating compliance with general security policies is advantageous because it reflects aggregates or trends in employees' security policy compliance (e.g., Bulgurcu et al. 2010; Herath and Rao 2009b; Siponen et al. 2014). This measurement is more generalizable across the gamut of compliance (and violation) opportunities that employees encounter in the workplace. Evaluating compliance with general security policies is similar to how some criminological scholars have utilized general compliance measures to study a range of behaviors, or patterns of deviance, as opposed to a single behavior (Pratt et al. 2006; Silberman 1976). Past research is unclear on the possible role that a general versus specific type of security policy may play in moderating relationships between security policy compliance and its antecedents, and whether certain theories are more or less amenable to the explanation of certain types of security policy compliance. We seek to bring clarity to this issue.

The fourth moderator in our study focuses on the differences associated with the location of the research study's participants. Past studies suggest that aspects of national culture may influence a respondent's perspective on security policy compliance, in terms of the degree of individualism, collectivism, freedom, hierarchy, and control (Hovav and D'Arcy 2012; Kam et al. 2015; Lowry and Moody 2015). For example, Hovav and D'Arcy (2012) found that the deterrent effectiveness of security countermeasures (i.e., security policies, security awareness programs, and computer monitoring) differed based on whether employees were from the United States or South Korea. They also found that certainty of sanctioning was a stronger deterrent to IS misuse intention for South Korean employees, whereas severity of sanctioning was a stronger deterrent for United States employees. Notably, past studies are limited to comparisons of only two countries and therefore the assertion of cross-cultural differences in security policy compliance has yet to be evaluated on a broad scale (Crossler et al. 2013). Based on the available data, we focused our analysis on the Asia-Pacific region, Europe, and North America. In doing so, we afford a more in-depth understanding of potential national culture differences in security policy compliance that encompasses various regions of the world.

Methodology

Meta-analysis is a research technique that quantitatively synthesizes the results of many independent, empirical studies that address similar research questions (Cooper et al. 2009; Glass 1976; Lipsey and Wilson 2001; Schmidt and Hunter 2015). A primary benefit of meta-analysis is that it provides a systematic approach to retrieving, coding, and analyzing research studies using statistical techniques that are more sophisticated than conventional review procedures (Lipsey and Wilson 2001). As such, meta-analysis is viewed as an instrumental tool to accurately and reliably summarize large amounts of research evidence (Templier and Paré 2015). Simply put, meta-analysis

> enables researchers to discover the consistencies in a set of seemingly inconsistent findings and to arrive at conclusions more accurate and credible than those presented in any one of the primary studies (Hunt 1997, p. 1).

Again, we recognize the publication of prior meta-analyses that consider similar issues as this paper (Sommestad and Hallberg 2013; Sommestad et al. 2014; Sommestad et al. 2015). Although these studies uncovered valuable insights, the distinct scope and timing of our study provide an opportunity to make a unique contribution to the field's understanding of security policy compliance. Specifically, 71 of the 95 (75%) studies included in our analysis were published subsequent to those included in Sommestad et al. (2014). As well, Sommestad and Hallberg (2013) and Sommestad et al. (2015) considered only papers related to the TPB (16 studies) and PMT (28 studies), respectively. Our study takes a broader, more holistic approach by considering publications across a range of theoretical bases.

Meta-Analysis Approach

This study follows the meta-analysis approach proposed by Lipsey and Wilson (2001), while also adopting the guidelines detailed within the Preferred Reporting Items for Systematic reviews and Meta-Analyses (PRISMA) (Liberati et al. 2009). In general, three core steps are performed in a meta-analysis: (a) the search for individual studies in the literature; (b) the coding of the identified studies; and (c) the analysis of the accumulated findings (Sabherwal et al. 2006). Each of these steps is explained in more detail below and is illustrated in Figure 2.

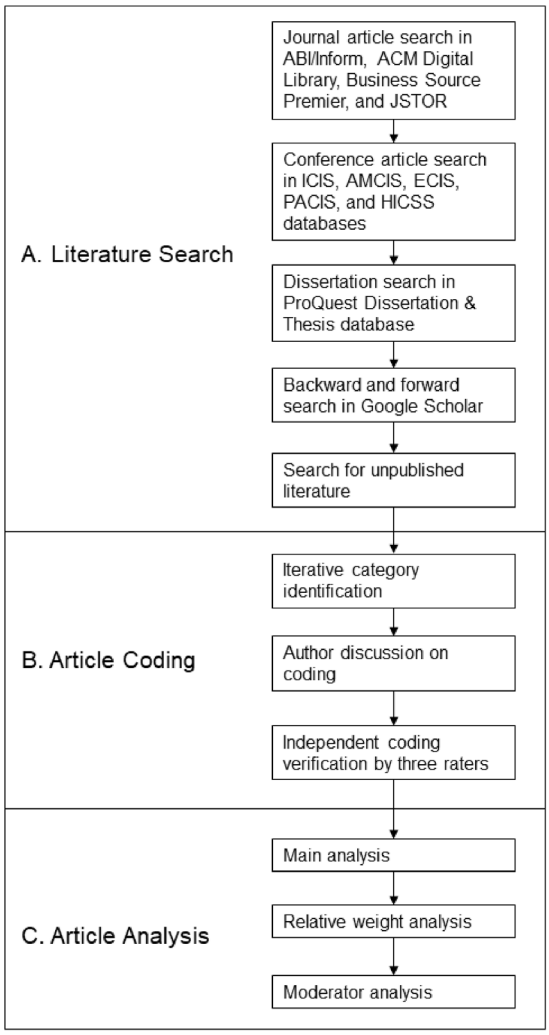

Figure 2. Methodological Activities

Literature Search

A systematic approach to the completion of a meta-analysis relies on a clear protocol and articulation of criteria for article eligibility, in order to demonstrate comprehensiveness and limit the potential for bias (Liberati et al. 2009). The time frame for all literature searches for this study was through January 2018. We began with an examination of the ABI/Inform, ACM Digital Library, Business Source Premier, and JSTOR databases for the journal publications using the terms "security policy," "cybersecurity policy," "information security policy," "security compliance," "security policy violation," "security policy noncompliance," "computer abuse," and "information systems misuse." These databases are frequently cited as key sources of IS literature reviews (Bandara et al. 2015; Schryen 2015). There was no restriction placed on the publication outlet. A total of 1,698 journal articles were identified through this search.

Past research suggests that journal publications are biased toward higher effect sizes and hypothesis-supporting results, but the potential for biased meta-analysis results can be minimized by including conference papers and unpublished studies (Dennis et al. 2001; Rosenthal 1979; Sabherwal et al. 2006; Templier and Paré 2015). To address this concern, we conducted searches for conference papers using the AIS Electronic Library repositories for the International Conference on Information Systems (ICIS), Americas Conference on Infor-

mation Systems (AMCIS), European Conference on Information Systems (ECIS), Pacific Asia Conference on Information Systems (PACIS), and Hawaii International Conference on System Sciences (HICSS). A total of 149 papers were identified through this search. We also searched for unpublished dissertations and theses using the ProQuest Dissertation & Thesis database. A total of 925 manuscripts were identified through this search. Both the conference and dissertation/thesis searches used the same keywords as the journal article search.[4]

Based on the initial set of papers that met our inclusion criteria (see "Inclusion Criteria" section below), we then conducted a backward search within the citations sections, as well as a forward search using Google Scholar to identify articles that subsequently cited the identified publications (Bandara et al. 2015; vom Brocke et al. 2015; Webster and Watson 2002). Where these searches identified papers from conferences other than those listed above, we included them. Notably, the Google Scholar search allowed us to account for papers from lesser-known conferences, thus helping to ensure the thoroughness of our search. This resulted in an additional nine conference papers added to our search results (for a total of 158; see Table 2). We also verified the completeness of our literature search by comparing our identified articles against recent literature reviews by Cram et al. (2017) and Balozian and Leidner (2017).

In order to further minimize the risk of publication bias impacting our results, we contacted members of the International Federation for Information Processing (IFIP) Working Group 8.11/11.13 and the AISWorld Listserv mailing list to request any unpublished manuscripts or working paper results that we could add to our analysis. One additional study was identified for inclusion in our analysis.[5]

[4]We emailed two authors directly for full text electronic copies of their dissertations, because these dissertations were only available as abstracts in the ProQuest Dissertation & Thesis database. Both authors responded and we used both dissertations in our analysis. In other cases where the ProQuest Dissertation & Thesis did not provide a full text copy of a dissertation or thesis, we were able to obtain a journal article that used the same dataset.

[5]The IFIP working group 8.11/11.13 (https://ifip.byu.edu) is comprised of many authors who have published in the area of security policy compliance. We emailed 45 members and received responses from 18. Of these, 16 indicated that they had no additional studies to contribute and two provided a working paper. Of these, one working paper met our inclusion criteria (Li and Luo 2017). However, the working paper was subsequently published as a conference paper and we have listed it as such in Table 2. The AISWorld Listserv mailing list is primarily comprised of IS faculty, doctoral students, and researchers who are members of the Association for Information Systems (Association for Information Systems 2017). In response to our email request, we received 12 responses that contained a total of 14 working papers. One of the received papers met our inclusion criteria (Ormond et al. 2019).

Inclusion Criteria

Articles were included in our scope when they met the following criteria. First, articles needed to be empirical studies at the user/employee unit of analysis that considered security policy issues in an organizational context. Conceptual papers, qualitative studies (e.g., Puhakainen and Siponen 2010), and empirical studies at other levels of analysis (e.g., Spears and Barki 2010; Straub 1990) were excluded. Studies that focused on legal, political, or industry policies, as well as behaviors not specific to organizations (e.g., security-related behaviors at home) were also excluded from our scope. This latter criterion eliminated certain PMT-based studies that considered protective security behaviors in the personal/home usage context (e.g., using anti-spyware on a home computer; Liang and Xue 2010). On this matter, we followed the provisions for security policy compliance literature advocated by Cram et al. (2017) and included only those PMT-based studies of policy-related behaviors in organizational contexts.

As a second criteria, papers were required to examine security policy compliance or violation as a dependent variable. Here, we included studies that used computer abuse and IS misuse as a dependent variable. This inclusive approach is consistent with prior reviews of the security policy compliance literature (Balozian and Leidner 2017; Cram et al. 2017; Siponen and Vance 2014; Sommestad et al. 2014), and is based on the notion that computer abuse and IS misuse behaviors are directly related to a failure of compliance and thus constitute security policy violations (Chu et al. 2015).

Third, eligible papers were required to report data sufficient to calculate an effect size statistic (i.e., sample size, correlation coefficient, and construct reliability) for at least one relationship between an independent variable and either security policy compliance or violation.[6] Notably, this eliminated several conference papers, especially those at the research-in-progress stage, which were captured in our initial searches. We took great care to find later journal articles that tied back to these conference papers and that contained the necessary statistical information. The correlations examined in each paper also needed to be unique and not duplicated across multiple papers that used the same dataset, as doing so can bias the aggregated effects (Wood 2008).

Finally, at least one independent variable within a study had to fit within our coded antecedent categories (see "Article Coding" section). A small number of studies were eliminated based on this criterion (five journal papers, one conference

[6]We identified 14 papers that did not include this information and contacted the authors of each paper to request the missing data. We received responses from five authors, but no additional data were provided.

Table 2. Paper Collection Results

	Journals	Conferences	Dissertations/ Theses	Unpublished Papers
Papers identified in searches	1698	158	925	15
Papers excluded due to scope criteria	1637	134	916	14
Total Included Papers	**61**	**24**	**9**	**1**

paper, and one dissertation), which indicates that the independent variables in these studies were not commonly used in the security policy compliance literature.

Table 2 provides a summary of the entire paper collection results and Appendix B provides a sample listing of excluded papers and the accompanying rationale.

A total of 95 papers met our inclusion criteria: 61 journal papers, 24 conference papers, 9 dissertations/theses, and 1 unpublished manuscript. Refer to Appendix A for details on the included papers. The quantity of in-scope studies is favorable when compared to several past meta-analyses in IS journals, including Wu and Lederer (2009) with 71 studies, Kohli and Devaraj (2003) with 66 studies, Dennis et al. (2001) with 61 studies, Hwang (2014) with 30 studies, Sharma and Yetton (2003) with 22 studies, and Lee and Xia (2006) with 21 studies.

Article Coding

Due to the wide range of theoretical foundations employed in the security policy compliance literature, a variety of independent variables were examined within the corpus of articles included in this analysis. In order to identify common groupings of variables where a meta-analysis could be performed, we first identified each of the independent variables examined across the 95 papers. Because several papers (noted in Appendix A) report on data from multiple studies or analyze distinct samples, a total of 114 independent datasets were included in our scope. We began by iteratively placing the independent variables in categories where a common theme existed. This was relatively straightforward in cases where common measurement instruments were used for the variables, such as with attitude or self-efficacy; however, other variables used different terminology for similar variables. For example, perceived threat severity and severity of breach were coded into the threat severity category. Similarly, perceived behavioral control was coded into the self-efficacy category because the two variables essentially measure the same latent construct (Ajzen 1991; Bulgurcu et al. 2010).

Where uncertainty existed in the categories, the authors discussed the variables and re-reviewed the instrument wording used in the studies to clarify if an independent variable could be grouped with other, similar variables or if a new category should be created (e.g., an initial category on punishment was revised into two categories named punishment expectancy and punishment severity). Where two independent variables were identified within a paper that could be grouped into a single category (e.g., general information security policy awareness and information security awareness), both variables were included and an average correlation was calculated for use in the analysis. Using the average correlation follows standard practice so as to avoid double-counting the relationship within a study (thus avoiding artificial inflation of the meta-analysis result) (Lipsey and Wilson 2001; O'Boyle et al. 2011; Schmidt and Hunter 2015). Theory also played a role in creating the categories. For example, creating distinct categories for punishment expectancy and punishment severity aligns with the tenets of DT, a prominent theory in the security policy compliance literature. Similarly, the creation of attitude, normative beliefs, and self-efficacy categories aligns with the TPB, another prominent theory in this research space.

In total, 401 independent variables were placed into 17 distinct categories (refer to Figure 1, as well as Appendix C for corresponding definitions). For each category, an average of 24 studies were included.[7] The resulting model is illustrated in Figure 1, where each box on the left represents one of the independent variable categories that are associated with the security policy compliance or violation dependent variable. Where an independent variable was not placed in a category, it was a consequence of too few other studies examining the same variable. In order to verify the reliability of our categor-

[7]A range of opinions exist as to the minimum quantity of papers that are sufficient to conduct a meta-analysis. Some perspectives, such as Valentine et al. (2010), suggest that two studies are adequate, while others (e.g., Doi et al. 2015; Sterne et al. 2000; Sutton 2006; Sutton et al. 2000) argue that five or more studies can serve to increase the power of the resulting analysis and decrease the likelihood of bias. We set our minimum level of studies per antecedent category at five. Notably, several of the results in the earlier meta-analyses of security policy compliance studies by Sommestad and his colleagues were based on only one or two papers.

ization of the independent variables included in our analysis, we followed the technique adopted by Gerow et al. (2014), whereby we asked three independent raters (a doctoral student and two faculty members) to match the independent variables from 10 different, randomly selected publications within our pool of in-scope articles (i.e., a total of 30 different articles) to one of the 17 antecedent categories. Cohen's Kappa (Cohen 1960) was calculated across the three raters as 1.00, 0.89, and 0.92 (average 0.94), which represents an "almost perfect" strength of agreement, according to Landis and Koch (1977).

Article Analysis

A separate meta-analysis was performed for each of the 17 independent variable categories depicted in Figure 1. Following the guidelines set by Lipsey and Wilson (2001), we took the reported correlation (r) for each individual study and calculated a weighted mean effect size by correcting the results for unreliability, transforming them into standard scores, and assigning weights based on the sample sizes used. All references to "effect size" hereafter relate to this weighted mean effect size. We augmented this main analysis with a meta-analytic relative weight analysis, using techniques developed by Johnson and his colleagues (e.g., Johnson 2000; Johnson and LeBreton 2004; Tonidandel and LeBreton 2011), to determine which of the independent variable categories was most strongly predictive of security policy compliance. We elaborate on these analyses later in the paper.

For papers where policy compliance was examined as the dependent variable, we used the correlation values reported in the study. However, for those papers where policy violation was studied as the dependent variable, we used the inverse of the reported correlation value in our analysis (e.g., if the correlation between detection certainty and violation intention was found to be -0.25, we coded the study as 0.25 to represent the relationship with compliance intention).

In order to evaluate the validity and reliability of the main meta-analysis results, we conducted tests for the significance (z-test) and homogeneity (Q-test) of each antecedent category, and calculated the credibility values, confidence intervals, percentage of variance attributable to sampling error, and Failsafe-N for each category. Details of these tests are outlined in the following section. We also analyzed the data for our four moderators as a means to help explain why inconsistent relationships may exist across different studies within a particular category (Schmidt and Hunter 2015). Appendix D provides details on the moderator characteristics for each paper included in the meta-analysis.

Meta-Analytic Results

The overall effect size and effect size magnitude for each of the 17 meta-analyses that comprised our main analysis are summarized in Table 3.

The effect sizes reported above are in a standardized form and represent the "average magnitude of the indexed relationship for specific categories of studies" (Lipsey and Wilson 2001, p. 146). As a result, these standardized effect sizes are distinct from the correlations from which they originate and therefore they should not be interpreted exactly as such (Cohen 1988; Lipsey and Wilson 2001). To be more specific, based on the aforementioned adjustments to the raw correlations (i.e., correcting for unreliability, transforming to standard scores, weighting by sample size), the effect sizes reported in this meta-analysis are generally larger (i.e., between .10 and .25 larger) than a simple mean of correlations across the individual studies (Lipsey and Wilson 2001; Schmidt and Hunter 2015).

To interpret the magnitude of effect sizes, we follow the quartile benchmarks set by Lipsey and Wilson (2001): "small" effect sizes are less than .30, "medium" are between .30 and .50, "large" are between .50 and .67, and "very large" are greater than .67. Our analysis revealed a range of overall effect sizes from 0.090 to 0.651. Our results indicated 2 in the small category, 10 in the medium category, and 5 in the large category. Specifically, three of the five categories with a large effect size (personal norms & ethics, attitude, normative beliefs) relate to employee attitudes, beliefs, and ethical characteristics, whereas several categories with lower effect sizes relate to punishment, threats, and rewards (punishment expectancy, punishment severity, resource vulnerability, rewards). In what could be considered the medium-to-large effect size range are factors that pertain to employee confidence related to security (self-efficacy, response efficacy) and management support in this domain (organizational support, SETA). We provide a fuller discussion of these results later.

In terms of validity, a z-test was conducted to evaluate the significance of each category's effect size. At $p < .001$, all of the categories were found to have a statistically significant relationship with security policy compliance, as the calculated z-test value is greater than the critical-z (3.29).[8] A test for

[8]The interpretation of p-values in meta-analysis is complex and thus can be easily misinterpreted. For example, a significant p-value may reflect a large effect size for a particular category, or a small effect size that is based on a large sample size. Hence, methodologists recommend focusing more on effect sizes for evaluating the independent variable categories in a meta-analysis (Borenstein et al. 2009; Schmidt and Hunter 2015).

Table 3. Meta-Analysis Results

Category	Overall Effect Size (Stand.)	Effect Size Magnitude[a]	Number of Studies[b]	Total Sample Size	Calculated z-test	Calculated-Q	Critical-Q	80% CV[c]	95% CI[d]	PVA[e]	Failsafe-N
Perceived Usefulness	0.651	Large	7	1,955	23.594	55.02	12.59	0.47, 0.83	0.60, 0.70	16.93%	232
Personal Norms & Ethics	0.579	Large	20	4,970	36.030	370.20	30.14	0.34, 0.82	0.55, 0.61	8.53%	537
Attitude	0.564	Large	37	10,975	52.877	768.49	51.00	0.27, 0.85	0.54, 0.59	5.81%	1163
Normative Beliefs	0.531	Large	43	12,416	53.005	702.82	58.12	0.25, 0.81	0.51, 0.55	7.67%	1163
Organizational Support	0.518	Large	12	2,749	24.060	71.42	19.68	0.29, 0.75	0.48, 0.56	16.71%	236
Self-efficacy	0.447	Medium	57	14,014	46.986	776.95	74.47	0.13, 0.76	0.43, 0.47	9.01%	891
Response Efficacy	0.442	Medium	24	6,019	29.855	379.02	35.17	0.17, 0.71	0.41, 0.47	12.86%	359
Perceived Benefits	0.432	Medium	11	2,274	18.534	425.84	18.31	-0.09, 0.95	0.39, 0.48	3.17%	136
SETA	0.418	Medium	30	8,398	34.569	372.91	42.56	0.17, 0.66	0.39, 0.44	9.75%	483
Detection Certainty	0.416	Medium	20	6,520	29.826	220.31	30.14	0.20, 0.64	0.39, 0.44	11.57%	362
Perceived Ease of Use	0.381	Medium	7	1,788	12.317	37.12	12.59	0.12, 0.64	0.32, 0.44	21.11%	58
Response Cost	-0.345	Medium	25	5,271	-22.100	489.36	36.42	-0.77, 0.08	-0.38, -0.31	9.23%	185
Threat Severity	0.342	Medium	22	5,700	22.060	129.47	32.67	0.11, 0.58	0.31, 0.37	19.01%	187
Punishment Severity	0.323	Medium	27	8,010	26.932	259.49	38.89	0.11, 0.54	0.30, 0.35	11.46%	284
Punishment Expectancy	0.317	Medium	29	7,979	25.899	289.54	41.34	0.10, 0.53	0.29, 0.34	14.28%	259
Resource Vulnerability	0.218	Small	20	6,061	14.819	281.54	30.14	-0.05, 0.48	0.19, 0.25	8.80%	74
Rewards	0.090	Small	10	4,612	5.401	172.62	16.92	-0.23, 0.41	0.06, 0.12	5.37%	3

[a]Lipsey and Wilson (2001) establish the magnitude of effect sizes at ≤ .30 (small), between .30 and .50 (medium), between .50 and .67 (large), and ≥ .67 (very large).
[b]The total number of studies across all categories is 401. Details on each of the individual papers as well as the associated categories examined are listed in Appendix A.
[c]CV refers to the calculated Credibility Value. See details below.
[d]CI refers to the calculated Confidence Interval. See details below.
[e]PVA refers to the percent of variance in observed correlations attributable to sampling error and other artifacts (Schmidt and Hunter 2015; Schmidt and Le 2014).

homogeneity (Q-test) was also conducted for each of the 17 meta-analysis categories in order to determine the possibility of moderating effects. Table 3 also lists the critical value for the chi-square distribution, where the degrees of freedom equal the number of effect sizes minus one. The calculated-Q is greater than the critical-Q value in all of the 17 categories. As a result, the null hypothesis of homogeneity is rejected and the variability across effect sizes exceeds what is expected based on sampling error (Lipsey and Wilson 2001).

Credibility values (80%) and confidence intervals (95%) were also calculated and are noted in Table 3. Credibility values provide further insight into whether moderators are operating, by indicating the distribution of values, while the confidence interval assesses the accuracy (i.e., the extent of sampling error) of the mean effect size estimate (Schmidt and Hunter 2015; Whitener 1990). Past research suggests that where a credibility value is

> sufficiently large or does include zero, then the mean corrected effect size is probably the mean of several subpopulations identified by the operation of moderators; if the interval is small or does not include zero, then the mean corrected size is probably the

> estimate of one population parameter, and moderators are not in operation (Whitener 1990, p. 317).

In comparison, a 95% confidence interval indicates that the average mean true score is within the calculated interval, with 95% confidence (Jiang et al. 2012).

For each category, the Failsafe-N ratio was also calculated. The results specify the number of studies with nonsignificant results that would be required to nullify an identified significant result (Rosenthal 1979). This metric is commonly used to put into context the level of risk associated with the "file-drawer problem," whereby the identification of unpublished studies with nonsignificant results would impact the accuracy of the meta-analysis findings (McDaniel et al. 2006). Where the resulting number is large relative to the studies examined, it provides additional confidence in the conclusions (Rosenberg 2005). A variety of techniques can be used to calculate the Failsafe-N, typically by drawing on either the calculated z-scores or effect sizes (Long 2001). We adopted Rosenthal's (1979) approach, with a p-critical value set at .01, as it is the original and most commonly used technique (Long 2001; Rosenberg 2005). The results are listed in Table 3. We note that a low Failsafe-N value exists for rewards, which suggests that additional studies of this category are warranted to establish the validity of our effect size estimate.

Publication bias refers to the potential for meta-analysis results to be biased due to the assumption that the effect sizes within published studies are representative of all existing studies (McDaniel et al. 2006; Rothstein et al. 2005; Schmidt and Hunter 2015). As our study included only one unpublished manuscript, we drew on the arguments of Dickersin (2005), Hopewell et al. (2005), and Kepes et al. (2012), who note the potential for publication bias between published literature (e.g., journals, book chapters) and grey literature (e.g., increasingly inaccessible literature such as conference papers and dissertations). To address this concern, we compared the mean effect sizes of published journal papers with those from conferences and dissertations/theses. In the 13 categories where we had sufficient data to conduct the analysis (i.e., five or more published studies and five or more grey literature studies), we found five categories where the effect sizes were significantly different at a $p < .05$ significance level. Refer to Table 4 for details. In one of these categories (attitude), the published studies were found to have a larger effect size, but in the other four categories (personal norms & ethics, punishment severity, resource vulnerability, response cost), the published study effect sizes were smaller, which is in contrast to the typical concern related to publication bias (Dickersin 2005; Schmidt and Hunter 2015).

In order to further investigate the potential for publication bias, we also calculated the Failsafe-N within each category for both published papers and grey literature. Past meta-analyses within the IS literature (e.g., Gerow et al. 2014; Sabherwal et al. 2006) have divided Failsafe-N by the quantity of studies and where this number is less than two, it indicates that publication bias is a potential problem. We completed this calculation for each of the 13 categories where we had sufficient data and no category was below two. Refer to Table 4 for details. Overall, this suggests that publication bias is not a pervasive problem within our study, but care should be taken in interpreting the results for categories where only a small number of publications were identified.

The Issue of Common Method Variance

A potential validity threat to the empirical findings in the security policy compliance literature, and therefore to our meta-analysis results, is the influence of common method variance (CMV). CMV is "variance that is attributable to the measurement method rather than to the constructs the measures represent" (Podsakoff et al. 2003; p. 879) and is typically thought to artificially inflate relationships among study variables (Sharma et al. 2009). CMV is a concern when all study data is collected at the same time from the same participants, using a single method (e.g., a self-report, single respondent "snapshot" survey design) (Podsakoff et al. 2003). Such was the case for the majority of studies in our meta-analysis, as 90 of the 95 studies employed a cross-sectional survey design using a single respondent and self-report measures (in some cases, a survey was used in combination with an experimental manipulation). Further, nearly all of these studies used similar measurement types (e.g., Likert-type scales) for both the independent and dependent variables, which heightens CMV concerns (Sharma et al. 2009).

Although some authors maintain that CMV is not substantial in IS research (e.g., Malhotra et al. 2006), evidence supports the possibility that CMV is a serious issue in major IS research domains, such as the technology acceptance model literature (Sharma et al. 2009) and the literature on information technology–business alignment (Gerow et al. 2014). In meta-analyses of these literature streams, the authors reported higher effect sizes for relationships measured using a common self-reporting method compared to those measured using independent sources of data (e.g., a combination of survey responses and computer system logs; survey responses from multiple respondents). Likewise, because almost all security policy compliance studies do not separate the measurement of antecedents and security policy compliance either by time,

Table 4. Results of Publication Bias Analysis

Category	Moderator Group	Weighted Effect Size	|Observed Difference|	Number of Studies	Total Sample Size	Calculated z-test value	80% CV[a]	95% CI[b]	PVA[c]	Failsafe-N
Attitude	Published	0.647	0.202	23	6,845	3.047*	0.37, 0.92	0.62, 0.67	6.12%	908
	Grey Literature	0.445		14	4,130		0.15, 0.74	0.41, 0.48	7.11%	292
Detection Certainty	Published	0.427	0.033	12	4,467	0.341	0.19, 0.66	0.39, 0.46	10.10%	258
	Grey Literature	0.394		8	2,053		0.19, 0.60	0.35, 0.44	15.08%	104
Normative Beliefs	Published	0.573	0.125	29	8,350	1.721	0.30, 0.84	0.55, 0.60	7.48%	904
	Grey Literature	0.448		14	4,066		0.15, 0.74	0.41, 0.48	9.30%	274
Organizational Support	Published	0.563	0.143	6	1,863	1.677	0.41, 0.72	0.51, 0.61	23.73%	191
	Grey Literature	0.420		5	759		0.10, 0.74	0.34, 0.50	14.47%	42
Personal Norms & Ethics	Published	0.494	0.258	15	3,522	-4.591*	0.31, 0.68	0.46, 0.53	24.50%	258
	Grey Literature	0.752		5	1,448		0.40, 1.00	0.70, 0.81	2.57%	303
Punishment Expectancy	Published	0.334	0.057	17	5,693	0.638	0.07, 0.60	0.31, 0.36	9.19%	210
	Grey Literature	0.277		12	2,286		0.16, 0.39	0.23, 0.32	67.96%	51
Punishment Severity	Published	0.263	0.173	18	5,315	-2.190*	0.03, 0.50	0.23, 0.29	12.55%	117
	Grey Literature	0.436		9	2,695		0.30, 0.57	0.40, 0.48	20.00%	188
Resource Vulnerability	Published	0.174	0.197	14	4,733	-2.144*	-0.09, 0.44	0.14, 0.21	10.60%	33
	Grey Literature	0.371		6	1,328		0.08, 0.66	0.31, 0.43	7.53%	54
Response Cost	Published	-0.264	0.372	16	4,419	3.755*	-0.63, 0.10	-0.30, -0.23	12.45%	90
	Grey Literature	-0.636		10	1,164		-1.00, -0.21	-0.70, -0.57	7.61%	136
Response Efficacy	Published	0.415	0.133	15	4,601	-1.581	0.18, 0.65	0.38, 0.45	12.67%	253
	Grey Literature	0.548		9	1,418		0.23, 0.87	0.48, 0.61	13.63%	111
Self-efficacy	Published	0.488	0.144	32	9,012	1.581	0.25, 0.72	0.47, 0.51	11.51%	708
	Grey Literature	0.344		28	5,918		0.00, 0.68	0.31, 0.37	9.20%	208
SETA	Published	0.491	0.159	16	4,524	1.934	0.23, 0.75	0.46, 0.52	9.22%	366
	Grey Literature	0.332		14	3,874		0.11, 0.55	0.30, 0.37	13.40%	135
Threat Severity	Published	0.315	0.099	12	4,110	-1.065	0.11, 0.52	0.28, 0.35	17.30%	118
	Grey Literature	0.414		10	1,590		0.14, 0.68	0.36, 0.47	24.18%	72

*Denotes z-test values that are significant at $p < .05$.
[a]CV refers to the calculated Credibility Value.
[b]CI refers to the calculated Confidence Interval.
[c]PVA refers to the percent of variance in observed correlations attributable to sampling error and other artifacts (Schmidt and Hunter 2015; Schmidt and Le 2014).

different methods, or different instruments, we cannot ignore the possibility of CMV within our results. Consequently, all effect sizes reported in this paper are subject to the CMV threat.

A number of meta-analytic studies published in top IS journals also suffer from CMV concerns; namely, those that meta-analyze literature where the bulk of studies rely on self-report surveys obtained from a single respondent at a single point in time (e.g., Gerow et al. 2013; Joseph et al. 2007; He and King 2008; Sabherwal et al. 2006; Wu and Du 2012; Wu and Lederer 2009; Wu and Lu 2013). Moving forward, the ideal way to address CMV is to control for it at the research design stage (a point we revisit in the "Limitations" section). This approach is in contrast with the more common tactic used by IS scholars of attempting to gauge the magnitude of CMV (and typically arguing it away) through *post hoc* statistical tests. Notably, several of these tests have been contested on their ability to accurately control and/or detect CMV. The popular Harman's one factor test, for example, is considered an insensitive test of CMV and is no longer recommended to deal with the problem (Chin et al. 2012; Podsakoff et al. 2003). More sophisticated statistical tests for CMV, such as the latent common method factor test and the marker variable test, also have known limitations (Chin et al. 2012; Richardson et al. 2009; Sharma et al. 2009). The point here is that the available selection of *post hoc* statistical tests cannot definitively rule out, nor control for, CMV.

With this caveat in mind, we attempted to address the potential CMV bias in our results, to the extent possible, based on the available data from the primary studies. Of the 90 studies in our meta-analysis that employed cross-sectional, single source survey designs, 51 addressed CMV through a combination of procedural (e.g., randomizing items on the survey instrument, using different scale anchors) and statistical remedies (e.g., Harman's one factor test, latent common method factor test, marker variable test), whereas 39 studies did not mention any techniques taken to address CMV. Hence, to assess whether CMV was a biasing factor in our

Table 5. Results of Common Method Variance Analysis

Category	Moderator Group	Weighted Effect Size	|Observed Difference|	Number of Studies	Total Sample Size	Calculated z-test value	80% CV[a]	95% CI[b]	PVA[c]	Fail-safe-N
Attitude	Accounts for CMV	0.652	0.152	22	6,307	2.513*	0.37, 0.94	0.62, 0.68	5.50%	902
	No CMV	0.500		11	3,872		0.29, 0.71	0.46, 0.54	8.67%	309
Detection Certainty	Accounts for CMV	0.367	0.134	9	4,107	-1.513	0.20, 0.54	0.33, 0.40	16.29%	176
	No CMV	0.501		10	2,286		0.25, 0.75	0.46, 0.55	8.88%	189
Normative Beliefs	Accounts for CMV	0.603	0.125	25	7,082	1.825	0.39, 0.82	0.58, 0.63	100%	857
	No CMV	0.478		15	4,646		0.16, 0.80	0.45, 0.51	6.75%	351
Personal Norms & Ethics	Accounts for CMV	0.500	0.138	9	2,093	-2.046*	0.29, 0.71	0.45, 0.55	20.08%	169
	No CMV	0.638		11	2,877		0.36, 0.91	0.60, 0.68	5.82%	376
Punishment Expectancy	Accounts for CMV	0.297	0.103	23	6,516	-1.232	0.09, 0.50	0.27, 0.32	17.47%	180
	No CMV	0.400		6	1,463		0.13, 0.67	0.35, 0.45	8.81%	84
Punishment Severity	Accounts for CMV	0.303	0.058	16	5,236	-0.724	0.07, 0.53	0.27, 0.33	9.55%	163
	No CMV	0.361		11	2,774		0.16, 0.56	0.32, 0.40	17.91%	124
Resource Vulnerability	Accounts for CMV	0.184	0.088	10	3,200	-1.006	-0.12, 0.49	0.14, 0.22	8.15%	27
	No CMV	0.272		8	2,430		0.03, 0.52	0.23, 0.32	8.40%	48
Response Cost	Accounts for CMV	-0.431	0.237	12	2,968	-2.115*	-0.82, -0.05	-0.47, -0.39	8.53%	175
	No CMV	-0.194		10	1,764		-0.57, 0.19	-0.25, -0.14	11.40%	11
Response Efficacy	Accounts for CMV	0.419	0.091	15	3,939	-1.119	0.14, 0.70	0.38, 0.45	12.62%	214
	No CMV	0.510		7	1,659		0.23, 0.79	0.45, 0.57	11.37%	122
Self-efficacy	Accounts for CMV	0.453	0.028	30	7,258	-0.326	0.15, 0.76	0.43, 0.48	9.43%	477
	No CMV	0.481		21	5,529		0.15, 0.81	0.45, 0.51	7.83%	401
SETA	Accounts for CMV	0.457	0.070	15	4,557	0.858	0.18, 0.74	0.43, 0.49	8.86%	325
	No CMV	0.387		14	3,647		0.19, 0.58	0.35, 0.42	12.05%	170
Threat Severity	Accounts for CMV	0.351	0.020	13	3,283	-0.231	0.06, 0.64	0.31, 0.39	13.60%	123
	No CMV	0.371		7	1,986		0.25, 0.50	0.31, 0.43	58.69%	65

* Denotes z-test values that are significant at $p < .05$.
[a]CV refers to the calculated Credibility Value.
[b]CI refers to the calculated Confidence Interval.
[c]PVA refers to the percent of variance in observed correlations attributable to sampling error and other artifacts (Schmidt and Hunter 2015; Schmidt and Le 2014).

meta-analysis results, we compared the effect sizes of those studies that addressed CMV to those studies that did not. These results are presented in Table 5. Of the 12 categories that had sufficient data (i.e., 5 or more studies that accounted for CMV and 5 or more studies that did not), we identified only 3 categories (personal norms & ethics, attitude, response cost) where the effect sizes were significantly different at $p < .05$ significance level. None of the 12 categories were found to have significant differences at a $p < .01$ level.

We also analyzed the data to determine if those studies that used more sophisticated statistical CMV techniques, namely the marker variable test, were found to have effect sizes that differed from studies that undertook more rudimentary CMV remedies (e.g., instrument randomization, Harman's one factor test). Of the studies included in our analysis, only nine used the marker variable test. As a result, only one category (normative beliefs) had sufficient data to compare effect sizes for this test. We found that there was no significant difference (at $p < .05$) in the effect size for studies that used the marker variable test compared to studies that did not use the marker variable test, but accounted for CMV in other ways.

To summarize, CMV is a serious concern in the security policy compliance literature due to the reliance on cross-sectional, single source survey designs. Although our comparisons of effect sizes did not show evidence of a strong CMV bias, we cannot definitively rule out CMV in our results, nor can we estimate its potential magnitude. We call on IS scholars to do better in reducing CMV in their study designs, rather than testing for it using *post hoc* statistical procedures. This way, future meta-analyses of the security policy compliance literature and other IS research domains will be in a better position to determine the influence of CMV.

Relative Weight Analysis

Shifting focus back to the main meta-analysis results in Table 3, they provide an indication of each category's relationship with security policy compliance. However, that analysis only accounts for the contribution of a particular category by itself, thus failing to satisfy the statistical definition of *relative* importance (Johnson and LeBreton 2004). To truly assess the

Table 6. Meta-Analytic Correlation Matrix Used for Relative Weight Analysis

Category	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1. Security Policy Compliance	—													
2. Attitude	.50 (37)	—												
3. Detection Certainty	.38 (20)	.43 (1)	—											
4. Normative Beliefs	.47 (43)	.40 (26)	.43 (5)	—										
5. Personal Norms & Ethics	.50 (20)	.28 (2)	.41 (2)	.34 (4)	—									
6. Punishment Expectancy	.30 (29)	.24 (8)	.61 (5)	.40 (8)	.39 (6)	—								
7. Punishment Severity	.31 (27)	.15 (5)	.49 (11)	.28 (6)	.43 (7)	.59 (19)	—							
8. Resource Vulnerability	.20 (20)	.31 (7)	.51 (2)	.26 (8)	.06 (1)	.22 (5)	.18 (4)	—						
9. Response Cost	-.31 (25)	-.22 (5)	-.22 (3)	-.08 (6)	-.03 (1)	-.10 (6)	-.08 (1)	-.07 (8)	—					
10. Response Efficacy	.40 (24)	.42 (5)	.13 (1)	.27 (5)	.26[a]	.18 (7)	.08 (3)	.15 (14)	-.28 (12)	—				
11. Rewards	.08 (10)	.26 (3)	.28 (1)	.14 (3)	.26[a]	.15 (4)	.12 (2)	.06 (6)	.44 (4)	-.04 (5)	—			
12. SETA	.39 (30)	.38 (10)	.56 (3)	.39 (9)	.27 (2)	.38 (5)	.38 (5)	.36 (1)	.00 (6)	.48 (3)	.18 (3)	—		
13. Self-Efficacy	.40 (57)	.36 (24)	.05 (6)	.37 (23)	.34 (1)	.06 (13)	.01 (8)	.12 (16)	-.28 (16)	.45 (19)	.01 (8)	.38 (15)	—	
14. Threat Severity	.33 (22)	.33 (5)	.26[a]	.28 (5)	.26[a]	.40 (8)	.02 (2)	.40 (16)	-.18 (12)	.38 (20)	-.01 (6)	.22 (1)	.23 (18)	—

Notes: In parentheses is the number of studies/independent samples in which the relationship was tested.
[a]Average effect size across all non-missing cells. As a technique to verify the accuracy of the effect sizes calculated using the Lipsey and Wilson (2001) approach in the main analysis, the correlations shown above were calculated using the Schmidt and Hunter (2015) approach. Only minor differences exist for the relationships between each of the categories and security policy compliance (column 1 in Table 6) in comparison to the effect size results reported in Table 3, which can be attributed to differences in terms of statistical artifact adjustments and the use of Fisher's z-transformation (Geganfurtner 2011; Hedges and Pigott 2001; Lipsey and Wilson, 2001; Schultze 2007). The overall consistency of the effect size estimates across the two approaches supports the robustness of our findings.

relative importance (i.e., relative contribution) of each category in predicting security policy compliance, in line with our overall research objective, a supplementary analysis is required in which the intercorrelations among the categories are taken into account. Accounting for such intercorrelations is warranted for the security policy compliance literature, because as with other organizational research streams (O'Boyle et al. 2011), there are substantive correlations among the variables that comprise our categories (see Table 6). Relative weight analysis is suited for this situation as it generates an estimate of the unique variance explained by each predictor after correcting for correlations among predictors (Johnson 2000). To compute the relative importance of each of our antecedent categories, we used Tonidandel and LeBreton's (2015) RWA-Web program.

The input to the RWA-Web program was a meta-analytic correlation matrix that we built by conducting separate meta-analyses for the relationships between all 17 categories and the security policy compliance criterion variables. The initial correlation matrix, shown in Appendix E, was the culmination of nearly 130 individual meta-analyses. In conducting these meta-analyses, we corrected for unreliability and sampling error. Again, for studies in which a particular category appeared more than once, we took the average of its correlation with the other variable(s) of interest so as to avoid double-counting the relationship (Lipsey and Wilson 2001; O'Boyle et al. 2011; Schmidt and Hunter 2015).

The empty cells in the correlation matrix in Appendix E indicate where a particular relationship was not examined in our corpus of studies. Missing correlations are common in meta-analytic investigations such as ours that have a relatively large number of predictors (Viswesvaran and Ones 1995). The literature provides strategies for handling this issue, which we drew upon (Bergh et al. 2016; Colquitt et al. 2000;

Table 7. Relative Weight Analysis

Category	Raw Relative Weights	Raw Relative Weights as a Percentage of R^2
Personal Norms & Ethics	.106	20.66%
Attitude	.091	17.73%
Normative Beliefs	.069	13.38%
Self-Efficacy	.039	7.52%
Response Cost	.037	7.28%
SETA	.032	6.27%
Response Efficacy	.032	6.26%
Punishment Severity	.028	5.50%
Threat Severity	.027	5.24%
Detection Certainty	.024	4.61%
Punishment Expectancy	.012	2.27%
Rewards	.011	2.10%
Resource Vulnerability	.006	1.18%
Total R^2	**.514**	

Note: Raw relative weights add up to R^2 and raw weights as a % of R^2 add up to 100%.

Viswesvaran and Ones 1995). First, we followed the approach of Colquitt et al. (2000) and trimmed the full correlation matrix in Appendix E by eliminating categories with either a large number of missing relationships or a large number of relationships based on a single study. Namely, we eliminated the organizational support, perceived benefits, perceived ease of use, and perceived usefulness categories. We reasoned that eliminating these categories was not detrimental to our study because we retained most categories related to the prominent theories (e.g., DT, PMT, TRA/TPB) and constructs (e.g., personal norms & ethics, SETA) in the security policy compliance literature. Moreover, given the dearth of studies that examined relationships among the eliminated categories, we felt that including their effect size estimates in a relative weight analysis would weaken its validity. Finally, the main analysis results in Table 3 still provide an indication of each eliminated category's worth in predicting security policy compliance, albeit not in a relative sense.

The trimmed correlation matrix had 91 completed cells and four empty cells (the correlations between detection certainty-threat severity, personal norms & ethics-response efficacy, personal norms & ethics-rewards, and personal norms & ethics-threat severity). We could not find suitable surrogate effect size estimates from the literature for these empty cells, so we set them to the average effect size across all non-missing cells in our correlation matrix (.26) (Bergh et al. 2016; Viswesvaran and Ones 1995). Table 6 provides the final input matrix used for the relative weight analysis and the results of this analysis are summarized in Table 7.

The relative weights in Table 7 represent the percentage of variance in security policy compliance that is uniquely attributable to each category. The rank order of the relative weights is largely consistent with that of the category effect sizes in the main analysis in Table 3, thereby supporting the robustness of our findings in terms of the importance of each category in predicting security policy compliance and confirming their explanatory power in the presence of other predictors. Regarding the relative weights, the personal norms & ethics, attitude, and normative beliefs categories explain the most variance, followed by several other categories that have similar explanatory power (e.g., response efficacy, self-efficacy, SETA). Of lesser relative importance are the rewards, punishment expectancy, and resource vulnerability categories. One somewhat differing result between the two analyses is that of response cost. Response cost emerged as the fifth-strongest predictor in the relative weight analysis as compared to its lower rank ordering (and on the lower end of the medium threshold) in the main analysis. The statistical effects of correlated predictors likely explain the differing results, which do align with the growing evidence that stressful security requirements can have a deleterious influence on employees' security policy compliance (D'Arcy et al. 2014; Posey et al. 2014).[9]

[9]We conducted an additional relative weight analysis that accounted for potentially inflated intercorrelations from CMV. Using the Malhotra et al. (2006) formula for CMV-adjusted correlation, we recalculated the correlation matrix in Table 6 by partialling out the influence of CMV at the 0.10 level. Next, we re-ran the relative weight analysis with the CMV-adjusted correlation matrix. The results were virtually identical to those in Table 7 in terms of ordering and relative strength of the antecedent categories. The only change was that the R^2 dropped to .436.

Table 8. Moderator Analysis

Category	Moderator Group	Weighted Effect Size	|Observed Difference|	Number of Studies	Total Sample Size	Calculate z-test value	80% CV[a]	95% CI[b]	PVA[c]	Failsafe-M
Moderator 1: Nature of the Dependent Variable										
Attitude	Compliance	0.601	0.181	28	8,700	2.596*	0.32, 0.88	0.58, 0.62	5.99%	1,057
	Violation	0.420		9	2,275		0.11, 0.73	0.37, 0.47	6.77%	126
Detection Certainty	Compliance	0.430	0.026	11	3,315	0.286	0.31, 0.55	0.39, 0.47	59.28%	185
	Violation	0.404		9	3,205		0.10, 0.71	0.37, 0.44	6.04%	177
Normative Beliefs	Compliance	0.526	0.038	35	10,662	-0.558	0.25, 0.80	0.50, 0.55	7.91%	981
	Violation	0.564		8	1,754		0.25, 0.88	0.51, 0.62	6.77%	183
Personal Norms & Ethics	Compliance	0.441	0.218	8	1,838	-3.169*	0.22, 0.66	0.39, 0.49	16.09%	111
	Violation	0.659		12	3,132		0.40, 0.92	0.62, 0.70	7.19%	444
Punishment Expectancy	Compliance	0.325	0.013	12	3,084	0.142	0.10, 0.55	0.29, 0.36	20.23%	106
	Violation	0.312		17	4,895		0.09, 0.53	0.28, 0.34	11.86%	153
Punishment Severity	Compliance	0.236	0.100	9	2,815	-1.066	0.04, 0.50	0.23, 0.31	12.53%	64
	Violation	0.336		18	5,195		0.14, 0.57	0.32, 0.38	11.71%	225
Self-efficacy	Compliance	0.470	0.288	50	12,907	3.078*	0.16, 0.78	0.45, 0.49	9.31%	924
	Violation	0.182		8	1,709		-0.02, 0.39	0.13, 0.24	24.10%	11
SETA	Compliance	0.477	0.268	23	6,607	3.100*	0.26, 0.69	0.45, 0.50	9.96%	498
	Violation	0.209		7	1,791		0.06, 0.36	0.16, 0.26	46.60%	21
Moderator 2: Nature of Policy Compliance										
Attitude	Actual	0.578	0.013	7	2,251	-0.198	0.21, 0.95	0.53, 0.63	5.97%	240
	Intended	0.591		34	10,101		0.32, 0.86	0.57, 0.61	5.55%	1,165
Normative Beliefs	Actual	0.521	0.017	10	2,657	-0.216	0.29, 0.75	0.48, 0.56	14.01%	230
	Intended	0.538		37	11,212		0.25, 0.82	0.52, 0.56	6.63%	1,067
Organizational Support	Actual	0.583	0.116	5	1,203	1.422	0.21, 0.96	0.52, 0.65	7.25%	132
	Intended	0.467		7	1,546		0.39, 0.54	0.41, 0.52	100%	107
Punishment Expectancy	Actual	0.211	0.136	7	1,733	-1.437	0.00, 0.42	0.16, 0.26	17.63%	20
	Intended	0.347		21	6,005		0.13, 0.57	0.32, 0.37	14.30%	241
Response Cost	Actual	-0.568	0.302	7	1,502	-3.094*	-0.97, -0.16	-0.63, -0.51	5.64%	153
	Intended	-0.266		20	4,387		-0.60, 0.07	-0.30, -0.23	14.51%	84
Response Efficacy	Actual	0.385	0.048	8	1,948	-0.551	0.04, 0.73	0.33, 0.44	14.32%	75
	Intended	0.433		20	5,559		0.21, 0.66	0.40, 0.46	14.69%	315
Self-efficacy	Actual	0.415	0.029	16	4,166	-0.334	0.11, 0.72	0.38, 0.45	10.81%	206
	Intended	0.444		49	12,529		0.14, 0.75	0.42, 0.46	9.34%	788
Threat Severity	Actual	0.415	0.070	8	1,948	0.776	0.24, 0.59	0.36, 0.47	46.65%	86
	Intended	0.345		18	5,240		0.11, 0.58	0.31, 0.38	14.77%	174
Moderator 3: Type of Security Policy										
Attitude	General	0.581	0.055	24	7,591	0.841	0.32, 0.84	0.56, 0.61	6.70%	864
	Specific	0.526		13	3,384		0.18, 0.87	0.49, 0.56	4.97%	301
Detection Certainty	General	0.487	0.138	11	3,331	1.534	0.31, 0.66	0.45, 0.53	25.93%	244
	Specific	0.349		9	3,189		0.09, 0.61	0.31, 0.39	8.84%	128
Normative Beliefs	General	0.562	0.126	30	9,330	1.724	0.32, 0.81	0.54, 0.58	9.23%	989
	Specific	0.436		13	3,086		0.12, 0.75	0.40, 0.48	6.61%	186
Personal Norms & Ethics	General	0.400	0.249	6	1,397	-3.491*	0.16, 0.64	0.34, 0.46	14.90%	69
	Specific	0.649		14	3,573		0.42, 0.88	0.61, 0.69	8.46%	489
Punishment Expectancy	General	0.451	0.169	9	1,680	1.915	0.15, 0.75	0.40, 0.50	8.78%	113
	Specific	0.282		20	6,299		0.11, 0.45	0.25, 0.31	21.37%	160
Punishment Severity	General	0.471	0.174	6	1,333	2.176*	0.33, 0.61	0.41, 0.53	38.49%	92
	Specific	0.297		21	6,677		0.08, 0.51	0.27, 0.32	10.88%	204
Resource Vulnerability	General	0.203	0.032	11	3,437	-0.345	-0.04, 0.45	0.16, 0.24	15.20%	33
	Specific	0.235		9	2,624		-0.07, 0.54	0.19, 0.28	5.77%	41
Response Cost	General	-0.364	0.097	19	3,898	-0.919	-0.83, 0.10	-0.40, -0.33	7.81%	157
	Specific	-0.267		7	1,685		-0.55, 0.01	-0.32, -0.21	23.43%	32
Response Efficacy	General	0.439	0.073	15	3,522	0.846	0.18, 0.70	0.40, 0.48	16.73%	192
	Specific	0.366		9	2,780		0.08, 0.65	0.32, 0.41	9.87%	122

Table 8. Moderator Analysis (Continued)

Category	Moderator Group	Weighted Effect Size	|Observed Difference|	Number of Studies	Total Sample Size	Calculate z-test value	80% CV[a]	95% CI[b]	PVA[c]	Failsafe-M
Self-efficacy	General	0.491	0.150	40	9,724	1.725	0.15, 0.83	0.47, 0.51	8.19%	737
	Specific	0.341		19	5,119		0.11, 0.57	0.31, 0.37	14.68%	196
Threat Severity	General	0.346	0.009	14	3,433	0.098	0.08, 0.61	0.30, 0.39	19.34%	100
	Specific	0.337		8	2,267		0.15, 0.53	0.29, 0.38	18.49%	87
SETA	General	0.421	0.010	20	5,845	0.114	0.19, 0.65	0.39, 0.45	9.96%	348
	Specific	0.411		10	2,553		0.13, 0.69	0.37, 0.46	9.44%	135
Moderator 4: Location of Respondents										
Attitude	Europe	0.589	0.074	5	1,903	-1.289	0.13, 1,00	0.53, 0.64	2.53%	187
	North America	0.663		18	4,816		0.46, 0.87	0.63, 0.69	9.60%	723
Detection Certainty	Asia-Pacific	0.576	0.204	7	1,580	2.233*	0.28, 0.88	0.52, 0.63	6.27%	177
	North America	0.372		10	3,876		0.22, 0.53	0.34, 0.41	19.73%	166
Normative Beliefs	Asia-Pacific	0.696	0.119	7	1,980	2.156*	0.49, 0.90	0.65, 0.74	9.46%	339
	Europe	0.577		5	1,903		0.25, 0.90	0.52, 0.63	6.43%	184
	Europe	0.577	0.009	5	1,903	0.144	0.25, 0.90	0.52, 0.63	6.43%	184
	North America	0.568		19	4,644		0.33, 0.81	0.54, 0.60	9.53%	495
	North America	0.568	0.128	19	4,644	-2.149*	0.34, 0.81	0.54, 0.60	9.53%	495
	Asia-Pacific	0.696		7	1,980		0.49, 0.90	0.65, 0.74	9.46%	339
Perceived Benefits	North America	0.415	0.040	5	1,314	-0.368	0.29, 0.54	0.35, 0.47	33.07%	74
	Asia-Pacific	0.455		6	960		-0.27, 1.00	0.38, 0.52	1.86%	63
Punishment Expectancy	Europe	0.251	0.007	8	2,081	-0.072	0.14, 0.36	0.20, 0.30	65.67%	39
	North America	0.244		12	3,744		0.11, 0.38	0.21, 0.28	29.38%	66
Punishment Severity	North America	0.285	0.089	12	3,521	-1.073	0.09, 0.48	0.25, 0.32	17.97%	92
	Asia-Pacific	0.374		7	1,797		0.13, 0.62	0.32, 0.42	14.30%	84
Response Cost	Asia-Pacific	-0.129	0.767	8	1,282	9.776*	-0.52, 0.26	-0.19, -0.07	11.61%	N/A
	Europe	-0.896		6	976		-1.00, -0.61	-0.97, -0.82	10.36%	214
	Europe	-0.896	0.630	6	976	-10.931*	-1.00, -0.61	-0.97, -0.82	10.36%	214
	North America	-0.266		10	3,113		-0.38, -0.15	-0.30, -0.23	60.20%	69
	North America	-0.266	0.137	10	3,113	-1.155	-0.38, -0.15	-0.30, -0.23	60.20%	69
	Asia-Pacific	-0.129		8	1,282		-0.52, 0.26	-0.19, -0.07	11.61%	N/A
Response Efficacy	Europe	0.349	0.165	12	3,384	-1.950	0.03, 0.67	0.31, 0.39	13.59%	121
	North America	0.514		7	1,691		0.42, 0.61	0.46, 0.57	78.35%	145
Resource Vulnerability	Europe	0.109	0.159	8	3,088	-1.823	-0.11, 0.33	0.07, 0.15	15.12%	3
	North America	0.268		7	1,815		-0.02, 0.56	0.22, 0.32	11.29%	39
Self-efficacy	Asia-Pacific	0.571	0.164	8	1,879	1.819	0.34, 0.81	0.52, 0.62	17.37%	178
	Europe	0.407		10	2,873		0.07, 0.74	0.36, 0.45	10.70%	133
	Europe	0.407	0.27	10	2,873	-0.320	0.07, 0.74	0.36, 0.45	10.70%	133
	North America	0.434		26	6,092		0.11, 0.76	0.41, 0.46	8.69%	388
	North America	0.434	0.137	26	6,092	-1.503	0.11, 0.76	0.41, 0.46	8.69%	388
	Asia-Pacific	0.571		8	1,879		0.34, 0.81	0.52, 0.62	17.37%	178
SETA	Asia-Pacific	0.486	0.054	10	2,548	0.691	0.25, 0.72	0.44, 0.53	13.85%	192
	North America	0.432		11	3,217		0.19, 0.68	0.39, 0.47	9.30%	204
Threat Severity	Europe	0.385	0.218	13	3,941	2.283*	0.18, 0.59	0.35, 0.42	23.65%	159
	North America	0.167		5	1,045		-0.08, 0.41	0.10, 0.23	26.30%	6

*Denotes z-test values that are significant at $p < .05$.

[a]CV refers to the calculated Credibility Value.

[b]CI refers to the calculated Confidence Interval.

[c]PVA refers to the percent of variance in observed correlations attributable to sampling error and other artifacts (Schmidt and Hunter 2015; Schmidt and Le 2014).

Moderator Analysis

Sufficient data were provided in the articles to calculate a total of 40 moderator results.[10] Of these, the moderator was found to be significant at $p < .05$ in 16 instances (denoted in Table 8 with an "*"). By calculating the z for the individual correlations and then the z-score to compute the normal curve deviation (Cohen et al. 2003), effect size differences were determined between the moderators. In accounting for sample size during the z-score calculation, we calculated the harmonic mean as it is considered to provide a precise approximation of sample size relative to arithmetic mean and the total (Viswesvaran and Ones 1995).

The findings of the moderator analysis are presented in Table 8 and are discussed in detail within the following section. Worth mentioning here, however, is the issue of potential outliers influencing the moderator results, particularly because the moderator analysis is based on a limited number of studies per moderator group. Although we found no extreme outliers, there were two studies (Kinnunen 2016, Li and Luo 2017) that reported correlations an order of magnitude higher than most others for their particular category. We reviewed the research designs of these two studies and found no apparent reason for the higher values. However, to ensure that the two studies were not unduly influencing our moderator results, we followed the guidance of Lipsey and Wilson (2001) and recoded the suspect correlations down to the next lower effect size magnitude (i.e., from very large to large). The results with these new correlation values showed the same 16 significant moderating effects at $p < .05$ as in Table 8.

Discussion

Our objective in this study was to clarify the relative importance of the antecedents to security policy compliance, as well as the moderators of these relationships, in an effort to promote theoretical advancement in this research space. Based on the findings outlined above, a series of valuable insights were uncovered and are summarized in Table 9.

First, three of the top five categories with the highest overall effect sizes and strongest relative importance in explaining security policy compliance (attitude, personal norms & ethics, and normative beliefs) are all oriented around inherent employee values. These categories are closely linked with the psychological and ethical characteristics of employees, rather than other, lower-ranked categories, such as punishment, threats, and rewards, which are typically associated with managerial actions. Although these characteristics may be able to be influenced incrementally and cultivated over time, managers may find increased short-term compliance benefits by hiring employees with attitudes and beliefs that are consistent with organizational objectives, as well as supporting a security-centric culture that can further promote these characteristics. Additionally, as normative beliefs are based on the influences of significant individuals wanting employees to do, or not do, certain behaviors, ensuring that key personnel within the organization have the proper attitude and/or possess norms and ethics consistent with the organization's strategic objectives can be leveraged to have a trickle-down effect that promotes compliance with lower-level employees.

In comparison, the categories that are generally seen to be more easily manipulated by management, such as punishment and rewards, are among those with the lowest effect size magnitudes and that exhibited weaker relative importance in predicting security policy compliance. Despite the extensive research and theoretical support demonstrating the potential for these activities to influence security policy compliance, our findings suggest that they are only minimally effective. However, as our moderator analysis notes below, there are some specific circumstances where punishment does exhibit a stronger link to compliance (e.g., with general policies). Future research is required to clarify any new forms of rewards and punishment that may prove to be effective, as well as additional circumstances in which existing rewards and punishments are especially effective. For example, in a healthcare-related context, the security and privacy of patient data is of paramount importance and compliance may be enhanced by the potential for punishment (e.g., penalties associated with HIPAA violations) or the severity of the implications of noncompliance (e.g., significant financial loss). Likewise, a respondent's specific job role and responsibilities may influence the relative importance of punishment and rewards.

Our results also suggest that activities related to perceptions of security policy usefulness, effectiveness of actions (response efficacy), confidence in skills (self-efficacy), and training (SETA) all have a medium or large effect size. Response efficacy, self-efficacy, and SETA also each showed what could be considered mid-range relative importance in terms of predicting security policy compliance. Although

[10] As noted above, the minimum number of studies within each antecedent category was set at five. In order to maintain the same statistical power within the moderator analysis, we maintained this minimum threshold for each of the moderator groups. Of the 68 possible moderator comparisons (i.e., 4 moderators across 17 categories), 40 groups had at least 5 studies in both moderator groups (e.g., for the attitude category, 5 or more studies were required to examine actual compliance *and* 5 or more studies were required to examine intended compliance). However, care should be taken in interpreting the results from those moderators with a small number of studies and/or sample sizes.

Table 9. Implications and Opportunities for Future Research

Relationship	Finding	Practical and Research Implications	Future Research Questions
Antecedent Relationships to Security Policy Compliance			
Attitude, personal norms & ethics, and normative beliefs with security policy compliance	Three of the five antecedents with the largest effect sizes and relative importance draw on the inherent characteristics of individual employees.	Companies should prioritize hiring employees with inherent values that are consistent with the organization's approach to security. Future research should utilize theories in which attitude, personal norms/ethics, and normative factors play a central role (e.g., TPB, theory of interpersonal behavior, morality theories, social learning theory).	What specific attitudes, values, norms, and beliefs are most associated with employees who comply with security policies?
Punishment expectancy, punishment severity, and rewards with security policy compliance	Three of the four antecedents with the smallest effect sizes relate to aspects of punishment and rewards. These same antecedents did not have strong relative importance.	Punishment is only effective in specific circumstances (e.g., see type of moderator below). Theories that incorporate these constructs (e.g., DT, PMT, RCT) need to consider contextual factors that may alter their explanatory ability.	To what extent does a respondent's industry and job role moderate the relationship between punishment/rewards and policy compliance?
Perceived usefulness, response efficacy, self-efficacy, and SETA with security policy compliance	Employee competency and skill-centric activities all have either a medium or large effect size. They also exhibited mid-range relative importance scores.	Training may be able to help convince employees of the value of policies (perceived usefulness), as well as cultivating their skills and confidence (self-efficacy, response efficacy). Future research should consider theory-informed training approaches that foster security competencies as a means to improve policy compliance.	How can organizations better train and educate employees to enhance their perceived usefulness of security policies, as well as their self-efficacy and response efficacy?
Moderators of the Antecedents to Security Policy Compliance			
Measurement of policy compliance versus policy violation	In the eight categories where there was sufficient data to compare the results associated with policy compliance to policy violation, four categories showed significant differences in the results: attitude, personal norms & ethics, self-efficacy, and SETA.	Policy compliance and policy violation do not appear to be consistently measuring opposite ends of the same behavior. Although our analysis shows that sometimes the results are similar (e.g., detection certainty), researchers should not assume that findings associated with policy compliance behavior can be uniformly applied to policy violation behavior (and vice versa).	What are the unique aspects of employee behavior associated with security policy compliance that differ from security policy violation behavior?
Response cost for actual versus intended compliance	Response cost has a small negative effect on *intended* compliance, but a large negative effect on *actual* compliance.	Using intended compliance as a proxy for actual compliance may be inaccurate for the response cost category, as it may *underestimate* the negative impact on compliance.	Do employees not foresee the negative influence of response cost when considering their compliance intentions, but recognize its stronger negative influence on actual compliance behavior?
Punishment severity for general versus specific policies	Punishment severity is more strongly linked with policy compliance when the policy is *general*, compared to when the policy is *specific*.	For companies seeking employee compliance with *general* security policies, the magnitude of the effect of punishment severity may justify an increased focus on this category. Theories that incorporate the related constructs (e.g., DT, RCT) are better suited for explaining *general* policy compliance.	Why does punishment severity relate more strongly to employee compliance with *general* security policies as compared with *specific* policies?

Table 9. Implications and Opportunities for Future Research (Continued)

Relationship	Finding	Practical and Research Implications	Future Research Questions
Personal norms & ethics for general versus specific policies	Personal norms & ethics have a medium effect on policy compliance with *general* security policies, but a large effect on policy compliance with *specific* security policies.	For companies seeking employee compliance with *specific* security policies, the magnitude of the effect of personal norms/ethics may justify an increased focus on these categories. Theories that incorporate personal norms/ethics constructs (e.g., theory of cognitive moral development, DT/RCT models that incorporate informal sanctions) are better suited for explaining *specific* policy compliance.	Why do personal norms and ethics relate more strongly to employee compliance with *specific* security policies as compared to *general* policies?
Normative beliefs in Asia-Pacific versus Europe and North America	For Asia-Pacific respondents, normative beliefs have a significantly stronger positive relationship with policy compliance, compared to both North American and European respondents.	Companies operating in the Asia-Pacific region may be receiving improved security policy compliance through normative beliefs. Theories that incorporate normative factors (e.g., TPB, theory of interpersonal behavior) may be particularly well suited to Asia-Pacific samples.	Are normative beliefs much more strongly linked with policy compliance in the Asia-Pacific region compared to Europe and North America?
Response cost in Europe versus Asia-Pacific and North America	For European respondents, response cost has a very large negative effect size, while only a small negative effect size in Asia-Pacific and North America.	Companies operating in Europe may be particularly susceptible to policy violations where the response cost is deemed to be high by employees. Theories that incorporate related constructs (e.g., PMT), may have weaker explanatory power in Asia-Pacific and North American samples.	Is response cost much more strongly linked with policy violations in Europe compared to Asia-Pacific and North America?

each of these categories has an important link to policy compliance on its own, the logical integration between the activities represents a powerful, yet relatively straightforward opportunity for organizations. Rather than focusing only on the periodic training and education of employees, our findings show the importance of convincing employees of the value of policies (perceived usefulness), as well as cultivating their skills and confidence (self-efficacy, response efficacy) (e.g., Puhakainen and Siponen 2010).

For example, organizations can share anecdotal evidence of how policies have mitigated security incidents in the past (both internal and external to the organization) to demonstrate that policies are both important and effective. Additionally, skills and confidence can be increased not only through more traditional training initiatives, but also by the appointment of a security "champion" on each project team or in each functional area of the organization. Such an approach could provide a more accessible training resource to employees who may be uncertain about compliance practices and procedures and thus boost the efficacy of all individuals within the group. Finally, future research could investigate the ways that training could more effectively facilitate these longer-term, ongoing objectives. The role of training is of particular importance in a North American environment, as we note in our moderator analysis below.

From a broader research perspective, our results suggest that many of the extant security policy compliance models are plagued by suboptimal theoretical framing, at least to a degree. Indeed, constructs from DT, PMT, and RCT are popular antecedents to security policy compliance (see Appendix A), yet these constructs fall within categories that have some of the weakest effect sizes and relative importance in our analysis. Notably, the relatively weak effects for the DT constructs (punishment expectancy, punishment severity) align with views that the theory is best suited for the study of malicious security policy violations and computer abuse activities (e.g., data manipulation or destruction, data theft) (D'Arcy and Herath 2011; Willison and Warkentin 2013), consistent with DT's criminological roots, rather than the more benign types of behaviors that are often the subject of security policy compliance studies (e.g., adhering to or violating policies regarding sharing passwords, insecure USB practices, locking computers, etc.). This is not to say that DT is irrelevant in the security policy compliance context, but it does appear that the influences of DT constructs are surpassed by those of other theories, such as those of the TPB.

Similarly, the small-to-medium effects and relative importance of certain PMT constructs (i.e., resource vulnerability, threat severity) align with recent claims that PMT is misspecified in security policy compliance contexts (unless

contextualized to situations of personal relevance; Johnston et al. 2015). Whereas this argument has previously been rooted in the referent PMT literature on health behavior, we give it an empirical backing based on a consolidated analysis of security policy compliance research. Taking this further, the limited amount of variance explained by several of the PMT constructs in our relative weight analysis suggests that the full PMT nomology is not essential for the study of security policy compliance. Notably, our finding on this matter contrasts with that of Boss et al. (2015), who recommended the complete PMT nomology in IS security contexts based on their two-study analysis.

In advancing the theoretical understanding of security policy compliance, our results point to the explanatory ability of theories in which attitudes, personal norms and ethics, and normative beliefs occupy a central position. Such theories can provide the foundation for contextualized models that incorporate additional constructs. The TPB fits this purpose and we recommend it over its predecessor, the TRA, because the former incorporates normative influences and self-efficacy. Additional candidates are the theory of interpersonal behavior (Triandis 1977), because attitude and social influence are central to this theoretical framework; theories of moral development (Kohlberg 1969) and moral identity (Aquino and Reed 2002); and social learning theory (Warkentin et al. 2011). Aside from the TPB, these theories have received little attention in the security policy compliance literature, yet our results suggest their superior explanatory ability over the oft-used DT, PMT, and RCT in this context.

Contextual Moderators

Our moderator analysis sought to explain some of the variation within categories in relation to security policy compliance and, in doing so, identify boundary conditions for the application of certain theories in this domain. Of particular interest are those moderators where one category is significantly different from the other.

For our first moderator, we focused on the differences stemming from the measurement of employee compliance with a security policy compared to measuring security policy violations. Overall, our results suggest that policy compliance and policy violation should not be considered opposite views of the same construct since four of the eight categories (where sufficient data were available) highlighted significant differences depending on the approach used to measure the dependent variable. However, because there were also four categories that did not display significant differences, we recognize that at least some fundamental elements may be shared between the two concepts. This finding supports past views (e.g., D'Arcy and Herath 2011; Guo 2013) that policy compliance and policy violation are distinguished by at least some unique elements. As noted, this is a critical issue and our empirical results offer a unique contribution compared to other, more limited assessments of the security policy compliance literature.

For example, we help rectify what we earlier labeled as an unresolved conflict with respect to the unified model of security policy compliance from Moody et al. (2018). In that study, the authors used policy violation as the dependent variable and did not include attitude as a construct in their model, nor did they include standalone constructs for social norms or moral considerations. Yet, the results of a number of other security policy compliance studies suggest that attitude, social norms, and moral considerations are important predictors of security policy compliance. Our moderator analysis suggests that the influences of security-related attitudes and moral considerations, in particular, depend on whether the dependent variable is positive (compliance) or negative (violation). It therefore stands to reason that the accuracy of theories that include attitudes and personal norms and ethics constructs depend on the types of security behavior to which they are applied.

Specifically, theories that incorporate personal norms and ethics constructs (e.g., theory of cognitive moral development; Kohlberg 1969; Myyry et al. 2009) appear better suited to the study of security policy violations as opposed to security policy compliance. On the other hand, theories such as social cognitive theory and social learning theory (Bandura 1977), which provide a basis for self-efficacy and other individual learning-related constructs (e.g., SETA) in the security policy compliance context, appear more suited to the study of security policy compliance. Moving forward, we recommend that researchers cease their attempts at a single, unified model of security policy compliance. Based on our results, such attempts are likely to be fruitless given the apparent differences between policy compliance and policy violations (and the other differences based on our moderator results, as described below). We therefore recommend further research to determine the unique aspects of employee behavior associated with security policy compliance that differ from security policy violation behavior.

The second moderator analysis examined the differences resulting from studies that examined actual compliance with security policies versus those studies that examined intended compliance. Our findings partially confirm past work (e.g., Jenkins and Durcikova 2013; Vance et al. 2014) suggesting that the use of intended compliance as a proxy for actual compliance is not uniformly reliable, since we found significantly different results for the response cost category. However, our

results did highlight seven antecedent categories where the relationships with actual versus intended compliance are not significantly different. Indeed, our results did not uncover a consistent pattern in those categories where variances did occur.

These findings lend some credence to our earlier point that the information security context is unique from other IS contexts where the intention-to-behavior linkage is much stronger (e.g., Venkatesh et al. 2003). This result is consistent with the view of IS security scholars who have advocated a move away from the intention construct, where possible, in an attempt to study actual security-related behaviors (Crossler et al. 2013; Lowry et al. 2017). Accordingly, future research should strive toward novel study designs that capture actual policy compliance behavior. We speculate that if/when researchers begin to utilize such designs in security policy compliance studies, the results will show even stronger evidence of a gap between intention and actual behavior. On this point, we note that each of the studies in our meta-analysis that included actual security policy compliance (or violation) measured the construct using self-reported responses. An argument can be made that self-reported actual behaviors are not much different than intended behaviors and, therefore, our finding of a moderating influence of actual versus intended security policy compliance for even one category (response cost) is conservative. With respect to this finding, one speculative explanation is that employees underestimate the burden of policy requirements when considering their compliance intentions; in contrast, such burdens have a strong negative influence on their actual compliance behavior. Future research could delve into this issue further and also seek to uncover why some employees intend to violate a policy to a lesser extent than they actually do (e.g., response cost).

Our third moderator analysis examined the differences stemming from the use of a general security policy versus a specific policy. For one category—punishment severity—the effect size was medium for general policies and small for specific policies. This suggests that employees interpret the narrow scope of specific policies to correspond to diminished sanctions, in comparison to the more severe punishments of general policies. We do not have a clear explanation for this result, but one conjecture is that when punishment can be applied more generally it is deemed as more severe. As well, even though our results did not show a particularly strong effect size or relative importance for perceived severity, the significant moderating influence of general versus specific policy for this category has practical importance. This is because many well-known industry standards for information security management (e.g., ISO/IEC 27002) draw heavily on punishment-based approaches for combating security policy violations and other forms of IS misuse and abuse (Theoharidou et al. 2005). Gaining a deeper understanding of how employees respond to such approaches (which, consequently, are incorporated within most firms' security policies) is therefore important for furthering the effectiveness and validity of such industry standards.

In contrast to our results for perceived severity, for the personal norms and ethics category, the effect size was medium for general policies, but extended to the large threshold for specific policies. This suggests that the more focused guidelines associated with specific policies increases the importance of norms and ethics in achieving policy compliance. In terms of boundary conditions, these results suggest that theoretical models that incorporate personal norms and ethics constructs (e.g., theory of cognitive moral development; Kohlberg 1969; Myyry et al. 2009) will have greater explanatory power when a specific security policy is being considered. Alternatively, theoretical models that incorporate punishment constructs (e.g., DT, RCT) will exhibit greater explanatory power when a general security policy is being considered.

Future research could explore why the antecedents to compliance with general and specific policies vary to this extent. One possible explanation for the variance of personal norms and ethics is that when policy guidelines are more specific and tailored to a particular technology (e.g., antivirus), an employee's inherent ethical outlook may be more easily understood and applied within the context of the desired behavior, when compared to a more general policy where an employee's ethical norms may be difficult to apply to a broad and wide-ranging policy. The results also suggest that the influences of moral and ethical considerations in the security policy compliance context are partially behavior-specific. An extension of this finding for organizations is that they have some power to foster security policy compliance, for example, by educating employees on their moral responsibilities toward specific behaviors, rather than solely relying on the hiring of employees with certain dispositional traits related to morality and ethics (e.g., having a principled ethical ideology or characteristics of a moral personality; McFerran et al. 2010).

The fourth moderator we considered was the location of the respondents. Our results are consistent with past research (Hovav and D'Arcy 2012; Kam et al. 2015; Lowry and Moody 2015) that suggests geographical location can influence security policy compliance. However, our results extend the discussion by highlighting the specific categories where these differences are most prominent. As well, our results answer past calls (e.g., Crossler et al. 2013) for research to analyze cross-cultural differences in security policy com-

pliance beyond a two-country comparison by making assessments on a broader scale.

Notably, most prior cross-cultural studies in the security policy compliance literature compare only countries from North America and East Asia (e.g., China, South Korea). In contrast, our consolidated analysis of the literature afforded us the ability to provide previously unexplored cross-cultural comparisons in this research space, such as between the North American and European regions and those of Europe and Asia-Pacific. Our results noted significant differences between the Asia-Pacific region and Europe/North America (detection certainty, normative beliefs), as well as between Europe and Asia-Pacific/North America (response cost, threat severity). This finding supports past views (e.g., Kam et al. 2015) that Asia-Pacific cultural characteristics play a significant role in compliance behaviors; in the normative beliefs category, the region was most likely to comply (0.696 effect size), while in the response cost category, the region was least likely to violate (-0.129 effect size). The finding also provides a boundary condition for the application of theories that incorporate normative constructs (e.g., TPB, theory of interpersonal behavior) and response cost constructs (e.g., PMT), as the models rooted in these theories may exhibit different explanatory power depending on the region in which they are applied.

Additionally, given the history of DT in the IS security literature, it is worth commenting on our moderator results that shed light on the application of DT to security policy compliance. These results suggest that DT's punishment expectancy and punishment severity constructs apply equally well across both compliance and violation behaviors. Notably, this finding contrasts with the views of IS security scholars who have speculated that DT is not suited for the study of positive security behaviors, such as policy compliance (D'Arcy and Herath 2011). Our collective findings on DT suggest that its constructs have some predictive ability across a range of positive and negative security-related behaviors, yet these constructs should be augmented with those from other theories to produce research models with adequate explanatory power.

Limitations

Our findings should be viewed through the lens of a few limitations. First, as previously noted, we recognize the possible role of CMV in influencing our results. To address this issue to the extent possible, we compared the effect sizes of studies that accounted for CMV to those that did not, as well as conducted a relative weight analysis based on a CMV-adjusted correlation matrix. Although the results did not substantially alter our findings overall, we cannot preclude the possibility that CMV is biasing all of the correlations in our data. In the future, researchers are encouraged to follow past guidance to control for and offset the influence of CMV, such as obtaining variable measurements from different sources, as well as temporally separating measurement (e.g., using a time lag) (Podsakoff et al. 2003), rather than using performative steps in the data analysis phase that cannot eliminate the threat of CMV.

Using separate data sources for independent and dependent variables is an ideal remedy for combatting CMV (Podsakoff et al. 2003). One of the very few examples of such a design in the security policy compliance literature is the Workman et al. (2008) study, in which the independent variables were captured with self-report survey measures and one of the dependent variables was captured with computer logs of actual security behavior. In citing this example, we recognize the extreme difficulties in obtaining actual employee security behavior due to a variety of reasons (Crossler et al. 2013; Kotulic and Clark 2004). If it is not possible to obtain data from different sources, capturing independent and dependent variables at different points in time is an alternative solution for alleviating CMV. As examples, Thatcher et al. (2018) used such a design in their two-part survey-based study of information technology mindfulness, as did D'Arcy and Greene (2014) in the security policy compliance context.

More broadly, our view is that security policy compliance research has reached the level of maturity where, moving forward, more stringent research designs that counter the validity threat of CMV are necessary. Doing so is crucial to the advancement of theory, research, and practice on security policy compliance. The lack of controlling for CMV is a deficiency in the IS literature in general, and we are not the first to raise this issue (e.g., Sharma et al. 2009; Straub and Burton-Jones 2007). We echo the views of IS scholars who consider CMV a threat to published findings in major IS research domains, and certainly with respect to the security policy compliance literature.

As a second limitation, there is the possibility that relevant antecedent categories within the papers we examined could have been omitted. Although we employed rigorous methods to construct 17 categories from a total of 401 independent variables, we also followed guidance from past literature to set the minimum number of studies per antecedent category at five. As a result, it is possible that additional categories could exist from those independent variables without a substantive presence in the current literature that could further illuminate the antecedents to security policy compliance.

Additionally, the veracity of our conclusions is closely associated with the quantity of papers that are included in the analysis, along with the accompanying sample sizes within the papers. In areas where fewer papers exist, such as in the rewards category or within some areas of the moderators (e.g., detection certainty, response cost), statistical power is reduced (Schmidt 1996; Schmidt and Hunter 2015). As well, the existence of unpublished papers or future publications with results that differ from the existing literature could alter a category's effect sizes and caution should be taken in interpreting the accompanying results. Although our quantity of in-scope publications is favorable compared with several past meta-analyses, we took the precautionary measures of including the calculation of confidence intervals and Failsafe-N for all categories and requesting unpublished papers from active scholars. However, despite these efforts, a possibility exists that effect size fluctuations could occur as more publications emerge. Similarly, the criteria we set for including studies in our analysis were chosen in order to encompass a broad range of security policy compliance issues, but not so broad as to erode the questions that our results could address. We recognize that other areas of behavioral IS security were deemed out of scope of our study (e.g., personal/home security behaviors outside of an organizational context), but that a future meta-analysis in such areas may very well be warranted.

Conclusion

Properly securing vital systems and data continues to be a pressing need for organizations operating in the digital age. Despite the many technical solutions available to security experts, human behavior (and the policies designed to govern their behavior) continues to be the focal point upon which security efforts often succeed or fail. A rich stream of literature has identified numerous antecedents to security policy compliance and theoretical perspectives that can frame this behavior; however, the inconsistencies and lack of theoretical congruence in this literature led us to conduct a meta-analysis that aggregates and analyzes the findings of 95 empirical papers addressing security policy compliance. Some of the most noteworthy findings revealed through this analysis include (1) the relative strength of the link between employee attitudes/norms/beliefs and policy compliance, (2) the relative weakness of the link between rewards/punishment/threats and policy compliance, (3) the support for security policy compliance and violation as representing at least partially distinct concepts, (4) the inconsistent links between the antecedent categories and actual versus intended compliance, (5) the inconsistent links between general security policies versus specific policies and compliance, and (6) the importance of selected antecedents for particular national cultures. We hope that our results bring greater clarity to the security policy compliance literature and provide guidance that facilitates future theoretical work in this domain.

Acknowledgments

The authors thank the senior editor, associate editor, and reviewers for their constructive and developmental feedback throughout the review process. We also thank Jane Webster, Jack Neil, and the Bentley University Data Innovation Network for their support.

References

Ajzen, I. 1991. "The Theory of Planned Behavior," *Organizational Behavior and Human Decision Processes* (50:2), pp. 179-211.

Aquino, K., and Reed, A. 2002. "The Self-Importance of Moral Identity," *Journal of Personality and Social Psychology* (83:6), pp. 1423-1440.

Association for Information Systems. 2017. "AISWorld List Usage Policy and Conditions" (https://aisnet.org/?ISWorldServPolicies; retrieved January 27, 2018).

Balozian, P., and Leidner, D. 2017. "Review of IS Security Compliance: Toward the Building Blocks of an IS Security Theory," *The DATA BASE for Advances in Information Systems* (48:3), pp. 11-43.

Bandara, W., Furtmueller, E., Gorbacheva, E., Miskon, S., and Beekhuyzen, J. 2015. "Achieving Rigor in Literature Reviews: Insights from Qualitative Data Analysis and Tool-Support," *Communications of the AIS* (34:8), pp. 154-204.

Bandura, A. 1977. "Self-Efficacy: Toward a Unified Theory of Behavioral Change," *Psychological Review* (84:2), pp. 191-215.

Bauer, S., and Bernroider, E. W. N. 2017. "From Information Security Awareness to Reasoned Compliant Action: Analyzing Information Security Policy Compliance in a Large Banking Organization," *The DATA BASE for Advances in Information Systems* (48:3), pp. 44-68.

Bergh, D. D., Aguinis, H., Heavey, C., Ketchen, D. J., Boyd, B. K., Su, P., Lau, C. L. L., and Joo, H. 2016. "Using Metaanalytic Structural Equation Modeling to Advance Strategic Management Research: Guidelines and an Empirical Illustration Via the Strategic Leadership–Performance Relationship," *Strategic Management Journal* (37:3), pp. 477-497.

Borenstein, M., Hedges, L. V., Higgins, J. P., and Rothstein, H. R. 2009. *Introduction to Meta-Analysis*, Chichester, UK: John Wiley & Sons, Ltd.

Boss, S. R., Galletta, D., Moody, G. D., Lowry, P. B., and Polak, P. 2015. "What Do Users Have to Fear? Using Fear Appeals to Engender Threats and Fear That Motivate Protective Behaviors in Users," *MIS Quarterly* (39:4), pp. 837-864.

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

Chin, W., Thatcher, J., and Wright, R. 2012. "Assessing Common Method Bias: Problems with the ULMC Technique," *MIS Quarterly* (36:3), pp. 1003-1019.

Chu, A. M. Y., Chau, P. Y. K., and So, M. K. P. 2015. "Explaining the Misuse of Information Systems Resources in the Workplace: A Dual-Process Approach," *Journal of Business Ethics* (131:1), pp. 209-225.

Cohen, J. 1960. "A Coefficient of Agreement for Nominal Scales," *Educational and Psychological Measurement* (20:1), pp. 37-46.

Cohen, J. 1988. *Statistical Power Analysis for the Behavioral Sciences* (2nd ed.), Hillsdale, NJ: Lawrence Erlbaum Associates.

Cohen, J., Cohen, P., West, S. G., and Aiken, L. S. 2003. *Applied Multiple Regression/Correlation Analysis for the Behavioral Sciences*, Mahwah, NJ: Lawrence Erlbaum Associates.

Colquitt, J. A., Conlon, D. E., Wesson, M. J., Porter, C. O. L. H., and Ng, K. Y. 2000. "Justice at the Millennium: A Meta-Analytic Review of 25 Years of Organizational Justice Research," *The Journal of Applied Psychology* (86:3), pp. 425-445.

Cooper, H., Hedges, L. V., and Valentine, J. C. (eds.). 2009. *The Handbook of Research Synthesis and Meta-Analysis*, New York: Russell Sage Foundation.

Cram, W. A., Proudfoot, J. G., and D'Arcy, J. 2017. "Organizational Information Security Policies: A Review and Research Framework," *European Journal of Information Systems* (26:6), pp. 605-641.

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* (32), pp. 90-101.

D'Arcy, J., and Greene, G. 2014. "Security Culture and the Employment Relationship as Drivers of Employees' Security Compliance," *Information Management & Computer Security* (22:5), pp. 474-489.

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* (29:6), pp. 643-658.

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

Dennis, A. R., Wixom, B. H., and Vandenberg, R. J. 2001. "Understanding Fit and Appropriation Effects in Group Support Systems Via Meta-Analysis," *MIS Quarterly* (25:2), pp. 167-193.

Dickersin, K. 2005. "Publication Bias: Recognizing the Problem, Understanding Its Origins, and Scope, and Preventing Harm," in *Publication Bias in Meta Analysis: Prevention, Assessment, and Adjustments,* H. R. Rothstein, A. J. Sutton, and M. Borenstein (eds.), Chichester, UK: John Wiley & Sons, Ltd., pp. 11-33.

Dimoka, A. 2010. "What Does the Brain Tell Us About Trust and Distrust? Evidence from a Functional Neuroimaging Study," *MIS Quarterly* (34:2), pp. 373-396.

Doi, S. A. R., Barendregt, J. J., Khan, S., Thalib, L., and Williams, G. M. 2015. "Advances in the Meta-Analysis of Heterogeneous Clinical Trials I: The Inverse Variance Heterogeneity Model," *Contemporary Clinical Trials* (45:Part A), pp. 130-138.

Foth, M. 2016. "Factors Influencing the Intention to Comply with Data Protection Regulations in Hospitals: Based on Gender Differences in Behaviour and Deterrence," *European Journal of Information Systems* (25:2), pp. 91-109.

Geganfurtner, A. 2011. "Comparing Two Handbooks of Meta-Analysis: Review of Hunter & Schmidt, Methods of Meta-Analysis: Correcting Error and Bias in Research Findings, and Borenstein, Hedges, Higgins, and Rothstein, Introduction to Meta-Analysis," *Vocations and Learning* (4:-), pp. 169-174.

Gerow, J. E., Ayyagari, R., Thatcher, J., and Roth, P. L. 2013. "Can We Have Fun @ Work? The Role of Intrinsic Motivation for Utilitarian Systems," *European Journal of Information Systems* (22:3), pp. 360-380.

Gerow, J. E., Grover, V., Thatcher, J., and Roth, P. L. 2014. "Looking Toward the Future of IT-Business Strategic Alignment through the Past: A Meta-Analysis," *MIS Quarterly* (38:4), pp. 1159-1185.

Glass, G. V. 1976. "Primary, Secondary, and Meta-Analysis of Research," *Review of Research in Education* (5:10), pp. 351-379.

Goo, J., Yim, M.-S., and Kim, D. J. 2014. "A Path to Successful Management of Employee Security Compliance: An Empirical Study of Information Security Climate," *IEEE Transactions on Professional Communication* (57:4), pp. 286-308.

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

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

He, J., and King, W. R. 2008. "The Role of User Participation in Information Systems Development: Implications from a Meta-Analysis," *Journal of Management Information Systems* (25:1), pp. 301–331.

Hedges, L. V., and Pigott, T. D. 2001. "The Power of Statistical Tests in Meta-Analysis," *Psychological Methods* (6:3), pp. 203-217.

Herath, T., and Rao, H. R. 2009a. "Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness," *Decision Support Systems* (47:2), pp. 154-165.

Herath, T., and Rao, H. R. 2009b. "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations," *European Journal of Information Systems* (18:2), pp. 106-125.

Hopewell, S., Clarke, M., and Mallett, S. 2005. "Grey Literature and Systematic Reviews," in *Publication Bias in Meta Analysis: Prevention, Assessment, and Adjustments,* H. R. Rothstein, A. J. Sutton, and M. Borenstein (eds.), Chichester, UK: John Wiley & Sons, Ltd., pp. 49-72.

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* (49:2), pp. 99-110.

Hui, K. L., Vance, A., and Zhdanov, D. 2016. "Securing Digital Assets," in *MIS Quarterly Research Curations* (https://misq.org/research-curations/).

Hunt, M. 1997. *How Science Takes Stock: The Story of Meta-Analysis*, New York: Russell Sage Foundation.

Hwang, M. I. 2014. "Disentangling the Effect of Top Management Support and Training on Systems Implementation Success: A Meta-Analysis," *Communications of the AIS* (35:2), pp. 19-37.

Ifinedo, P. 2012. "Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory," *Computers & Security* (31:1), pp. 83-95.

Jenkins, J. L., and Durcikova, A. 2013. "What, I Shouldn't Have Done That? The Influence of Training and Just-in-Time Reminders on Secure Behavior," in *Proceedings of the 34th International Conference on Information Systems*, Milan, Italy.

Jenkins, J. L., Durcikova, A., Ross, G., and Nunamaker Jr., J. F. 2010. "Encouraging Users to Behave Securely: Examining the Influence of Technical, Managerial, and Educational Controls on Users' Secure Behavior," in *Proceedings of the 31st International Conference on Information Systems*, St. Louis, MO.

Jiang, K., Lepak, D. P., Hu, J., and Baer, J. 2012. "How Does Human Resource Management Influence Organizational Outcomes? A Meta-Analytic Investigation of Mediating Mechanisms," *Academy of Management Journal* (55:6), pp. 1264-1294.

Johnson, J. W. 2000. "A Heuristic Method for Estimating the Relative Weight of Predictor Variables in Multiple Regression," *Multivariate Behavioral Research* (35:1), pp. 1-19.

Johnson, J. W., and LeBreton, J. M. 2004. "History and Use of Relative Importance Indices in Organizational Research," *Organizational Research Methods* (7:3), pp. 238-257.

Johnston, A. C., Warkentin, M., and Siponen, M. 2015. "An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset through Sanctioning Rhetoric," *MIS Quarterly* (39:1), pp. 113-134.

Joseph, D., Ng, K.-Y., Koh, C., and Ang, S. 2007. "Turnover of Information Technology Professionals: A Narrative Review, Meta-Analytic Structural Equation Modeling, and Model Development," *MIS Quarterly* (31:3), pp. 547-577.

Kam, H.-J., Katerattanakul, P., and Hong, S.-G. 2015. "A Tale of Two Cities: Policy Compliance of the Banks in the United States and South Korea," *European Conference on Information Systems*, Münster, Germany.

Kaspersky Lab. 2017. "Human Factor in IT Security: How Employees Are Making Businesses Vulnerable from Within" (https://usa.kaspersky.com/about/press-releases/2017_kaseprsky-lab-survey-one-in-four-hide-cybersecurity-incidents-from-their-employers; retrieved October 4, 2017).

Kepes, S., Banks, G. C., McDaniel, M., and Whetzel, D. L. 2012. "Publication Bias in the Organizational Sciences," *Organizational Research Methods* (15:4), pp. 624-662.

Kinnunen, S. 2016. "Exploring Determinants of Different Information Security Behaviors," Master's Thesis, University of Jyväskylä.

Kohlberg, L. 1969. "Stage and Sequence: The Cognitive Developmental Approach to Socialization," in *Handbook of Socialization Theory,* D. A. Goslin (ed.),Chicago: Rand McNally, pp. 347-380.

Kohli, R., and Devaraj, S. 2003. "Measuring Information Technology Payoff: A Meta-Analysis of Structural Variables in Firm-Level Empirical Research," *Information Systems Research* (14:2), pp. 127-145.

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

Landis, J. R., and Koch, G. G. 1977. "The Measurement of Observer Agreement for Categorical Data," *Biometrics* (33:1), pp. 159-174.

Lee, G., and Xia, W. 2006. "Organizational Size and IT Innovation Adoption: A Meta-Analysis," *Information & Management* (43:8), pp. 975-985.

Li, H., and Luo, X. 2017. "The Role of Situational Moral Judgment and Deterrence on Information Security Policy Violation," in *Proceedings of 1st International Conference on Internet Plus, Big Data & Business Innovation*, Beijing, China.

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* (24:6), pp. 479-502.

Li, H., Zhang, J., and Sarathy, R. 2010. "Understanding Compliance with Internet Use Policy from the Perspective of Rational Choice Theory," *Decision Support Systems* (48:4), pp. 635-645.

Liang, H., and Xue, Y. 2010. "Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective," *Journal of the Association for Information Systems* (11:7), pp. 394-413.

Liberati, A., Altman, D. G., Tetzlaff, J., Mulrow, C., Gøtzsche, P. C., Ioannidis, J. P. A., Clarke, M., Devereaux, P. J., Kleijnen, J., and Moher, D. 2009. "The Prisma Statement for Reporting Systematic Reviews and Meta-Analyses of Studies That Evaluate Health Care Interventions: Explanation and Elaboration," *PLoS Medicine* (6:7), pp. 1-28.

Lipsey, M. W., and Wilson, D. B. 2001. *Practical Meta-Analysis*, Thousand Oaks, CA: SAGE Publications.

Long, J. 2001. "An Introduction to and Generalization of the "Fail-Safe N"," paper presented at the annual meeting of the Southwest Educational Research Association, New Orleans, LA.

Lowry, P. B., Dinev, T., and Willison, R. 2017. "Why Security and Privacy Research Lies at the Centre of the Information Systems (IS) Artefact: Proposing a Bold Research Agenda," *European Journal of Information Systems* (26:6), pp. 546-563.

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* (25:5), pp. 465-488.

Malhotra, N. K., Kim, S. S., and Patil, A. 2006. "Common Method Variance in IS Research: A Comparison of Alternative Approaches and a Reanalysis of Past Research," *Management Science* (52:12), pp. 1865-1883.

McDaniel, M., Rothstein, H. R., and Whetzel, D. L. 2006. "Publication Bias: A Case Study of Four Test Vendors," *Personnel Psychology* (59:4), pp. 927-953.

McFerran, B., Aquino, K., and Duffy, M. 2010. "How Personality and Moral Identity Relate to Individuals' Ethical Ideology," *Business Ethics Quarterly* (20:1), pp. 35-56.

Moody, G. D., Siponen, M., and Pahnila, S. 2018. "Toward a Unified Model of Information Security Policy Compliance," *MIS Quarterly* (42:1), pp. 285-331.

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

O'Boyle Jr., E. H., Humphrey, R. H., Pollack, J. M., Hawver, T. H., and Story, P. A. 2011. "The Relation between Emotional Intelligence and Job Performance: A Meta-Analysis," *Journal of Organizational Behavior and Human Decision Processes* (32:5), pp. 788-818.

Ormond, D., Warkentin, M., and Crossler, R. E. 2019. "Integrating Cognition with an Affective Lens to Better Understand Information Security Policy Compliance," *Journal of the Association for Information Systems* (forthcoming).

Pahnila, S., Karjalainen, M., and Siponen, M. 2013. "Information Security Behavior: Towards Multi-Stage Models," in *Proceedings of the Pacific Asia Conference on Information Systems*, Jeju Island, South Korea.

Parker, D. B. 1998. *Fighting Computer Crime: A New Framework for Protecting Information*, New York: Wiley.

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., and Podsakoff, N. P. 2003. "Common Method Bias in Behavioral Research: A Critical Review of the Literature and Recommended Remedies," *Journal of Applied Psychology* (88:5), pp. 879-903.

Ponemon Institute. 2016. "Managing Insider Risk through Training & Culture," Ponemon Institute© Research Report, Traverse City, MI.

Posey, C., Roberts, T. L., Lowry, P. B., and Hightower, R. T. 2014. "Bridging the Divide: A Qualitative Comparison of Information Security Thought Patterns between Information Security Professionals and Ordinary Organizational Insiders," *Information & Management* (51), pp. 551-567.

Pratt, T. C., Cullen, F. T., Blevins, K. R., Daigle, L. E., and Madensen, T. D. 2006. "The Empirical Status of Deterrence Theory: A Meta-Analysis," in *Taking Stock: The Status of Criminological Theory,* F. T. Cullen, J. P. Wright, and K. R. Blevins (eds.), New Brunswick, NJ: Transaction Publishers, pp. 37-76.

Puhakainen, P., and Siponen, M. 2010. "Improving Employees' Compliance through Information Systems Security Training: An Action Research Study," *MIS Quarterly* (34:4), pp. 757-778.

PwC. 2016. "The Global State of Information Security Survey 2016" (http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html; retrieved January 30, 2017).

Richardson, H. A., Simmering, M. J., and Sturman, M. C. 2009. "A Tale of Three Perspectives: Examining Post Hoc Statistical Techniques for Detection and Correction of Common Method Variance," *Organizational Research Methods* (12:4), pp. 762-800.

Rosenberg, M. S. 2005. "The File-Drawer Problem Revisited: A General Weighted Method for Calculating Fail-Safe Numbers in Meta-Analysis," *Evolution* (59:2), pp. 464-468.

Rosenthal, R. 1979. "The "File Drawer Problem" and Tolerance for Null Results," *Psychological Bulletin* (86:3), pp. 638-641.

Rothstein, H. R., Sutton, A. J., and Borenstein, M. 2005. "Publication Bias in Meta-Analysis," in *Publication Bias in Meta Analysis: Prevention, Assessment, and Adjustments,* H. R. Rothstein, A. J. Sutton, and M. Borenstein (eds.), Chichester, UK: John Wiley & Sons, Ltd., pp. 1-7.

Sabherwal, R., Jeyaraj, A., and Chowa, C. 2006. "Information System Success: Individual and Organizational Determinants," *Management Science* (52:12), pp. 1849-1864.

Schmidt, F. L. 1996. "Statistical Significance Testing and Cumulative Knowledge in Psychology: Implications for Training of Researchers," *Psychological Methods* (1:2), pp. 115-129.

Schmidt, F. L., and Hunter, J. E. 2015. *Methods of Meta-Analysis: Correcting Error and Bias in Research Findings* (3rd ed.), Thousand Oaks, CA: SAGE Publications.

Schmidt, F. L., and Le, H. 2014. "Software for the Hunter-Schmidt Meta-Analysis Methods, Version 2.0," unpublished paper, Department of Management & Organizations, University of Iowa,

Schryen, G. 2015. "Writing Qualitative IS Literature Reviews—Guidelines for Synthesis, Interpretation, and Guidance of Research," *Communications of the Association for Information Systems* (37:12), pp. 286-325.

Schultze, R. 2007. "Current Methods for Meta-Analysis: Approaches, Issues, and Developments," *Zeitschrift für Psychologie* (*Journal of Psychology*) (215:2), pp. 90-103.

Sharma, R., and Yetton, P. 2003. "The Contingent Effects of Management Support and Task Interdependence on Successful Information Systems Implementation," *MIS Quarterly* (27:4), pp. 533-555.

Sharma, R., Yetton, P., and Crawford, J. 2009. "Estimating the Effect of Common Method Variance: The Method-Method Pair Technique with an Illustration from TAM Research," *MIS Quarterly* (33:3), pp. 473-490.

Shropshire, J., Warkentin, M., and Sharma, S. 2015. "Personality, Attitudes, and Intentions: Predicting Initial Adoption of Information Security Behavior," *Computers & Security* (49), pp. 177-191.

Silberman, M. 1976. "Toward a Theory of Criminal Deterrence," *American Sociological Review* (41:3), pp. 442-461.

Siponen, M. 2000. "A Conceptual Foundation for Organizational Information Security Awareness," *Information Management & Computer Security* (8:1), pp. 31-41.

Siponen, M., Mahmood, M. A., and Pahnila, S. 2014. "Employees' Adherence to Information Security Policies: An Exploratory Field Study," *Information & Management* (51:2), pp. 217-224.

Siponen, M., and Vance, A. 2014. "Guidelines for Improving the Contextual Relevance of Field Surveys: the Case of Information Security Policy Violations," *European Journal of Information Systems* (23:3), pp. 289-305.

Sommestad, T., and Hallberg, J. 2013. "A Review of the Theory of Planned Behaviour in the Context of Information Security Policy Compliance," in *Proceedings of the IFIP International Information Security Conference: Security and Privacy Protection in Information Systems Processing,* E. Janczewski, H. Wolf, and S. Shenoi (eds.), Berlin: Springer, pp. 257-271.

Sommestad, T., Hallberg, J., Lundholm, K., and Bengtsson, J. 2014. "Variables Influencing Information Security Policy Compliance: A Systematic Review of Quantitative Studies," *Information Management & Computer Security* (22:1), pp. 42-75.

Sommestad, T., Karlzén, H., and Hallberg, J. 2015. "A Meta-Analysis of Studies on Protection Motivation Theory and Information Security Behaviour," *International Journal of Information Security and Privacy* (9:1), pp. 26-46.

Spears, J. L., and Barki, H. 2010. "User Participation in Information Systems Security Risk Management," *MIS Quarterly* (34:3), pp. 503-522.

Sterne, J. A. C., Gavaghan, D., and Egger, M. 2000. "Publication and Related Bias in Meta-Analysis: Power of Statistical Tests and Prevalence in the Literature," *Journal of Clinical Epidemiology* (53:11), pp. 1119-1129.

Straub, D. 1986. "Deterring Compute Abuse: The Effectiveness of Deterrent Countermeasures in the Computer Security Environment," unpublished D.B.A. Thesis, Indiana University.

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

Straub, D., and Burton-Jones, A. 2007. "Veni, Vidi, Vici: Breaking the TAM Logjam," *Journal of the AIS* (8:4), pp. 223-229.

Sutton, A. J. 2006. "Evidence Concerning the Consequences of Publication and Related Biases," in *Publication Bias in Meta-Analysis: Prevention, Assessment and Adjustments,* H. R. Rothstein, A. J., Sutton and M. Borenstein (eds.), Chichester, UK: John Wiley & Sons, Ltd., pp. 175-192.

Sutton, S. G., Song, F., Gilbody, S. M., and Abrams, K. R. 2000. "Modelling Publication Bias in Meta-Analysis: A Review," *Statistical Methods in Medical Research* (9:5), pp. 421-445.

Templier, M., and Paré, G. 2015. "A Framework for Guiding and Evaluating Literature Reviews," *Communications of the AIS* (37:6), pp. 112-137.

Thatcher, J., Wright, R., Sun, H., Zagenczyk, T. J., and Klein, R. 2018. "Mindfulness in Information Technology Use: Definitions, Distinctions, and a New Measure," *MIS Quarterly* (42:3), pp. 831-847.

Theoharidou, M., Kokolakis, S., Karyda, M., and Kiountouzis, E. 2005. "The Insider Threat to Information Systems and the Effectiveness of ISO17799," *Computers & Security* (24:6), pp. 472-484.

Thomson, M. E., and von Solms, R. 1998. "Information Security Awareness: Educating Your Users Effectively," *Information Management & Computer Security* (6:4), pp. 167-173.

Tonidandel, S., and LeBreton, J. M. 2011. "Relative Importance Analyses: A Useful Supplement to Multiple Regression Analyses," *Journal of Business and Psychology* (26:1), pp. 1-9.

Tonidandel, S., and LeBreton, J. M. 2015. "RWA Web: A Free, Comprehensive, Web-Based, and User-Friendly Tool for Relative Weight Analyses," *Journal of Business and Psychology* (30:2), pp. 207-216.

Triandis, H. C. 1977. *Interpersonal Behavior*. Monterey, CA: Brooks/Cole Publishing Company.

Valentine, J. C., Piggott, T. D., and Rothstein, H. R. 2010. "How Many Studies Do You Need? A Primer on Statistical Power for Meta-Analysis," *Journal of Educational and Behavioral Statistics* (35:2), pp. 215-247.

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 AIS* (15:10), pp. 679-722.

Venkatesh, V., Morris, M. G., Davis, G. B., and Davis, F. D. 2003. "User Acceptance of Information Technology: Toward a Unified View," *MIS Quarterly* (27:3), pp. 425-478.

Viswesvaran, C., and Ones, D. S. 1995. "Theory Testing: Combining Psychometric Meta-Analysis and Structural Equations Modeling," *Personnel Psychology* (48:4), pp. 865-885.

vom Brocke, J., Simons, A., Riemer, K., Niehaves, B., and Plattfaut, R. 2015. "Standing on the Shoulders of Giants: Challenges and Recommendations of Literature Search in Information Systems Research," *Communications of the AIS* (37:9), pp. 205-224.

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* (20:3), pp. 267-284.

Webster, J., and Watson, R. T. 2002. "Analyzing the Past to Prepare for the Future: Writing a Literature Review," *MIS Quarterly* (26:2), pp. xiii-xxiii.

Whitener, E. M. 1990. "Confusion of Confidence Intervals and Credibility Intervals in Meta-Analysis," *Journal of Applied Psychology* (75:3), pp. 315-321.

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

Wood, J. A. 2008. "Methodology for Dealing with Duplicate Study Effects in a Meta-Analysis," *Organizational Research Methods* (11:1), pp. 79-95.

Workman, M., Bommer, W. H., and Straub, D. W. 2008. "Security Lapses and the Omission of Information Security Measures: A Threat Control Model and Empirical Test," *Computers in Human Behavior* (24:6), pp. 2799-2816.

Wu, J., and Du, H. 2012. "Toward a Better Understanding of Behavioral Intention and System Usage Constructs," *European Journal of Information Systems* (21:6), pp. 680-698.

Wu, J., and Lederer, A. 2009. "A Meta-Analysis of the Role of Environment-Based Voluntariness of Information Technology Acceptance," *MIS Quarterly* (33:2), pp. 419-432.

Wu, J., and Lu, X. 2013. "Effects of Extrinsic and Intrinsic Motivators on Using Utalitarian, Hedonic, and Dual-Purposed Information Systems: A Meta-Analysis," *Journal of the AIS* (14:3), pp. 153-191.

Yazdanmehr, A., and Wang, J. 2016. "Employees' Information Security Policy Compliance: A Norm Activation Perspective," *Decision Support Systems* (92), pp. 36-46.

About the Authors

W. Alec Cram is an assistant professor in the Information and Process Management Department at Bentley University. He received his Ph.D. from Queen's University. Alec previously worked as an IT Audit Manager at Deloitte, where he obtained the CISSP and CISA designations. He currently teaches undergraduate and graduate information security classes, while his research focuses on how information systems control initiatives can contribute to improving the performance of organizational processes. Alec's work has been published in outlets including *Information Systems Journal, European Journal of Information Systems, Journal of the AIS,* and *Information & Management*.

John D'Arcy is an associate professor in the Department of Accounting & MIS, Lerner College of Business and Economics, at the University of Delaware. His research focuses on the behavioral aspects of information security, with emphasis on strategies for

mitigating insider threats. Within this research program, he has investigated various individual and organizational factors that contribute to employees' security-related behavior. A separate line of his research focuses on IT security investment strategies and how they influence the likelihood of data breaches. John's research has been published in journals such as *MIS Quarterly*, *Information Systems Research*, *Journal of Management Information Systems*, *European Journal of Information Systems,* and *MIT Sloan Management Review*. He received his Ph.D. from the Fox School of Business and Management, Temple University.

Jeffrey Proudfoot is an assistant professor in the Information and Process Management Department at Bentley University. His research centers on behavioral information security with emphases on automated credibility assessment and insider threat detection. Jeff's research has been published in journals including *Journal of Management Information Systems, Journal of the AIS, European Journal of Information Systems,* and *Decision Support Systems*. Jeff has contributed to over $1 million in Department of Homeland Security, Center for Identification Technology Research, and National Science Foundation grants. His prior research affiliations include the Center for the Management of Information and the National Center for Border Security and Immigration (BORDERS), a Department of Homeland Security Center of Excellence. He received his Ph.D. from the Eller College of Management at the University of Arizona.

MIS Quarterly

RESEARCH ARTICLE

SEEING THE FOREST *AND* THE TREES: A META-ANALYSIS OF THE ANTECEDENTS TO INFORMATION SECURITY POLICY COMPLIANCE

W. Alec Cram
Bentley University, 175 Forest Street,
Waltham, MA 02452 U.S.A. {wcram@bentley.edu}

John D'Arcy
Department of Accounting and MIS, University of Delaware, 356 Purnell Hall
Newark, DE 19716 U.S.A. {jdarcy@udel.edu}

Jeffrey G. Proudfoot
Bentley University, 175 Forest Street,
Waltham, MA 02452 U.S.A. {jproudfoot@bentley.edu}

Appendix A

Included Studies

Table A1. Papers Included in the Meta-Analysis

Authors (Year)[a]	Publication Name	Publication Type	Sample Size(s)	Primary Theoretical or Conceptual Base	Antecedent Categories Examined
Abed et al. (2016)	Americas Conference on Information Systems	Conference	275	Cognitive dissonance theory, technology acceptance model, expectation confirmation theory, IS continuance model	Attitude Perceived usefulness Normative beliefs SETA
Al-Omari et al. (2013)	Hawaii International Conference on System Sciences	Conference	445	Theory of planned behavior	Attitude Normative beliefs Personal norms & ethics
Al-Omari et al. (2012a)	Americas Conference on Information Systems	Conference	878	Theory of planned behavior	Attitude Normative beliefs Self-efficacy SETA
Al-Omari et al. (2012b)	Hawaii International Conference on System Sciences	Conference	205	Theory of planned behavior, theory of reasoned action, rational choice theory, technology acceptance model	Detection certainty Normative beliefs Perceived ease of use Perceived usefulness Self-efficacy SETA

Table A1. Papers Included in the Meta-Analysis (Continued)

Authors (Year)[a]	Publication Name	Publication Type	Sample Size(s)	Primary Theoretical or Conceptual Base	Antecedent Categories Examined
Arunothong (2014)	Ph.D. Dissertation	Dissertation	613	Social exchange theory, social penetration theory	Detection certainty Punishment severity
Aurigemma and Leonard (2015)	Journal of Information Systems Security	Journal	221	Affective organizational commitment, theory of planned behavior, rational choice theory	Attitude Normative beliefs Perceived benefits Response cost Self-efficacy
Aurigemma and Mattson (2014)[d]	Americas Conference on Information Systems	Conference	239	Theory of planned behavior, deterrence theory	Attitude Punishment expectancy Punishment severity
Aurigemma and Mattson (2017a)[d]	Information & Computer Security	Journal	239	Deterrence theory, theory of planned behavior, rational choice theory	Normative beliefs Self-efficacy
Aurigemma and Mattson (2017b)[d]	Computers & Security	Journal	239	Theory of planned behavior	Attitude Normative beliefs Self-efficacy
Bauer and Bernroider (2017)	Data Base for Advances in Information Systems	Journal	97	Theory of reasoned action, neutralization theory	Attitude Normative beliefs SETA
Boss et al. (2009)	European Journal of Information Systems	Journal	1671	Social influence theory, organismic integration theory, agency theory, control theory	Detection certainty Reward
Boss et al. (2015)[b]	MIS Quarterly	Journal	104, 327	Protection motivation theory	Resource vulnerability Response cost Response efficacy Rewards[g] Self-efficacy Threat severity
Brady (2010)	Ph.D. Dissertation	Dissertation	76	Theory of reasoned action, theory of planned behavior	Organizational support Self-efficacy SETA
Bulgurcu et al. (2010)	MIS Quarterly	Journal	464	Theory of planned behavior, rational choice theory, deterrence theory	Attitude Normative beliefs Perceived benefits Punishment expectancy Rewards Response cost Resource vulnerability Self-efficacy SETA
Burns et al. (2018)	Decision Sciences	Journal	411	Expectancy theory	Attitude Self-efficacy SETA Response efficacy
Chan et al. (2005)	Journal of Information Privacy & Security	Journal	104	None noted	Organizational support Self-efficacy
Chen et al. (2016)	Journal of Computer Information Systems	Journal	231	Awareness-motivation-capability framework	Punishment severity Rewards Self-efficacy SETA

Table A1. Papers Included in the Meta-Analysis (Continued)

Authors (Year)[a]	Publication Name	Publication Type	Sample Size(s)	Primary Theoretical or Conceptual Base	Antecedent Categories Examined
Cheng et al. (2013)	Computers & Security	Journal	185	Social control, deterrence theory	Normative beliefs Personal norms & ethics Punishment expectancy Punishment severity
Cheng et al. (2014)	Computers in Human Behavior	Journal	230	Deterrence theory, neutralization theory	Detection certainty Perceived benefits Punishment severity
Chu et al. (2015)	Journal of Business Ethics	Journal	208	Theory of planned behavior	Attitude Normative beliefs Self-efficacy
D'Arcy (2005)[c]	Ph.D. Dissertation	Dissertation	238, 269	Deterrence theory	Detection certainty Punishment expectancy Punishment severity Self-efficacy SETA
D'Arcy and Greene (2014)	Information Management & Computer Security	Journal	127	Social exchange theory	Detection certainty Organizational support
D'Arcy et al. (2014)	Journal of Management Information Systems	Journal	539	Coping theory, moral disengagement theory, social cognitive theory	Personal norms & ethics Response cost
D'Arcy et al. (2018)	AIS Transactions on Replication Research	Journal	150	Moral disengagement theory, coping theory	Response cost
D'Arcy and Lowry (2019)[c]	Information Systems Journal	Journal	77, 628	Rational choice theory, theory of planned behavior	Attitude Detection certainty Normative beliefs Perceived benefits Personal norms & ethics Response cost Self-efficacy
Devgan (2012)	Ph.D. Dissertation	Dissertation	189	Theory of planned behavior	Normative beliefs Perceived ease of use Perceived usefulness Self-efficacy
Dinev and Hu (2007)	Journal of the Association for Information Systems	Journal	332	Theory of planned behavior	Attitude Normative beliefs Perceived ease of use Perceived usefulness Self-efficacy SETA
Dinev et al. (2009)	Information Systems Journal	Journal	227	Theory of planned behavior, rational choice theory, technology acceptance model, IS continuance model	Attitude Normative beliefs Perceived ease of use Perceived usefulness Self-efficacy SETA
Donalds (2015)	SIG GlobDev Pre-ECIS Workshop	Conference	137	Cybersecurity awareness and training	Organizational support SETA

Table A1. Papers Included in the Meta-Analysis (Continued)

Authors (Year)[a]	Publication Name	Publication Type	Sample Size(s)	Primary Theoretical or Conceptual Base	Antecedent Categories Examined
Dugo (2007)	Ph.D. Dissertation	Dissertation	113	Theory of planned behavior, deterrence theory	Attitude Normative beliefs Punishment expectancy Punishment severity Self-efficacy
Foth (2012)	Journal of Public Health	Journal	557	Technology acceptance model, protection motivation theory	Attitude Normative beliefs Perceived ease of use Perceived usefulness Resource vulnerability Threat severity
Goo et al. (2014)	IEEE Transactions on Professional Communication	Journal	581	Safety climate and performance model	Normative beliefs Organizational support SETA
Guo and Yuan (2012)[e]	Information & Management	Journal	306	Deterrence theory, theory of reasoned action, social cognitive theory	Attitude
Guo et al. (2011)[e]	Journal of Management Information Systems	Journal	306	Composite behavior model, theory of reasoned action, theory of planned behavior	Attitude Normative beliefs Perceived benefits Punishment expectancy Resource vulnerability
Haeussinger and Kranz (2013)	International Conference on Information Systems	Conference	475	Deterrence theory, theory of planned behavior	Normative beliefs SETA
Han et al. (2017)[c]	Computers & Security	Journal	111, 102	Rational choice theory	Perceived benefits Response cost SETA
Hanus (2014)	Ph.D. Dissertation	Dissertation	172	Threat avoidance theory, protection motivation theory	Attitude Punishment expectancy Resource vulnerability Response cost Rewards Self-efficacy SETA Threat severity
Harrington (1996)[c]	MIS Quarterly	Journal	219	Deterrence theory	Personal norms & ethics
Herath and Rao (2009a)[f]	Decision Support Systems	Journal	312	Deterrence theory, protection motivation theory	Detection certainty Normative beliefs Punishment severity Response efficacy
Herath and Rao (2009b)[f]	European Journal of Information Systems	Journal	312	Deterrence theory, agency theory	Attitude Normative beliefs Resource vulnerability Response efficacy Self-efficacy Threat severity
Herath et al. (2018)	Information Technology & People	Journal	233	Social cognitive theory	SETA

Table A1. Papers Included in the Meta-Analysis (Continued)

Authors (Year)[a]	Publication Name	Publication Type	Sample Size(s)	Primary Theoretical or Conceptual Base	Antecedent Categories Examined
Hovav and D'Arcy (2012)[c]	Information & Management	Journal	366, 360	Deterrence theory	Detection certainty Punishment expectancy Punishment severity
Hovav and Putri (2016)	Pervasive & Mobile Computing	Journal	230	Reactance theory, psychological contract theory, protection motivation theory, organizational justice theory	Response cost Response efficacy SETA
Hu et al. (2012)	Decision Sciences	Journal	148	Theory of planned behavior	Attitude Normative beliefs Organizational support Self-efficacy
Huang et al. (2016)	Pacific Asia Conference on Information Systems	Conference	234	Theory of planned behavior, social cognition theory	Self-efficacy SETA
Humaidi and Balakrishnan (2018)	Health Information Management Journal	Journal	454	Theory of planned behavior	Organizational support Self-efficacy
Hwang et al. (2017)	Online Information Review	Journal	415	Prospect theory, protection motivation theory	Normative beliefs Response cost Self-efficacy SETA
Ifinedo (2012)	Computers & Security	Journal	124	Theory of planned behavior, protection motivation theory	Attitude Normative beliefs Resource vulnerability Response cost Response efficacy Self-efficacy Threat severity
Ifinedo (2014a)	Information & Management	Journal	124	Theory of planned behavior, social cognitive theory, social bond theory	Personal norms & ethics
Ifinedo (2014b)	Mediterranean Conference on Information Systems	Conference	201	Social cognitive theory	Rewards Self-efficacy SETA
Ifinedo (2016)	Information Systems Management	Journal	176	Deterrence theory, rational choice theory, organizational climate perspective	Detection certainty Organizational support Punishment severity Response cost
Jaafar and Ajis (2013)	International Journal of Business and Social Science	Journal	400	Social cognitive theory	Organizational support Self-efficacy
Jenkins (2013)[b]	Ph.D. Dissertation	Dissertation	332, 162	Theory of planned behavior, field theory	Attitude Normative beliefs Self-efficacy
Jenkins and Durcikova (2013)	International Conference on Information Systems	Conference	194	Theory of planned behavior, dual-task interference theory	Attitude Normative beliefs Self-efficacy SETA

Table A1. Papers Included in the Meta-Analysis (Continued)

Authors (Year)[a]	Publication Name	Publication Type	Sample Size(s)	Primary Theoretical or Conceptual Base	Antecedent Categories Examined
Jenkins et al. (2010)	International Conference on Information Systems	Conference	108	Theory of planned behavior, dual-processing theory, yield shift theory, expectancy value theory	Attitude Organizational support Perceived ease of use Response Cost Self-efficacy
Jeon and Hovav (2015)[c]	HawaiiInter-national Conference on System Sciences	Conference	40, 49	Psychological ownership, rational choice theory, deterrence theory	Detection certainty Perceived benefits Response cost Self-efficacy
Johnston and Warkentin (2010)	MIS Quarterly	Journal	275	Protection motivation theory, fear appeals model	Resource vulnerability Response efficacy Self-efficacy Threat severity
Johnston et al. (2015)	MIS Quarterly	Journal	559	Protection motivation theory, deterrence theory	Punishment expectancy Punishment severity Resource vulnerability Response efficacy Self-efficacy Threat severity
Johnston et al. (2010)	Americas Conference on Information Systems	Conference	435	Social learning theory	Self-efficacy
Kam et al. (2015)[c]	European Conference on Information Systems	Conference	127, 121	Competing values framework	Normative beliefs
Kinnunen (2016)[c]	MS Thesis	Thesis	119, 111, 118, 112	Deterrence theory, protection motivation theory, stress-as-offense-to-self theory	Punishment expectancy Response cost Response efficacy Self-efficacy Threat severity
Kranz and Haeussinger (2014)	International Conference on Information Systems	Conference	444	Theory of planned behavior, organismic integration theory, self-determination theory	Attitude Normative beliefs Self-efficacy
Kuo et al. (2017)	Journal of Medical Systems	Journal	262	Deterrence theory	Detection certainty Normative beliefs Punishment expectancy Punishment severity
Lebek et al. (2014)	International Conference on Information Systems	Conference	208	Theory of planned behavior, expectancy-valence theory	Organizational support Personal norms & ethics
Lee et al. (2016)	Pacific Asia Conference on Information Systems	Conference	211	Rational choice theory	Detection certainty
Li and Luo (2017)[c]	Unpublished	Conference	265	Not noted	Personal norms & ethics Punishment expectancy Punishment severity
Li et al. (2014)	Information Systems Journal	Journal	241	Organizational justice	Punishment expectancy Punishment severity Personal norms & ethics

Table A1. Papers Included in the Meta-Analysis (Continued)

Authors (Year)[a]	Publication Name	Publication Type	Sample Size(s)	Primary Theoretical or Conceptual Base	Antecedent Categories Examined
Li, Zhang, and Sarathy (2010)	Decision Support Systems	Journal	246	Rational choice theory	Detection certainty Perceived benefits Personal norms & ethics Punishment severity Normative beliefs Resource vulnerability
Li and Cheng (2013)	Pacific Asia Conference on Information Systems	Conference	428	Rational choice theory	Detection certainty Perceived benefits Punishment severity Resource vulnerability
Liao et al. (2009)	Journal of Computer Information Systems	Journal	205	Theory of planned behavior, deterrence theory, theory of ethics	Attitude Normative beliefs Punishment expectancy Punishment severity Self-efficacy
Lowry et al. (2015)	Information Systems Journal	Journal	533	Fairness theory, reactance theory	Punishment expectancy Punishment severity SETA
Mani et al. (2015)	Americas Conference on Information Systems	Conference	105	Protection motivation theory	Resource vulnerability Response efficacy Response cost Self-efficacy Threat severity
Martinez (2015)	Ph.D. Dissertation	Dissertation	106	Theory of planned behavior	Attitude Normative beliefs Self-efficacy
Moody et al. (2018)[b]	MIS Quarterly	Journal	274, 393	Theory of reasoned action, neutralization techniques, health belief model, theory of planned behavior, theory of interpersonal behavior, protection motivation theory, deterrence theory, theory of self-regulation, extended parallel processing model, control balance theory	Attitude Normative beliefs Punishment expectancy Punishment severity Resource vulnerability Response efficacy Rewards Self-efficacy Threat severity
Moquin and Wakefield (2016)	Journal of Computer Information Systems	Journal	138	Protection motivation theory, theory of planned behavior	Attitude Normative beliefs Punishment expectancy SETA
Ormond et al. (2019)[c]	Unpublished	Unpublished	331	TBD	Attitude
Pahnila et al. (2013)[c]	Pacific Asia Conference on Information Systems	Conference	340, 173	Protection motivation theory	Resource vulnerability Response efficacy Self-efficacy Threat severity
Park et al. (2017)	Computers & Security	Journal	123	Deterrence theory	Personal norms & ethics Punishment severity SETA
Peace et al. (2003)	Journal of Management Information Systems	Journal	201	Theory of planned behavior, expected utility theory, deterrence theory	Attitude Normative beliefs Punishment expectancy Punishment severity Self-efficacy

Table A1. Papers Included in the Meta-Analysis (Continued)

Authors (Year)[a]	Publication Name	Publication Type	Sample Size(s)	Primary Theoretical or Conceptual Base	Antecedent Categories Examined
Putri and Hovav (2014)	European Conference on Information Systems	Conference	230	Reactance theory, protection motivation theory, organizational justice theory	Organizational support Response cost Response efficacy SETA Threat severity
Safa et al. (2016)	Computers & Security	Journal	296	Social bond theory, involvement theory	Attitude Personal norms & ethics SETA
Shropshire et al. (2015)	Computers & Security	Journal	170	Theory of reasoned action, technology acceptance model	Perceived ease of use Perceived usefulness
Sikolia et al. (2016)	Americas Conference on Information Systems	Conference	110	Protection motivation theory, theory of reasoned action, cognitive evaluation theory	Resource vulnerability Response efficacy Self-efficacy Threat severity
Siponen et al. (2014)	Information & Management	Journal	669	Protection motivation theory, theory of reasoned action, cognitive evaluation theory	Attitude Normative beliefs Resource vulnerability Response efficacy Rewards Self-efficacy Threat severity
Siponen and Vance (2010)	MIS Quarterly	Journal	395	Neutralization theory	Personal norms & ethics Punishment expectancy
Sommestad et al. (2015)	Information and Computer Security	Journal	306	Theory of planned behavior, protection motivation theory	Attitude Normative beliefs Resource vulnerability Response efficacy Response cost Self-efficacy Threat severity
Son (2011)	Information & Management	Journal	602	Deterrence theory, intrinsic and extrinsic motivation models	Punishment expectancy Punishment severity
Son and Park (2016)	International Journal of Information Management	Journal	209	Deterrence theory, procedural justice	Punishment expectancy Punishment severity
Talib and Dhillon (2015)	International Conference on Information Systems	Conference	290	Intrinsic motivation/ empowerment model, structural empowerment theory	Self-efficacy SETA
Vance et al. (2012)	Information & Management	Journal	210	Protection motivation theory	Resource vulnerability Response cost Response efficacy Rewards[g] Self-efficacy Threat severity
Wall et al. (2013)	Journal of Information Privacy & Security	Journal	95	Self-determination theory, psychological reactance theory	Response efficacy Self-efficacy
Warkentin et al. (2011)	European Journal of Information Systems	Journal	202	Social learning theory	Self-efficacy

Table A1. Papers Included in the Meta-Analysis (Continued)

Authors (Year)[a]	Publication Name	Publication Type	Sample Size(s)	Primary Theoretical or Conceptual Base	Antecedent Categories Examined
Yazdanmehr and Wang (2016)	Decision Support Systems	Journal	201	Norm activation theory, social norms theory	Detection certainty Normative beliefs Personal norms & ethics
Zhang et al. (2009)	Information Management & Computer Security	Journal	176	Risk compensation theory, theory of planned behavior	Attitude Normative beliefs Self-efficacy

[a]Where a conference paper or dissertation was subsequently published as a journal article using the same dataset, we excluded the earlier publication to avoid a duplication of data.

[b]Two separate studies were conducted in Boss et al. (2015); Jenkins (2013); and Moody et al. (2018). In the Boss et al. paper, the rewards category was only applicable to the second study. In the Moody et al. study, the attitude, normative beliefs, punishment severity, resource vulnerability, and self-efficacy categories were only applicable to the first study.

[c]A single study was conducted, but multiple scenarios, samples, or groupings were utilized. In Harrington (1996), five scenarios were used for the personal norms & ethics category. In Kinnunan (2016), four scenarios were used for the punishment expectancy, response cost, response efficacy, self-efficacy, and threat severity categories. In Li and Luo (2017), three scenarios were used for the personal norms & ethics, punishment expectancy, and punishment severity categories. In D'Arcy (2005) (detection certainty, punishment expectancy, punishment severity, self-efficacy, SETA), Han et al. (2017) (SETA, response cost, perceived benefits), Hovav and D'Arcy (2012) (detection certainly, punishment expectancy, punishment severity); Jeon and Hovav (2015) (detection certainty, perceived benefits, response cost, self-efficacy); Kam et al. (2015) (normative beliefs); Ormond et al. (2019) (attitude), and Pahnila et al. (2013) (resource vulnerability, response efficacy, self-efficacy, threat severity), two groupings or independent samples were used. In D'Arcy and Lowry (2019), one within-person level grouping used the attitude, normative beliefs, and response cost categories, while a second between-individual level grouping used the detection certainty, normative beliefs, perceived benefits, personal norms & ethics, and self-efficacy categories.

[d]The same sample of 239 participants was used in Aurigemma and Mattson (2014, 2017a, 2017b); however, the data utilized in our analysis was unique: the 2014 paper used compliance with a flash media policy as the dependent variable, the 2017a paper used the same dependent variable, but with some new independent variables, and the 2017b paper used a tailgating policy as the dependent variable.

[e]Guo et al. (2011) and Guo and Yuan (2012) use the same dataset, but only some of the independent variables overlap between the two studies. Where a variable is duplicated, we used the data from the 2011 paper. For the attitude category, we used data from the "attitude toward security policy" construct in the 2011 paper and the "personal self-sanctions" construct in the 2012 paper.

[f]Herath and Rao (2009a, 2009b) use the same dataset, but only some of the independent variables overlap between the two studies. Where a variable is duplicated, we used the data from the 2009a paper. For the response efficacy category, we used data from the "response efficacy" construct in the 2009b paper and the "perceived effectiveness" construct in the 2009a paper.

[g]Boss et al. (2015) and Vance et al. (2012) measure maladaptive rewards (i.e., the benefits of not complying with a security policy). The correlations for these studies were reversed to match those studies that measured rewards.

Appendix B

Excluded Papers

The listing of papers in the table below highlights publications that were excluded from our meta-analysis, including details of our rationale. Our aim is to provide transparency into our exclusion process, although we note that the listing is a representative collection of excluded papers, rather than a comprehensive listing of all excluded papers. The primary exclusion criteria noted in the "Methodology" section are reflected in the table below. We note that examples of our third exclusion criteria are separated below in terms of either "Duplicated data set" or "Did not report data for effect size calculation." Also of note is the category "Insufficient independent variable categorization," which was used during the analysis phase, when too few independent variables from a paper were also seen in other papers (thus leaving the variable uncategorized) and a meta-analysis was unable to be performed.

Table B1. Sample of Papers Excluded from the Meta-Analysis

Authors (Year)	Journal	Exclusion Criteria 1	Exclusion Criteria 2	Exclusion Criteria 3a	Exclusion Criteria 3b	Exclusion Criteria 4
Arunothong and Nazareth (2017)	Journal of Information Privacy and Security			X		
Anderson and Agarwal (2010)	MIS Quarterly	X				
Aurigemma and Mattson (2018)	Computers & Security	X				
Backhouse et al. (2006)	MIS Quarterly		X			
Balozian et al. (2019)	Journal of Computer Information Systems			X		
Baskerville et al. (2014)	Information Technology & People			X		
Bauer and Bernroider (2014)	Information Institute Conferences			X		
Belanger et al. (2017)	Information & Management			X		
Boss (2007)	PhD Dissertation				X	
Boss and Kirsch (2007)	International Conference on Information Systems				X	
Brown (2017)	PhD Dissertation			X		
Bulgurcu et al. (2009)	European and Mediterranean Conference on Information Systems					X
Burns et al. (2015)	AIS Transactions on Human-Computer Interaction			X		
Chen et al. (2012)	Journal of Management Information Systems			X		
Chen and Zahedi (2016)	MIS Quarterly	X				
Chu et al. (2018)	Journal of Business Ethics			X		
Crossler (2009)	PhD Dissertation	X				
Crossler et al. (2014)	Journal of Information Systems			X		
Crossler et al. (2017)	Journal of Information Systems					X
Culnan and Williams (2009)	MIS Quarterly		X			
D'Arcy and Devaraj (2012)	Decision Sciences				X	
D'Arcy and Hovav (2007)	Journal of Information Systems Security				X	
D'Arcy and Hovav (2009)	Journal of Business Ethics				X	
D'Arcy et al. (2009)	Information Systems Research				X	
Foth (2016)	European Journal of Information Systems			X		
Godlove (2011)	PhD Dissertation			X		
Greene and D'Arcy (2010)	Annual Symposium on Information Assurance				X	
Guo (2010)	PhD Dissertation				X	
Hamid et al. (2017)	Journal of Engineering and Applied Sciences			X		

Table B1. Sample of Papers Excluded from the Meta-Analysis (Continued)

Authors (Year)	Journal	Exclusion Criteria 1	Exclusion Criteria 2	Exclusion Criteria 3a	Exclusion Criteria 3b	Exclusion Criteria 4
Herath et al. (2014)	Information Systems Journal	X				
Hovav (2017)	Hawaii International Conference on System Sciences			X		
Hsu et al. (2015)	Information Systems Research		X			
Hu et al. (2015)	Journal of Management Information Systems			X		
Humaidi et al. (2014)	IEEE Conference on e-Learning, e-Management, and e-Services				X	
Ifinedo (2017)	SIGMIS-Computer and People Research Conference			X		
Ifinedo (2018)	Information Resources Management Journal				X	
Johnston et al. (2016)	European Journal of Information Systems			X		
Karjalainen and Siponen (2011)	Journal of the Association for Information Systems		X			
Karlsson et al. (2017)	Information & Computer Security			X		
Kim et al. (2016)	Information & Management					X
Kim et al. (2014)	The Scientific World Journal			X		
Klein and Luciano (2016)	Journal of Information Systems and Technology Management			X		
Li, Sarathy, and Zhang (2010)	International Conference on Information Systems				X	
Li (2017)	PhD Dissertation			X		
Liang and Xue (2009)	MIS Quarterly		X			
Liang and Xue (2010)	Journal of the Association for Information Systems	X				
Liang et al. (2013)	Information Systems Research		X			
Liu (2015)	European Journal of Information Systems		X			
Lowry and Moody (2015)	Information Systems Journal			X		
Lowry et al. (2014)	Journal of Business Ethics					X
Moody and Siponen (2013)	Information & Management		X			
Mutchler (2012)	PhD Dissertation	X				
Myyry et al. (2009)	European Journal of Information Systems					X
Nsoh et al. (2015)	International Journal of Strategic Information Technology and Applications			X		
Posey et al. (2013)	MIS Quarterly		X			
Shephard and Mejias (2016)	International Journal of Human-Computer Interaction			X		
Silic et al. (2017)	Information & Management			X		
Smith et al. (2010)	MIS Quarterly		X			
Spears and Barki (2010)	MIS Quarterly		X			
Straub (1990)	Information Systems Research			X		
Talib (2015)	PhD Dissertation				X	
Turel et al. (2017)	Journal of Computer Information Systems		X			
Vance et al. (2014)	Journal of the Association for Information Systems		X			
Vance et al. (2013)	Journal of Management Information Systems			X		
Vance et al. (2015)	MIS Quarterly			X		
Wall et al. (2016)	Journal of the Association for Information Systems			X		
Wall and Palvia (2013)	Americas Conference on Information Systems				X	
Warkentin, Johnston et al. (2016)	Decision Support Systems	X				

Table B1. Sample of Papers Excluded from the Meta-Analysis (Continued)

Authors (Year)	Journal	Exclusion Criteria 1	Exclusion Criteria 2	Exclusion Criteria 3a	Exclusion Criteria 3b	Exclusion Criteria 4
Warkentin, Walden et al. (2016b)	Journal of the Association for Information Systems		X			
Williams et al. (2014)	Journal of Organizational and End User Computing			X		
Willison and Backhouse (2006)	European Journal of Information Systems		X			
Willison et al. (2018)	Information Systems Journal			X		
Workman et al. (2008)	Computers in Human Behavior			X		
Workman and Gathegi (2007)	Journal for the American Society for Information Science and Technology			X		
Xue et al. (2011)	Information Systems Research		X			

Notes:
Exclusion Criteria 1: Not focused on security policy issues in an organizational context.
Exclusion Criteria 2: Dependent variable is not security policy compliance-specific.
Exclusion Criteria 3a: Did not report data for effect size calculation.
Exclusion Criteria 3b: Duplicated data set.
Exclusion Criteria 4: Insufficient independent variable categorization.

Appendix C

Independent Variable Categories in Our Meta-Analysis

Table C1. Category Definitions

Category	Definition
Attitude	The degree to which the performance of the compliance behavior is positively valued by the employee. (Bulgurcu et al. 2010)
Detection certainty[a]	The likelihood that an act of noncompliance will be detected by management. (Herath and Rao 2009b)
Normative beliefs	Belief as to whether or not a significant person wants the individual to do the behavior in question. (Herath and Rao 2009b)
Organizational support	Information security is clearly important to the organization, as viewed by the actions and communications of top management. (D'Arcy and Greene 2014)
Perceived benefits	The overall expected favorable consequences of complying with a security policy. (Han et al. 2017)
Perceived ease of use	The degree to which employees believe that complying with a security policy will be free of effort. (Foth et al. 2012)
Perceived usefulness	The degree to which employees believe that complying with a security policy will enhance their job performance. (Foth et al. 2012)
Personal norms & ethics	Personal belief about the appropriateness of a behavior. (Li et al. 2014)
Punishment expectancy[a]	An employee's perception of the probability that they will be caught if they violate a security policy. (Li et al. 2014)
Punishment severity[b]	The harshness of the sanctions that result from an act of noncompliance. (Johnston et al. 2015)
Resource vulnerability	An employee's assessment of the probability of exposure to a substantial security threat. (Herath and Rao 2009b)
Response cost	Beliefs about how costly performing the recommended response will be. (Herath and Rao 2009b)
Response efficacy	The effectiveness of a recommended coping response in reducing a security threat. (Siponen et al. 2014)
Rewards[c]	The tangible (e.g., prizes) and/or intangible (e.g., acknowledgment from a superior) compensation received by an employee in return for compliance with the security policy. (Boss et al. 2009; Bulgurcu et al. 2010; Siponen et al. 2014)
Security Education, Training, and Awareness (SETA)	Ongoing efforts to provide users with general knowledge of the information security environment, developing the skills necessary to perform any required security procedures, and promoting awareness of day-to-day security issues within the organization. (D'Arcy et al. 2009; Furnell et al. 2002; Lee and Lee 2002; Whitman et al. 2001)
Self-efficacy	Self-confidence about the ability to perform a behavior. (Herath and Rao 2009b)
Threat severity	An employee's assessment of the consequences of the security threat. (Herath and Rao 2009b)

[a]The rationale for detection certainty being a distinct category from punishment expectancy is that organizational efforts to increase the certainty of detection (e.g., security audits and computer monitoring) do not necessarily equate to increased expectations of punishment. This view is asserted in the seminal DT literature (Gibbs 1975; Tittle 1980). As well, several prior security policy compliance studies support the distinctiveness of constructs related to detection certainty versus those related to punishment perceptions (e.g., D'Arcy et al. 2009; Herath and Rao 2009a, 2009b; Ifinedo 2016; Li and Cheng 2013). Our results align with this view as the effect size for detection certainty was .10 larger than that of punishment expectancy (see Table 3) and exhibited stronger relative importance (Table 7).

[b]A small number of studies combined the measurement items for punishment certainty and punishment severity into a single construct (D'Arcy et al. 2014; D'Arcy and Lowry 2019; Herath et al. 2018; Hovav and Putri 2016). In these cases, we did not code the variable into either the punishment certainty of punishment severity category; it was ungrouped for our analysis.

[c]Included in this category is the concept of "maladaptive rewards," which refer to the rewards associated with not complying with a security policy (Boss et al. 2015; Vance et al. 2012)..

Appendix D

Moderators by Paper

Table D1. Moderator Details by Paper

Authors (Year)	Moderator #1		Moderator #2*		Moderator #3		Moderator #4**		
	Policy Compliance	Policy Violation	Actual Compliance	Intended Compliance	General Policy	Specific Policy	Asia-Pacific	Europe	North America
Abed et al. (2016)	X			X	X				
Al-Omari et al. (2013)	X			X	X				
Al-Omari et al. (2012a)	X			X	X				
Al-Omari et al. (2012b)	X			X	X				
Arunothong (2014)		X		X		X			
Aurigemma and Leonard (2015)	X			X	X				X
Aurigemma and Mattson (2014)	X			X	X				X
Aurigemma and Mattson (2017a)	X			X		X			X
Aurigemma and Mattson (2017b)	X			X		X			X
Bauer and Bernroider (2017)	X			X	X			X	
Boss et al. (2015)	X			X		X			X
Boss et al. (2009)	X		X		X				X
Brady (2010)	X			X	X				X
Bulgurcu et al. (2010)	X			X	X				X
Burns et al. (2018)	X			X	X				X
Chan et al. (2005)	X		X		X				
Chen et al. (2016)	X			X	X				X
Cheng et al. (2013)		X		X		X	X		
Cheng et al. (2014)		X		X		X	X		
*Chu et al. (2015)		X	X	X	X				
D'Arcy (2005)		X		X		X			X
D'Arcy and Greene (2014)	X			X	X				X
D'Arcy et al. (2014)		X		X		X			X
D'Arcy et al. (2018)		X		X		X			X
D'Arcy and Lowry (2019)	X		X		X				X
*Devgan (2012)	X		X	X	X		X		
Dinev and Hu (2007)	X			X		X			X
Dinev et al. (2009)	X			X		X	X		
Donalds (2015)	X		X		X				
Dugo (2007)		X		X	X				X
Foth et al. (2012)	X			X	X			X	
Goo et al. (2014)	X			X	X		X		
Guo and Yuan (2012)		X		X		X			X
Guo et al. (2011)		X		X		X			X
Haeussinger and Kranz (2013)	X			X	X				
Han et al. (2017)	X			X	X		X		

Table D1. Moderator Details by Paper (Continued)

Authors (Year)	Moderator #1		Moderator #2*		Moderator #3		Moderator #4**		
	Policy Compliance	Policy Violation	Actual Compliance	Intended Compliance	General Policy	Specific Policy	Asia-Pacific	Europe	North America
Harrington (1996)		X		X		X			X
Herath and Rao (2009a)	X			X	X				X
Herath and Rao (2009b)	X			X	X				X
Herath et al. (2018)		X		X		X	X		
Hovav and D'Arcy (2012)		X		X		X	X		X
Hovav and Putri (2016)	X			X		X	X		
Hu et al. (2012)	X			X	X				X
Huang et al. (2016)	X			X	X				
Humaidi and Balakrishnan (2018)	X		X		X		X		
Hwang et al. (2017)	X			X	X		X		
Ifinedo (2012)	X			X	X				X
Ifinedo (2014a)	X			X	X				X
Ifinedo (2014b)		X		X	X				X
Ifinedo (2016)	X			X	X				X
Jaafar and Ajis (2013)	X		X		X		X		
Jenkins (2013)	X			X		X			X
*Jenkins and Durcikova (2013)	X		X	X	X				
Jenkins et al. (2010)	X		X		X				
Jeon and Hovav (2015)	X			X	X		X		
Johnston and Warkentin (2010)	X			X		X			
Johnston et al. (2015)	X			X		X		X	
Johnston et al. (2010)	X			X	X				
Kam et al. (2015)	X		X		X		X		X
Kinnunen (2016)	X		X		X			X	
Kranz and Haeussinger (2014)	X			X	X				
Kuo et al. (2017)		X		X	X		X		
Lebek et al. (2014)	X			X	X				
Lee et al. (2016)	X			X	X		X		
Li and Luo (2017)		X		X		X			
Li et al. (2014)	X			X		X			X
Li, Zhang, and Sarathy et al. (2010)	X			X		X			
Li and Cheng (2013)		X		X		X	X		
Liao et al. (2009)		X		X		X			
Lowry et al. (2015)		X	X			X			X
Mani et al. (2015)	X			X		X	X		
Martinez (2015)	X			X	X				X
Moody et al. (2018)		X		X		X		X	
Moquin and Wakefield (2016)	X		X			X			
Ormond et al. (2019)		X		X		X			
*Pahnila et al. (2013)		X	X	X	X			X	
Park et al. (2017)		X		X	X		X		

Table D1. Moderator Details by Paper (Continued)

Authors (Year)	Moderator #1		Moderator #2*		Moderator #3		Moderator #4**		
	Policy Compliance	Policy Violation	Actual Compliance	Intended Compliance	General Policy	Specific Policy	Asia-Pacific	Europe	North America
Peace et al. (2003)		X		X		X			X
Posey et al. (2011)		X	X			X			X
Putri and Hovav (2014)	X			X		X	X		
Safa et al. (2016)	X			X	X		X		
Shropshire et al. (2015)	X			X		X			X
Sikolia et al. (2016)	X			X	X				X
*Siponen et al. (2014)	X		X	X	X			X	
Siponen and Vance (2010)		X		X		X		X	
*Sommestad et al. (2015)	X		X	X	X			X	
Son (2011)	X		X			X			X
Son and Park (2016)	X			X		X	X		
Talib and Dhillon (2015)	X			X	X				X
Vance et al. (2012)	X			X	X			X	
Wall et al. (2013)	X			X	X				X
Warkentin et al. (2011)	X			X		X			
Yazdanmehr and Wang (2016)	X			X	X				X
Zhang et al. (2009)	X			X	X				
TOTAL	**69**	**26**	**19**	**82**	**58**	**37**	**22**	**10**	**42**

* Where both actual and intended compliance are measured (i.e., Chu et al. 2015, Devgan 2012, Jenkins and Durcikova 2013, Pahnila et al. 2013, Siponen et al. 2014, Sommestad et al. 2015), our main analysis draws on the actual compliance measurements, since the intended compliance variable is employed as a proxy for actual compliance. However, both actual and intended compliance measurements are included in the analysis for Moderator #1.

**Papers with no Moderator #3 entry either (1) collected data from a location outside of Asia-Pacific, Europe, and North America; (2) no region was specified in the paper; or (3) several regions were drawn upon, but were unable to be separated for analysis.

Appendix E

Preliminary Meta-Analytic Correlation Matrix

Table E1. Preliminary (Non-Trimmed) Meta-Analytic Correlation Matrix

Category	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1. Security Policy Compliance	–																	
2. Attitude	.50 (37)	–																
3. Detection Certainty	.38 (20)	.43 (1)	–															
4. Normative Beliefs	.47 (43)	.40 (26)	.43 (5)	–														
5. Organizational Support	.45 (12)	.30 (2)	.41 (3)	.49 (2)	–													
6. Perceived Benefits	.43 (11)	.51 (2)	-.38 (5)	.31 (2)		–												
7. Perceived Ease of Use	.37 (7)	.40 (4)	.37 (1)	.26 (5)	.25 (1)		–											
8. Perceived Usefulness	.56 (7)	.64 (4)	.38 (1)	.53 (6)			.34 (6)	–										
9. Personal Norms & Ethics	.50 (20)	.28 (2)	.41 (2)	.34 (4)	.20 (1)	-.51 (1)			–									
10. Punishment Expectancy	.30 (29)	.24 (8)	.61 (5)	.40 (8)		.39 (1)			.39 (6)	–								
11. Punishment Severity	.31 (27)	.15 (5)	.49 (11)	.28 (6)	.45 (1)	-.17 (3)			.43 (7)	.59 (19)	–							
12. Resource Vulnerability	.20 (20)	.31 (7)	.51 (2)	.26 (8)		.09 (3)	.05 (1)		.06 (1)	.22 (5)	.18 (4)	–						
13. Response Cost	-.31 (25)	-.22 (5)	-.22 (3)	-.08 (6)	-.05 (3)	-.03 (6)	-.28 (1)		-.03 (1)	-.10 (6)	-.08 (1)	-.07 (8)	–					
14. Response Efficacy	.40 (24)	.42 (5)	.13 (1)	.27 (5)	.40 (1)					.18 (7)	.08 (3)	.15 (14)	-.28 (12)	–				
15. Rewards	.08 (10)	.26 (3)	.28 (1)	.14 (3)		.32 (1)				.15 (4)	.12 (2)	.06 (6)	.44 (4)	-.04 (5)	–			
16. SETA	.39 (30)	.38 (10)	.56 (3)	.39 (9)	.59 (4)	.40 (3)	.26 (3)	.44 (4)	.27 (2)	.38 (5)	.38 (5)	.36 (1)	.00 (6)	.48 (3)	.18 (3)	–		
17. Self-Efficacy	.40 (57)	.36 (24)	.05 (6)	.37 (23)	.48 (6)	.43 (4)	.58 (5)	.35 (4)	.34 (1)	.06 (13)	.01 (8)	.12 (16)	-.28 (16)	.45 (19)	.01 (8)	.38 (15)	–	
18. Threat Severity	.33 (22)	.33 (5)		.28 (5)	.22 (1)		.06 (1)	.15 (1)		.40 (8)	.02 (2)	.40 (16)	-.18 (12)	.38 (20)	-.01 (6)	.22 (1)	.23 (18)	–

Note: The number of studies/independent samples in which the relationship was tested appear in parentheses.

References[1]

*Abed, J., Dhillon, G., and Ozkan, S. 2016. "Investigating Continuous Security Compliance Behavior: Insights from Information Systems Continuance Model," in *Proceedings of the 22nd Americas Conference on Information Systems*, San Diego, CA.

*Al-Omari, A., Deokar, A., El-Gayar, O., Walters, J., and Aleassa, H. 2013. "Information Security Policy Compliance: An Empirical Study of Ethical Ideology," in *Proceedings of the 46th Hawaii International Conference on System Sciences*, Maui, HI.

*Al-Omari, A., El-Gayar, O., and Deokar, A. 2012a. "Information Security Policy Compliance: The Role of Information Security Awareness," in *Proceedings of the 18th Americas Conference on Information Systems*, Seattle, WA.

*Al-Omari, A., El-Gayar, O., and Deokar, A. 2012b. "Security Policy Compliance: User Acceptance Perspective," in *Proceedings of the 45th Hawaii International Conference on System Sciences*, Maui, HI.

Anderson, C. L., and Agarwal, R. 2010. "Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions," *MIS Quarterly* (34:3), pp. 613-643.

*Arunothong, W. 2014. "Three Research Essays on Propensity to Disclose Medical Information through Formal and Social Information Technologies," unpublished doctoral dissertation, University of Wisconsin-Milwaukee.

Arunothong, W., and Nazareth, D. L. 2017. "The Effect of Procedural and Technological Security Countermeasures on the Propensity to Misuse Medical Data," *Journal of Information Privacy and Security* (13:2), pp. 69-83.

*Aurigemma, S., and Leonard, L. 2015. "The Influence of Employee Affective Organizational Commitment on Security Policy Attitudes and Compliance Intentions," *Journal of Information System Security* (11:3), pp. 201-222.

*Aurigemma, S., and Mattson, T. 2014. "Do It or Else! Exploring the Effectiveness of Deterrence on Employee Compliance with Information Security Policies," in *Proceedings of the 20th Americas Conference on Information Systems*, Savannah, GA.

*Aurigemma, S., and Mattson, T. 2017a. "Deterrence and Punishment Experience Impacts on ISP Compliance Attitudes," *Information & Computer Security* (25:4), pp. 421-436.

*Aurigemma, S., and Mattson, T. 2017b. "Privilege or Procedure: Evaluating the Effect of Employee Status on Intent to Comply with Socially Interactive Information Security Threats and Controls," *Computers & Security* (66:-), pp. 218-234.

Aurigemma, S., and Mattson, T. 2018. "Exploring the Effect of Uncertainty Avoidance on Taking Voluntary Protective Security Actions," *Computers & Security* (73), pp. 219-234.

Backhouse, J., Hsu, C. W., and Silva, L. 2006. "Circuits of Power in Creating De Jure Standards: Shaping an International Information Systems Security Standard," *MIS Quarterly* (30:Special Issue), pp. 413-438.

Balozian, P., Leidner, D., and Warkentin, M. 2019. "Managers' and Employees' Differing Responses to Security Approaches," *Journal of Computer Information Systems* (forthcoming).

Baskerville, R., Park, E. H., and Kim, J. 2014. "An Emote Opportunity Model of Computer Abuse," *Information Technology & People* (27:2), pp. 155-181.

Bauer, S., and Bernroider, E. W. N. 2014. "An Analysis of the Combined Influences of Neutralization and Planned Behavior on Desirable Information Security Behavior," in *Information Institute Conferences,* G. Dhillon and S. Samonas (eds.), Las Vegas, NV.

*Bauer, S., and Bernroider, E. W. N. 2017. "From Information Security Awareness to Reasoned Compliant Action: Analyzing Information Security Policy Compliance in a Large Banking Organization," *The DATA BASE for Advances in Information Systems* (48:3), pp. 44-68.

Belanger, F., S., C., Enget, K., and Negangard, E. 2017. "Determinants of Early Conformance with Information Security Policies," *Information & Management* (54:7), pp. 887-901.

Boss, S. R. 2007. "Control, Perceived Risk and Information Security Precautions: External and Internal Motivations for Security Behavior," unpublished doctoral dissertation, University of Pittsburgh.

*Boss, S. R., Galletta, D., Moody, G. D., Lowry, P. B., and Polak, P. 2015. "What Do Users Have to Fear? Using Fear Appeals to Engender Threats and Fear That Motivate Protective Behaviors in Users," *MIS Quarterly* (39:4), pp. 837-864.

Boss, S. R., and Kirsch, L. J. 2007. "The Last Line of Defense: Motivating Employees to Follow Corporate Security Guidelines," in *Proceedings of the 28th International Conference on Information Systems*, Montreal, QC.

*Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., and Boss, R. W. 2009. "If Someone Is Watching, I'll Do What I'm Asked: Mandatoriness, Control, and Information Security," *European Journal of Information Systems* (18:2), pp. 151-164.

*Brady, J. W. 2010. "An Investigation of Factors That Affect HIPAA Security Compliance in Academic Medical Centers," unpublished doctoral dissertation, Nova Southeastern University.

Brown, D. 2017. "Examining the Behavioral Intention of Individuals' Compliance with Information Security Policies," unpublished doctoral dissertation, Walden University.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2009. "Roles of Information Security Awareness and Perceived Fairness in Information Security Policy Compliance," in *Proceedings of the European and Mediterranean Conference on Information Systems*, Izmir, Turkey.

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

[1]Articles used in the meta-analysis are marked with an asterisk.

*Burns, A. J., Roberts, T. L., Posey, C., Bennett, R. J., and Courtney, J. F. 2018. "Intentions to Comply Versus Intentions to Protect: A VIE Theory Approach to Understanding the Influence of Insiders' Awareness of Organizational SETA Efforts," *Decision Sciences* (49:6), pp. 1187-1228.

Burns, A. J., Young, J., Roberts, T. L., Courtney, J. F., and Ellis, T. S. 2015. "Exploring the Role of Contextual Integrity in Electronic Medical Record (EMR) System Workaround Decisions: An Information Security and Privacy Perspective," *AIS Transactions on Human–Computer Interaction* (7:3), pp. 142-165.

*Chan, M., Woon, I., and Kankanhalli, A. 2005. "Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior," *Journal of Information Privacy & Security* (1:3), pp. 18-41.

*Chen, X., Chen, L., and Wu, D. 2016. "Factors That Influence Employees' Security Policy Compliance: An Awareness-Motivation-Capability Perspective," *Journal of Computer Information Systems* (58:4), pp. 312-324.

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

Chen, Y., and Zahedi, F. M. 2016. "Individuals' Internet Security Perceptions and Behaviors: Polycontextual Contrasts Between the United States and China," *MIS Quarterly* (40:1), pp. 205-222.

*Cheng, L., Li, Y., Li, W., Holm, E., and Zhai, Q. 2013. "Understanding the Violation of IS Security Policy in Organizations: An Integrated Model Based on Social Control and Deterrence Theory," *Computers & Security* (39), pp. 447-459.

*Cheng, L., Li, W., Zhai, Q., and Smyth, R. 2014. "Understanding Personal Use of the Internet at Work: An Integrated Model of Neutralization Techniques and General Deterrence Theory," *Computers in Human Behavior* (38), pp. 220-228.

*Chu, A. M. Y., Chau, P. Y. K., and So, M. K. P. 2015. "Explaining the Misuse of Information Systems Resources in the Workplace: A Dual-Process Approach," *Journal of Business Ethics* (131:1), pp. 209-225.

Chu, M. Y., So, M. K. P., and Chung, R. S. W. 2018. "Applying the Randomized Response Technique in Business Ethics Research: The Misuse of Information Systems Resources in the Workplace," *Journal of Business Ethics* (151:1), pp. 195-212.

Crossler, R. E. 2009. "Protection Motivation Theory: Understanding the Determinants of Individual Security Behavior," unpublished doctoral dissertation, Virginia Polytechnic Institute and State University.

Crossler, R. E., Long, J. H., Loraas, T. M., and Trinkle, B. S. 2014. "Understanding Compliance with Bring Your Own Device Policies Utilizing Protection Motivation Theory: Bridging the Intention-Behavior Gap," *Journal of Information Systems* (28:1), pp. 209-226.

Crossler, R. E., Long, J. H., Loraas, T. M., and Trinkle, B. S. 2017. "The Impact of Moral Intensity and Ethical Tone Consistency on Policy Compliance," *Journal of Information Systems* (31:2), pp. 49-64.

Culnan, M. J., and Williams, C. C. 2009. "How Ethics Can Enhance Organizational Privacy: Lessons from the Choicepoint and TJX Data Breaches," *MIS Quarterly* (33:4), pp. 673-687.

*D'Arcy, J. 2005. "Security Countermeasures and Their Impact on Information Systems Misuse: A Deterrence Perspective," unpublished doctoral dissertation, Temple University.

D'Arcy, J., and Devaraj, S. 2012. "Employee Misuse of Information Technology Resources: Testing a Contemporary Deterrence Model," *Decision Sciences* (43:6), pp. 1091-1124.

*D'Arcy, J., and Greene, G. 2014. "Security Culture and the Employment Relationship as Drivers of Employees' Security Compliance," *Information Management & Computer Security* (22:5), pp. 474-489.

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

*D'Arcy, J., Herath, T., Yim, M.-S., Nam, K., and Rao, H. R. 2018. "Employee Moral Disengagement in Response to Stressful Information Security Requirements: A Methodological Replication of a Coping-Based Model," *AIS Transactions on Replication Research* (4:8), pp. 1-18.

D'Arcy, J., and Hovav, A. 2007. "Towards a Best Fit between Organizational Security Countermeasures and Information Systems Misuse Behaviors," *Journal of Information System Security* (3:2), pp. 3-30.

D'Arcy, J., and Hovav, A. 2009. "Does One Size Fit All? Examining the Differential Effects of IS Security Countermeasures," *Journal of Business Ethics* (89), pp. 59-71.

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

*D'Arcy, J., and Lowry, P. B. 2019. "Cognitive-Affective Drivers of Employees' Daily Compliance with Information Security Policies: A Multilevel, Longitudinal Study," *Information Systems Journal* (29:1), pp. 43-69.

*Devgan, V. 2012. "Satisfactions, Self-Efficacy, and Compliance in Mandatory Technology Settings," Trident University International.

*Dinev, T., and Hu, Q. 2007. "The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies," *Journal of the AIS* (8:7), pp. 386-408.

*Dinev, T., Goo, J., Hu, Q., and Nam, K. 2009. "User Behaviour Towards Protective Information Technologies: The Role of National Cultural Differences," *Information Systems Journal* (19:4), pp. 391-412.

*Donalds, C. 2015. "Cybersecurity Policy Compliance: An Empirical Study of Jamaican Government Agencies," in *Proceedings of the SIG GlobDev 2015 Pre-ECIS Workshop*, Munster, Germany.

*Dugo, T. M. 2007. "The Insider Threat to Organizational Information Security: A Structural Model and Empirical Test," unpublished doctoral dissertation, Auburn University.

Foth, M. 2016. "Factors Influencing the Intention to Comply with Data Protection Regulations in Hospitals: Based on Gender Differences in Behaviour and Deterrence," *European Journal of Information Systems* (25:2), pp. 91-109.

*Foth, M., Schusterschitz, C., and Flatscher-Thöni, M. 2012. "Technology Acceptance as an Influencing Factor of Hospital Employees' Compliance with Data-Protection Standards in Germany," *Journal of Public Health* (20:3), pp. 253-268.

Furnell, S. M., Gennatou, M., and Dowland, P. S. 2002. "A Prototype Tool for Information Security Awareness and Training," *Logistics Information Management* (15:5/6), pp. 352-357.

Gibbs, J. P. 1975. *Crime, Punishment, and Deterrence*, New York: Elsevier.

Godlove, T. 2011. "Examination of the Factors That Influence Teleworkers' Willingness to Comply with Information Security Guidelines," unpublished doctoral dissertation, University of Fairfax.

*Goo, J., Yim, M.-S., and Kim, D. J. 2014. "A Path to Successful Management of Employee Security Compliance: An Empirical Study of Information Security Climate," *IEEE Transactions on Professional Communication* (57:4), pp. 286-308.

Greene, G., and D'Arcy, J. 2010. "Assessing the Impact of Security Culture and the Employee-Organization Relationship in IS Security Compliance," in *Proceedings of the 5th Annual Symposium on Information Assurance*, Albany, NY.

Guo, K. H. 2010. "Information Systems Security Misbehavior in the Workplace: The Effects of Job Performance Expectation and Workgroup Norm," unpublished doctoral dissertation, McMaster University.

*Guo, K. H., and Yuan, Y. 2012. "The Effects of Multilevel Sanctions on Information Security Violations: A Mediating Model," *Information & Management* (49:6), pp. 320-326.

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

*Haeussinger, F. J., and Kranz, J. J. 2013. "Information Security Awareness: Its Antecedents and Mediating Effects on Security Compliant Behavior," in *Proceedings of the 34th International Conference on Information Systems*, Milan, Italy.

Hamid, H. A., Yusof, M. M., and Dali, N. R. S. M. 2017. "Security Compliance Behaviour of Saas Cloud Users: A Pilot Study," *Journal of Engineering and Applied Sciences* (12:16), pp. 4150-4155.

*Han, J., Kim, Y. J., and Kim, H. 2017. "An Integrative Model of Information Security Policy Compliance with Psychological Contract: Examining a Bilateral Perspective," *Computers & Security* (66), pp. 52-65.

*Hanus, B. T. 2014. "The Impact of Information Security Awareness of Compliance with Information Security Policies: A Phishing Perspective," unpublished doctoral dissertation, University of North Texas.

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

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* (24:1), pp. 61-84.

*Herath, T., and Rao, H. R. 2009a. "Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness," *Decision Support Systems* (47:2), pp. 154-165.

*Herath, T., and Rao, H. R. 2009b. "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organizations," *European Journal of Information Systems* (18:2), pp. 106-125.

*Herath, T., Yim, M.-S., D'Arcy, J., Kichan, N., and Raghav, H. R. 2018. "Examining Employee Security Violations: Moral Disengagement and Its Environmental Influences," *Information Technology & People* (31:6), pp. 1135-1162.

Hovav, A. 2017. "How Espoused Culture Influences Misuse Intention: A Micro-Institutional Theory Perspective," in *Proceedings of the 50th Hawaii International Conference on System Sciences*, Waikoloa, HI.

*Hovav, A., and D'Arcy, J. 2012. "Applying an Extended Model of Deterrence Across Cultures: An Investigation of Information Systems Misuse in the US and South Korea," *Information & Management* (49:2), pp. 99-110.

*Hovav, A., and Putri, F. F. 2016. "This Is My Device! Why Should I Follow Your Rules? Employees' Compliance with BYOD Security Policy," *Pervasive and Mobile Computing* (32), pp. 35-49.

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

*Hu, Q., Dinev, T., Hart, P., and Cooke, D. 2012. "Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture," *Decision Sciences* (43:4), 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* (31:4), pp. 6-48.

*Huang, H.-W., Parolia, N., and Cheng, K.-T. 2016. "Willingness and Ability to Perform Information Security Compliance Behavior: Psychological Ownership and Self-Efficacy Perspective," in *Proceedings of the Pacific Asia Conference on Information Systems*, Chiayi, Taiwan.

*Humaidi, N., and Balakrishnan, V. 2018. "Indirect Effect of Management Support on Users' Compliance Behaviour Towards Information Security Policies," *Health Information Management Journal* (47:1), pp. 17-27.

Humaidi, N., Balakrishnan, V., and Shahrom, M. 2014. "Exploring User's Compliance Behavior Towards Health Information System Security Policies Based on Extended Health Belief Model," in *Proceedings of the IEEE Conference on e-Learning, e-Management and e-Services*, Melbourne, Australia.

*Hwang, I., Kim, D., Kim, T., and Kim, S. 2017. "Why Not Comply with Information Security? An Empirical Approach for the Causes of Non-Compliance," *Online Information Review* (41:1), pp. 2-18.
*Ifinedo, P. 2012. "Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory," *Computers & Security* (31:1), pp. 83-95.
*Ifinedo, P. 2014a. "Information Systems Security Policy Compliance: An Empirical Study of the Effects of Socialisation, Influence, and Cognition," *Information & Management* (51:1), pp. 69-79.
*Ifinedo, P. 2014b. "Socal Cognitiv Determinants of Non-Malicious, Counterproductive Computer Security Behaviors: An Empirical Analysis," in *Proceedings of the Mediterranean Conference on Information Systems*, Verona, Italy.
*Ifinedo, P. 2016. "Critical Times for Organizations: What Should Be Done to Curb Workers' Noncompliance with IS Security Policy Guidelines?," *Information Systems Management* (33:1), pp. 30-41.
Ifinedo, P. 2017. "Effects of Organization Insiders' Self-Control and Relevant Knowledge on Participation in Information Systems Security Deviant Behavior," in *Proceedings of the SIGMIS-Computers and People Research Conference*, Bangalore, India.
Ifinedo, P. 2018. "Roles of Organizational Climate, Social Bonds, and Perceptions of Security Threats on IS Security Policy Compliance Intentions," *Information Resources Management Journal* (31:1), pp. 53-82.
*Jaafar, N. I., and Ajis, A. 2013. "Organizational Climate and Individual Factors Effects on Information Security Compliance Behaviour," *International Journal of Business and Social Science* (4:10), pp. 118-130.
*Jenkins, J. L. 2013. "Alleviating Insider Threats: Mitigation Strategies and Detection Techniques," unpublished doctoral dissertation, University of Arizona.
*Jenkins, J. L., and Durcikova, A. 2013. "What, I Shouldn't Have Done That? The Influence of Training and Just-in-Time Reminders on Secure Behavior," in *Proceedings of the 34th International Conference on Information Systems*, Milan, Italy.
*Jenkins, J. L., Durcikova, A., Ross, G., and Nunamaker Jr., J. F. 2010. "Encouraging Users to Behave Securely: Examining the Influence of Technical, Managerial, and Educational Controls on Users' Secure Behavior," in *Proceedings of the 31st International Conference on Information Systems*, St. Louis, MO.
*Jeon, S.-H., and Hovav, A. 2015. "Empowerment or Control: Reconsidering Employee Security Policy Compliance in Terms of Authorization," in *Proceedings of the 48th Hawaii International Conference on System Sciences*, Kauai, HI.
*Johnston, A. C., and Warkentin, M. 2010. "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly* (34:3), pp. 549-566.
Johnston, A. C., Warkentin, M., Mcbride, M., and Carter, L. 2016. "Dispositional and Situational Factors: Influences on Information Security Policy Violations," *European Journal of Information Systems* (25:3), pp. 231-251.
*Johnston, A. C., Warkentin, M., and Siponen, M. 2015. "An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset through Sanctioning Rhetoric," *MIS Quarterly* (39:1), pp. 113-134.
*Johnston, A. C., Wech, B., Jack, E., and Beavers, M. 2010. "Reigning in the Remote Employee: Applying Social Learning Theory to Explain Information Security Policy Compliance Attitudes," in *Proceedings of the 16th Americas Conference on Information Systems*, Lima, Peru.
*Kam, H.-J., Katerattanakul, P., and Hong, S.-G. 2015. "A Tale of Two Cities: Policy Compliance of the Banks in the United States and South Korea," in *Proceedings of the European Conference on Information Systems*, Münster, Germany.
Karjalainen, M., and Siponen, M. 2011. "Toward a New Meta-Theory for Designing Information Systems (IS) Security Training Approaches," *Journal of the AIS* (12:8), pp. 518-555.
Karlsson, F., Karlsson, M., and Åström, J. 2017. "Measuring Employees' Compliance—The Importance of Value Pluralism," *Information & Computer Security* (25:3), pp. 279-299.
Kim, J., Park, E. H., and Baskerville, R. 2016. "A Model of Emotion and Computer Abuse," *Information & Management* (53:1), pp. 91-108.
Kim, S. H., Yang, K. H., and Park, S. 2014. "An Integrative Behavioral Model of Information Security Policy Compliance," *The Scientific World Journal* (2014), pp. 1-12.
*Kinnunen, S. 2016. "Exploring Determinants of Different Information Security Behaviors," unpublished doctoral dissertation, University of Jyväskylä.
Klein, R. H., and Luciano, E. M. 2016. "What Influences Information Security Behavior? A Study with Brazilian Users," *Journal of Information Systems and Technology Management* (13:3), pp. 479-496.
*Kranz, J. J., and Haeussinger, F. J. 2014. "Why Deterrence Is Not Enough: The Role of Endogenous Motivations on Employees' Information Security Behavior," in *Proceedings of the 35th International Conference on Information Systems*, Auckland, New Zealand.
*Kuo, K.-M., Talley, P. C., Hung, M.-C., and Chen, Y.-L. 2017. "A Deterrence Approach to Regulate Nurses' Compliance with Electronic Medical Records Privacy Policy," *Journal of Medical Systems* (41:198), pp. 1-10.
*Lebek, B., Guhr, N., and Breitner, M. H. 2014. "Transformational Leadership and Employees' Information Security Performance: The Mediating Role of Motivation and Climate," in *Proceedings of the 35th International Conference on Information Systems*, Auckland, New Zealand.
*Lee, H., Jeon, S., and Zeelim-Hovav, A. 2016. "Impact of Psychological Empowerment, Position and Awareness of Audit on Information Security Policy Compliance Intention," in *Proceedings of the Pacific Asia Conference on Information Systems*, Chiayi, Taiwan.
Lee, J., and Lee, Y. 2002. "A Holistic Model of Computer Abuse within Organizations," *Information Management & Computer Security* (10:2), pp. 57-63.

*Li, H., and Luo, X. 2017. "The Role of Situational Moral Judgment and Deterrence on Information Security Policy Violation," in *Proceedings of 1st International Conference on Internet Plus, Big Data & Business Innovation*, Beijing, China.
Li, H., Sarathy, R., and Zhang, J. 2010. "Understanding Compliance with Internet Use Policy: An Integrative Model Based on Command-and-Control and Self-Regulatory Approaches," in *Proceedings of the 31st First International Conference on Information Systems*, St. Louis, MO.
*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* (24:6), pp. 479-502.
*Li, H., Zhang, J., and Sarathy, R. 2010. "Understanding Compliance with Internet Use Policy from the Perspective of Rational Choice Theory," *Decision Support Systems* (48:4), pp. 635-645.
*Li, W., and Cheng, L. 2013. "Effects of Neutralization Techniques and Rational Choice Theory on Internet Abuse in the Workplace," in *Proceedings of the Pacific Asia Conference on Information Systems*, Jeju Island, South Korea.
Li, Y. 2017. "Information Security Research: External Hacking, Insider Breach, and Profound Technologies," unpublished doctoral dissertation, Iowa State University.
Liang, H., and Xue, Y. 2009. "Avoidance of Information Technology Threats: A Theoretical Perspective," *MIS Quarterly* (33:1), pp. 71-90.
Liang, H., and Xue, Y. 2010. "Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective," *Journal of the AIS* (11:7), pp. 394-413.
Liang, H., Xue, Y., and Wu, L. 2013. "Ensuring Employees' IT Compliance: Carrot or Stick?," *Information Systems Research* (24:2), pp. 279-294.
*Liao, Q., Gurung, A., Luo, X., and Li, L. 2009. "Workplace Management and Employee Misuse: Does Punishment Matter?," *Journal of Computer Information Systems* (50:2), pp. 49-59.
Liu, C.-C. 2015. "Types of Employee Perceptions of Information Security Using Q Methodology: An Empirical Study," *European Journal of Information Systems* (10:4), pp. 557-575.
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* (25:5), pp. 465-488.
*Lowry, P. B., Posey, C., Bennett, R. 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* (25:3), pp. 193-230.
Lowry, P. B., Posey, C., Roberts, T. L., and Bennett, R. J. 2014. "Is Your Banker Leaking Your Personal Information? The Roles of Ethics and Individual-Level Cultural Characteristics in Predicting Organizational Computer Abuse," *Journal of Business Ethics* (121:3), pp. 385-401.
*Mani, D., Heravi, A., Mubarak, S., and Choo, K.-K. R. 2015. "Employees' Intended Information Security Behaviour in Real Estate Organisations: A Protection Motivation Perspective," in *Proceedings of the 21st Americas Conference on Information Systems*, Fajardo, Puerto Rico.
*Martinez, A. M. 2015. "Antecedents of Employee Participation in Internal Control Design and Intent to Comply with Information System Security Policies," unpublished doctoral dissertation, Capella University.
Moody, G. D., and Siponen, M. 2013. "Using the Theory of Interpersonal Behavior to Explain Non-Work-Related Personal Use of the Internet at Work," *Information & Management* (50:6), pp. 322-335.
*Moody, G. D., Siponen, M., and Pahnila, S. 2018. "Toward a Unified Model of Information Security Policy Compliance," *MIS Quarterly* (42:1), pp. 285-331.
*Moquin, R., and Wakefield, R. L. 2016. "The Roles of Awareness, Sanctions, and Ethics in Software Compliance," *The Journal of Computer Information Systems* (56:3), pp. 261-270.
Mutchler, L. A. 2012. "Expanding Protection Motivation Theory: The Role of Individual Experience in Information Security Policy Compliance," unpublished doctoral dissertation, Mississippi State University.
Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., and Vance, A. 2009. "What Levels of Moral Reasoning and Values Explain Adherence to Information Security Rules? An Empirical Study," *European Journal of Information Systems* (18:2), pp. 126-139.
Nsoh, M. W., Hargiss, K., and Howard, C. 2015. "Information Systems Security Policy Compliance: An Analysis of Management Employee Interpersonal Relationship and the Impact on Deterrence," *International Journal of Strategic Information Technology and Applications* (6:2), pp. 12-39.
*Ormond, D., Warkentin, M., and Crossler, R. E. 2019. "Integrating Cognition with an Affective Lens to Better Understand Information Security Policy Compliance," *Journal of the Association for Information Systems* (forthcoming).
*Pahnila, S., Karjalainen, M., and Siponen, M. 2013. "Information Security Behavior: Towards Multi-Stage Models," in *Proceedings of the Pacific Asia Conference on Information Systems*, Jeju Island, South Korea.
*Park, E. H., Kim, J., and Park, Y. S. 2017. "The Role of Information Security Learning and Individual Factors in Disclosing Patients' Health Information," *Computers & Security* (65:-), pp. 64-76.
*Peace, A. G., Galletta, D. F., and Thong, J. Y. L. 2003. "Software Piracy in the Workplace: A Model and Empirical Test," *Journal of Management Information Systems* (20:1), pp. 153-177.
*Posey, C., Bennett, R. J., Roberts, T. L., and Lowry, P. B. 2011. "When Computer Monitoring Backfires: Privacy Invasions and Organizational Injustice as Precursors to Computer Abuse," *Journal of Information System Security* (7:1), pp. 24-47.

Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., and Courtney, J. F. 2013. "Insiders' Protection of Organizational Information Assets: Development of a Systematics-Based Taxonomy and Theory of Diversity for Protection-Motivated Behaviors," *MIS Quarterly* (37:4), pp. 1189-1210.

*Putri, F. F., and Hovav, A. 2014. "Employees' Compliance with BYOD Security Policy: Insights from Reactance, Organizational Justice, and Protection Motivation Theory," in *Proceedings of the 22nd European Conference on Information Systems*, Tel Aviv, Israel.

*Safa, N. S., Von Solms, R., and Furnell, S. 2016. "Information Security Policy Compliance Model in Organizations," *Computers & Security* (56:1), pp. 70-82.

Shephard, M. M., and Mejias, R. J. 2016. "Nontechnical Deterrence Effects of Mild and Severe Internet Use Policy Reminders in Reducing Employee Internet Abuse," *International Journal of Human-Computer Interaction* (32:7), pp. 557-567.

*Shropshire, J., Warkentin, M., and Sharma, S. 2015. "Personality, Attitudes, and Intentions: Predicting Initial Adoption of Information Security Behavior," *Computers & Security* (49), pp. 177-191.

*Sikolia, D., Twitchell, D., and Sagers, G. 2016. "Employees' Adherence to Information Security Policies: A Partial Replication," in *Proceedings of the 22nd Americas Conference on Information Systems*, San Diego, CA.

Silic, M., Barlow, J. B., and Back, A. 2017. "A New Perspective on Neutralization and Deterrence: Predicting Shadow IT Usage," *Information & Management* (54:8), pp. 1023-1037.

*Siponen, M., Mahmood, M. A., and Pahnila, S. 2014. "Employees' Adherence to Information Security Policies: An Exploratory Field Study," *Information & Management* (51:2), pp. 217-224.

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

Smith, S., Winchester, D., Bunker, D., and Jamieson, R. 2010. "Circuits of Power: A Study of Mandated Compliance to an Information Systems Security "De Jure" Standard in a Government Organization," *MIS Quarterly* (34:3), pp. 463-486.

*Sommestad, T., Karlzén, H., and Hallberg, J. 2015. "The Sufficiency of the Theory of Planned Behavior for Explaining Information Security Policy Compliance," *Information and Computer Security* (23:2), pp. 200-217.

*Son, J.-Y. 2011. "Out of Fear or Desire? Toward a Better Understanding of Employees' Motivation to Follow IS Security Policies," *Information & Management* (48:7), pp. 296-302.

*Son, J.-Y., and Park, J. 2016. "Procedural Justice to Enhance Compliance with Non-Work-Related Computing (NWRC) Rules: Its Determinants and Interaction with Privacy Concerns," *International Journal of Information Management* (36:3), pp. 309-321.

Spears, J. L., and Barki, H. 2010. "User Participation in Information Systems Security Risk Management," *MIS Quarterly* (34:3), pp. 503-522.

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

Talib, Y. Y. A. 2015. "Intrinsic Motivation and Information Systems Security Policy Compliance in Organizations," unpublished doctoral dissertation, Virginia Commonwealth University.

*Talib, Y. Y. A., and Dhillon, G. 2015. "Employee ISP Compliance Intentions: An Empirical Test of Empowerment," in *Proceedings of the 36th International Conference of Information Systems*, Fort Worth, TX.

Tittle, C. R. 1980. *Sanctions and Social Deviance: The Question of Deterrence*, New York: Praeger.

Turel, O., Xu, Z., and Guo, K. 2017. "Organizational Citizenship Behavior Regarding Security: Leadership Approach Perspective," *Journal of Computer Information Systems* (Forthcoming:-), pp. 1-15.

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 AIS* (15:10), pp. 679-722.

Vance, A., Lowry, P. B., and Eggett, D. 2013. "Using Accountability to Reduce Access Policy Violations in Information Systems," *Journal of Management Information Systems* (29:4), pp. 263-289.

Vance, A., Lowry, P. B., and Eggett, D. 2015. "Increasing Accountability through User-Interface Design Artifacts: A New Approach to Addressing the Problem of Access-Policy Violations," *MIS Quarterly* (39:2), pp. 345-366.

*Vance, A., Siponen, M., and Pahnila, S. 2012. "Motivating IS Security Compliance: Insights from Habit and Protection Motivation Theory," *Information & Management* (49:3-4), pp. 190-198.

Wall, J. D., Lowry, P. B., and Barlow, J. B. 2016. "Organizational Violations of Externally Governed Privacy and Security Rules: Explaining and Predicting Selective Violations under Conditions of Strain and Excess," *Journal of the AIS* (17:1), pp. 39-76.

Wall, J. D., and Palvia, P. 2013. "Control-Related Motivations and Information Security Policy Compliance: The Effect of Reflective and Reactive Autonomy," in *Proceedings of the 19th Americas Conference on Information Systems*, Chicago, IL.

*Wall, J. D., Palvia, P., and Lowry, P. B. 2013. "Control-Related Motivations and Information Security Policy Compliance: The Role of Autonomy and Efficacy," *Journal of Information Privacy and Security* (9:4), pp. 52-79.

*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* (20:3), pp. 267-284.

Warkentin, M., Johnston, A. C., Shropshire, J., and Barnett, W. D. 2016. "Continuance of Protective Security Behavior: A Longitudinal Study," *Decision Support Systems* (92), pp. 25-35.

Warkentin, M., Walden, E., Johnston, A. C., and Straub, D. W. 2016. "Neural Correlates of Protection Motivation for Secure IT Behaviors: An fMRI Examination," *Journal of the AIS* (17:3), pp. 194-215.

Whitman, M. E., Townsend, A. M., and Aalberts, R. J. 2001. "Information Systems Security and the Need for Policy," in *Information Security Management: Global Challenges in the New Millennium,* G. Dhillon (ed.),Hershey PA: IGI Global, pp. 10-20.

Williams, C. K., Wynn, D., Madupalli, R., Karahanna, E., and Duncan, B. K. 2014. "Explaining Users' Security Behaviors with the Security Belief Model," *Journal of Organizational and End User Computing* (26:3), pp. 23-46.

Willison, R., and Backhouse, J. 2006. "Opportunities for Computer Abuse: Considering Systems Risk from the Offender's Perspective," *European Journal of Information Systems* (15:4), pp. 403-414.

Willison, R., Warkentin, M., and Johnston, A. C. 2018. "Examining Employee Computer Abuse Intentions: Insights from Justice, Deterrence and Neutralization Perspectives," *Information Systems Journal* (28:2), pp. 266-293.

Workman, M., Bommer, W. H., and Straub, D. W. 2008. "Security Lapses and the Omission of Information Security Measures: A Threat Control Model and Empirical Test," *Computers in Human Behavior* (24:6), pp. 2799-2816.

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* (58:2), pp. 212-222.

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

*Yazdanmehr, A., and Wang, J. 2016. "Employees' Information Security Policy Compliance: A Norm Activation Perspective," *Decision Support Systems* (92:-), pp. 36-46.

*Zhang, J., Reithel, B. J., and Li, H. 2009. "Impact of Perceived Technical Protection on Security Behaviors," *Information Management & Computer Security* (17:4), pp. 330-340.