European Journal of Information Systems (2017)

www.palgrave.com/journals

LITERATURE REVIEW

Organizational information security policies: a review and research framework

W. Alec Cram[1], Jeffrey G. Proudfoot[1] and John D'Arcy[2]

[1] *Bentley University, 175 Forest Street, Waltham, MA 02452, USA;* [2] *University of Delaware, 220 Purnell Hall, Newark, DE 19716, USA*

Correspondence: W. Alec Cram, Bentley University, 175 Forest Street, Waltham, MA 02452, USA.
Tel: 781.891.2811;
E-mail: wcram@bentley.edu

Abstract

A major stream of research within the field of information systems security examines the use of organizational policies that specify how users of information and technology resources should behave in order to prevent, detect, and respond to security incidents. However, this growing (and at times, conflicting) body of research has made it challenging for researchers and practitioners to comprehend the current state of knowledge on the formation, implementation, and effectiveness of security policies in organizations. Accordingly, the purpose of this paper is to synthesize what we know and what remains to be learned about organizational information security policies, with an eye toward a holistic understanding of this research stream and the identification of promising paths for future study. We review 114 influential security policy-related journal articles and identify five core relationships examined in the literature. Based on these relationships, we outline a research framework that synthesizes the construct linkages within the current literature. Building on our analysis of these results, we identify a series of gaps and draw on additional theoretical perspectives to propose a revised framework that can be used as a basis for future research.
European Journal of Information Systems (2017).
doi:10.1057/s41303-017-0059-9

Keywords: information security; policy; security policy; compliance; literature review; research framework

Introduction

Information security remains a critical activity within today's organizations in light of continued data breaches, systems outages, and malicious software (PwC, 2016; Verizon, 2016). Although outside factors (e.g., external hackers, natural disasters) pose a significant threat to the security of an organization's information and technology resources, the actions of employees are often viewed as being a greater security risk (Willison and Warkentin, 2013). A fundamental approach to address the risks associated with such insiders is the adoption of information security policies (hereafter, security policies), which specify the standards, boundaries, and responsibilities for users of information and technology resources in order to facilitate the prevention, detection, and response to security incidents (Bulgurcu *et al*, 2010; Lowry & Moody, 2015). However, security issues originating from employee actions remain a persistent problem for today's organizations (Johnston *et al*, 2016), including recent examples at Morgan Stanley and Gillette (Schmerken, 2015; Weldon, 2015).

As a result, organizations have placed an increasing reliance on security policies, developed in part to guide employee compliance with external regulations such as the Sarbanes–Oxley (SOX) Act, The Health Insurance Portability and Accountability Act (HIPAA), The Payment Card Industry

Special Issue Editors:
Paul Benjamin Lowry, Tamara Dinev, Robert Willison

Received: 22 January 2016
Last Revised: 30 May 2017
Accepted: 14 June 2017

Data Security Standard (PCI DSS), and the European Union Data Protection Directive (EU DPD) (Kiel *et al*, 2016; King and Raja, 2012; Koops, 2014; Wall *et al*, 2016). As well, the reputational, financial, and legal implications of information security incidents have motivated organizations to implement detailed policies related to topics including access controls and authorization, data classification, data storage, and virus protection (Siponen, 2006; Spears & Barki, 2010; Wiant, 2005). The information systems (IS) security academic research community has followed suit, having published a substantial number of articles on the formation, implementation, and effectiveness of security policies in organizations. Growth in this research stream is evidenced by a number of scholarly review articles (see Appendix A for details), which include classifications of security policy studies within the broader IS security literature (Siponen and Oinas-Kukkonen, 2007; Siponen *et al*, 2008; Soomro *et al*, 2016; Zafar & Clark, 2009), as well as more granular reviews that focus on subsets of the security policy literature, including security awareness, culture, and compliance (Guo, 2013; Karlsson *et al*, 2015; Lebek *et al*, 2014). In particular, the subject of employees' security policy compliance has garnered much attention, with reviews that provide taxonomies of this behavior (Guo, 2013), meta-analyze its antecedents (Sommestad *et al*, 2014), dissect its theoretical and philosophical underpinnings (D'Arcy and Herath, 2011; Lebek *et al*, 2014; Wall *et al*, 2015), and discuss pertinent methodological and research issues (Crossler *et al*, 2013; Siponen & Vance, 2014; Willison and Warkentin, 2013).

Taken as a collective, the findings presented in the security policy literature have made it difficult for academics and practitioners to comprehend the current state of knowledge in the domain. In particular, whether focused on the categorization of security policy studies within the broader IS security literature, or a particular security policy-related issue or topic (e.g., security compliance, security policy design, theoretical/methodological reviews), the extant reviews of the security policy literature are largely descriptive in nature and do not include a substantive analysis of the high-level themes and interrelationships that exist within this body of work. Furthermore, the extant reviews have yet to consider a process life cycle approach toward understanding how the array of security policy-related foci ultimately influence organizational security objectives, which may be a function of the preponderance of variance-based studies of security policies.

With this in mind, we submit that it is time to take stock of the security policy literature and provide an updated, overarching representation of this work. Accordingly, the objective of this research is to synthesize what we know and what remains to be learned about security policies in organizations. Specifically, we pose the following research question: *how can security policy research be synthesized into a framework that explains the key construct relationships, identifies knowledge gaps, and highlights future research directions?* Our approach draws on Rowe's (2014) concept of a literature review for understanding, which aims to synthesize a stream of research, identify problems, gaps, and research opportunities within it, and provide a foundation for future theorizing. We draw on a total of 114 security policy-related publications from 34 journals (see Appendix A and B for a complete listing) using a systematic approach to create an initial research framework that synthesizes current research and identifies gaps, as well as a revised framework that highlights future research directions.

Our results identify ten unique constructs and five sets of relationships that are examined in the security policy literature: (1) influences on the design and implementation of policies (e.g., standards and guidelines); (2) the influence of security policies on the organization (e.g., security culture) and individual employees (e.g., socioemotional well-being); (3) the influence of the organization and individual employee factors on policy compliance (e.g., dispositional traits, sanctions, rewards); (4) the influence of policy compliance on organizational objectives (e.g., the frequency of security incidents); and (5) adjustments to policy design (e.g., policy updating and maintenance). Among these, we find that the vast majority of research is oriented around understanding the drivers of security policy compliance and that relatively few studies consider how and why security policies are designed and implemented, how security policy compliance actually drives overall performance of an organization's security program, and how security policies are adapted over time. As we delineate in our research framework, we view these less-studied aspects of security policies as influential toward organizational security objectives and thus worthy of additional research.

This study makes important contributions to research and practice. First, by extending prior descriptive and granular reviews of the security policy literature, our findings synthesize patterns, insights, and inconsistencies from across a broad range of IS security research to develop a research framework that outlines both influences on and consequences of security policies. The results draw primarily from positivist foundations within the security policy literature to articulate what we know about security policies in organizations and thus can inform practitioners on how to more effectively design, implement, and oversee security policies in order to prevent and detect future incidents. As well, our framework defines the core constructs of security policy research and highlights the trends from existing studies. This synthesis represents a comprehensive view of the state of security policy research, highlighting the areas of focus within the field, as well as identifying areas that are less understood. Our proposal for future research provides specific guidance for addressing the gaps existing in the current research, as well as the application of supplementary theoretical lenses that can provide new insights into security policy construct relationships. Finally, our research framework delineates both a

temporal process by which security polices influence organizational security objectives, and categories of contributing factors at points in time. In this manner, we provide an important building block for future theory building efforts that bring both process and variance perspectives to the study of security policies in organizations.

We begin by providing an overview of the terminology used in security policy research, a brief history of research in the field, and an introduction to the theoretical bases associated with security policy studies. Next, we outline our research methodology in terms of scope, boundaries, paper selection criteria, and analysis approach. Our results are then presented by first introducing the core constructs and relationships that emerge from our analysis, followed by our research framework. We provide a relationship-by-relationship summary of key insights from the literature, as well as identified gaps and inconsistencies. Finally, the implications of our results are discussed, including a revised research framework that outlines a series of future research directions.

Conceptual foundations

Research indicates that most organizations have some type of security policy in place (Goel and Chengalur-Smith, 2010). However, security policies differ greatly among organizations depending on the value and sensitivity of the information and technology resources to be protected, as well as the potential implications of damage, modification, or disclosure of the information to the organization (Landoll, 2016; Whitman *et al*, 2001). As the term "security policy" varies in meaning depending on the context of its usage, the literature espouses numerous definitions and related concepts. A common classification is the following three-level division of security policies (Baskerville and Siponen, 2002; Whitman, 2008): at the highest level is the enterprise information security policy, or what is known as the security program policy. This executive-level document is not a policy per se, but rather top management's articulation of the organization's strategic direction, scope, and tone for all security efforts (Dhillon, 1997; Whitman, 2008). Enterprise information security policies are philosophical in nature and guide the development, implementation, and management of the security program, as well as assign responsibilities for the various areas of security. A key motivation for an enterprise information security policy is to ensure compliance with regulatory requirements by exhibiting evidence of a comprehensive security program (Whitman, 2008).

Moving down a level are the issue-specific security policies that address specific areas of technology, such as the use of e-mail, the Internet, or social media; the configuration of employee workstations; use of personal equipment on organizational networks; and prohibitions against hacking or testing organizational security controls, to name a few. Issue-specific security policies include the guidelines and procedures (i.e., acceptable use policies) that employees must adhere to in their daily interactions with information and technology resources and describe penalties for non-compliance and other undesirable computing behaviors. Because these policies describe employees' roles and responsibilities in operational terms, they are most often associated with the term security policy in the research literature and hence have received the bulk of scholarly attention. For example, studies of the drivers of employees' security compliance have described security policies as "established rules that address specific security issues by providing instructions to the employees as to what they should do when they interact with the information and technology resources of their organization" (Bulgurcu *et al*, 2010, p. 527) and as "a set of formalized procedures, guidelines, roles and responsibilities to which employees are required to adhere to safeguard and use properly the information and technology resources of their organizations" (Lowry & Moody, 2015, p. 434).

At the lowest level are the technical security policies that relate to the security architecture of technological systems. Unlike enterprise and issue-specific security policies, technical security policies (also known as automated security polices; Baskerville and Siponen, 2002) are not formalized as written documents, distributed to users, and agreed upon. Instead, technical security policies combine standards and procedures with the configuration or maintenance of a system. Common examples include access control lists which define whether users may or may not access a particular system, as well as firewall rulesets which designate the flow of network traffic into and out of an organization (Goel and Chengalur-Smith, 2010; Whitman, 2008).

In line with the literature reviewed for this study, we associate the term security policy with its non-technical, organizational variant and focus primarily on the operational level, issue-specific security policies that are described above. Technical security policies are a computer security (as opposed to information security) topic and as such are generally investigated within more technical research communities (Dhillon and Backhouse, 2001). Similar to other authors (e.g., Dhillon, 1997), we view enterprise information security policies as a proxy for an organization's overall information security strategy; this area is also beyond the scope of our study.

Security policy research overview

Turning to the scholarly literature on security policies, as noted at the outset, much of the research to date has focused on the individual and organizational drivers of employees' security policy compliance. To gain an understanding of the progression of this research stream, we first briefly introduce those studies that have assessed negative computing behaviors in organizational contexts (e.g., computer abuse, IS misuse, unethical computer use). This is worthwhile because many of the negative behaviors investigated in these studies were not explicitly

labeled as security policy non-compliance, yet exhibit at least some shared elements of policy-relevant behavior based on today's standards. We recognize that security policies were not as prevalent at the time of some of these studies, which may partially explain the exclusion of the security policy labeling for their behaviors of interest.

A number of empirical studies within the IS ethics literature have utilized ethical behavioral models to predict a broad array of unacceptable, inappropriate, illegal, and/or unethical uses of IS in the workplace (Cronan and Douglas, 2006). These studies often incorporate elements from the theory of reasoned action, theory of planned behavior, and theories of moral reasoning and development, along with additional individual and situational characteristics. Among the key variables that have been shown to predict unethical IS behavior are attitude, personal normative beliefs, ego strength, moral judgment, and perceived ethical importance (Banerjee *et al*, 1998; Chatterjee *et al*, 2015; Moores and Chang, 2006; Peace *et al*, 2003; Thong and Yap, 1998).

Outside of the IS ethics literature, various studies have investigated computer abuse and misuse of IS resources as their behaviors of interest. As the terms *abuse* and *misuse* are more synonymous with negative computing behaviors that are intentionally disruptive to IS security, these studies have focused on the predictive influence of disincentives or sanctions rooted in deterrence theory. Deterrence theory predicts that the greater the perceived certainty, severity, and swiftness of sanctions for an illicit act, the more individuals are deterred from that act (D'Arcy and Herath, 2011). IS security scholars have used deterrence theory to frame a number of early studies of security-related behavior (refer to Appendix F to view the frequency with which deterrence theory has been used in the papers included in this review); indeed, Siponen *et al* (2008) reviewed the IS security literature for the period 1990–2004 and found deterrence theory as the single most cited theory. The seminal study in this area comes from Straub (1990), who used investment in security countermeasures (e.g., security policies, technical controls) as proxies for perceived certainty and severity of formal sanctions; he found that the use of countermeasures was associated with reduced incidences of computer abuse. More contemporary work has explored extended deterrence models that consider security countermeasures (e.g., user awareness of security policies, awareness programs, and computer monitoring) as antecedents to sanction perceptions, as well as the influence of informal sanctions, such as shame and moral beliefs, in decisions toward computer abuse, IS misuse, and security policy non-compliance (e.g., D'Arcy & Devaraj, 2012; D'Arcy *et al*, 2009; Hu *et al*, 2011; Vance *et al*, 2013).

Along with these deterrence-based studies, emerging research has shifted from the broader categories of unethical IS behavior and computer abuse and misuse to a more narrow domain of security policy compliance. We speculate that this shift is partially due to the practical difficulties of obtaining valid instances of employees' negative computing behaviors, coupled with the increase in security policies. The range of topics examined in this literature draws on multiple theoretical bases and the results point to a variety of individual and situational factors that predict and explain employees' security policy compliance. See Table 1 below for a summary of the most prominent theory bases, as well as Appendix F for a more comprehensive analysis.

The scope of security policy compliance research is evident based on scholarly reviews of the topic. For example, Guo (2013) reviewed extant literature to develop a classification of security policy-related behaviors, whereas Crossler *et al* (2013) used prior findings as a basis for proposing future research directions in behavioral IS security research. Other reviews classify security policy compliance studies in terms of the antecedents of this behavior (Lebek *et al*, 2014; Padayachee, 2012; Sommestad *et al*, 2014) and the theories and methodical approaches utilized (D'Arcy and Herath, 2011; Lebek *et al*, 2014; Siponen & Vance, 2014; Wall *et al*, 2015; Willison and Warkentin, 2013). We should also note that while the security policy compliance literature is well established at this point, debates exist regarding the appropriate level of specificity and generality of constructs and other methodological issues. For instance, Siponen & Vance (2014) promote the study of more nuanced, behavior-specific security policies (e.g., a password usage policy), rather than general policy statements that are behavior neutral. In their view, exploring behavior-specific policies improves the contextual relevance of security policy research. D'Arcy and Herath (2011) speculated that some of the disparate results of deterrence-based studies of security policy compliance are driven by the inconsistent measurement of key constructs and the exclusion of contingency variables. In sum, although the study of the drivers of employees' security policy compliance is the most extensive and mature component of security policy research, ample opportunities remain for additional work to help clarify and extend past findings.

The remaining components of security policy research – that is, the study of the inputs to and organizational consequences of security policies – are not nearly as voluminous and often lack theoretical foundations and direction (see Appendix F for details). These areas of the literature may be more a product of the technical, functionalist paradigm that served as the intellectual basis for much of the early IS security research (Dhillon and Backhouse, 2001; Siponen and Oinas-Kukkonen, 2007). This paradigmatic orientation manifests itself in a highly structured, technical approach to the study of IS security that is largely devoid of theorizing (e.g., risk assessment checklists, security evaluation methods). Notable exceptions, which we later detail, are the application of theories of user participation to the design of security policies to promote improved security performance (Spears & Barki, 2010), as well as the use of control theory to explain formal and informal security controls as drivers of security policy effectiveness (Hsu *et al*, 2015).

Table 1 Compliance-oriented security policy theory links and examples

Topic Studied	*Theory Base*	*Sample Publications*
Use of sanctions	Deterrence theory	Bulgurcu *et al* (2010), D'Arcy *et al* (2009), Herath & Rao (2009a)
Cognitive rationalizations toward security policy non-compliance	Neutralization theory and moral disengagement theory	Barlow *et al* (2013), D'Arcy *et al* (2014), Siponen & Vance (2010)
Self-control	Criminological self-control theory	Hu *et al* (2015), (2011)
Attitudes toward compliance and non-compliance with security policies	Theory of reasoned action and the theory of planned behavior	Bulgurcu *et al* (2010), Guo *et al* (2011), Hu *et al* (2012)
Fear appeals	Deterrence theory and protection motivation theory	Boss *et al* (2009), Boss *et al* (2015), Johnston & Warkentin (2010a)
Moral reasoning and moral beliefs regarding security policy compliance	Kohlberg's theory of cognitive moral development and contemporary deterrence theory	D'Arcy & Devaraj (2012), Hu *et al* (2011), Li *et al* (2014), Myyry *et al* (2009)
Organizational trust	Fairness theory	Lowry *et al* (2015)
Perceived accountability for security policy non-compliance	Accountability theory	Vance *et al* (2013; 2015)
Perceived rewards for security policy compliance	Rational choice theory	Bulgurcu *et al* (2010), Chen *et al* (2012), Li *et al* (2010), Hu *et al* (2011), Vance & Siponen (2012)
Personal and workplace norms regarding security policy compliance	The theory of reasoned action and the theory of planned behavior	Bulgurcu *et al* (2010), Guo *et al* (2011), Siponen *et al* (2010)
Security awareness or security education and training awareness	Rational choice theory and protection motivation theory	Bulgurcu *et al* (2010), Posey *et al* (2015)
Security policy mandatoriness	Control theory	Boss *et al* (2009), Lowry & Moody (2015)
Self-efficacy toward security policy compliance	Theory of planned behavior and protection motivation theory	Boss *et al* (2009), Bulgurcu *et al* (2010), Siponen *et al* (2010), Warkentin *et al* (2011)
Social environment toward security policy compliance	Social learning theory	Warkentin *et al* (2011)
Stress due to security policy requirements	Transactional stress theory and coping theory	D'Arcy *et al* (2014)
Threat and coping appraisals	Protection motivation theory	Boss *et al* (2015), Johnston & Warkentin (2010a), Siponen *et al* (2010)

In looking at the disparate collection of constructs and theoretical perspectives that have been employed within security policy research, it is difficult to understand how the various components of this research stream relate in a cohesive fashion. For one, the security policy compliance review papers described above are limited to this subset of the literature (i.e., security policy compliance and related behavior) and not the broader security policy literature that includes the inputs to and organizational consequences of security policies. Other reviews similarly focus on subsets of the security policy literature, such as security culture and employees' security awareness (Karlsson *et al*, 2015; Lebek *et al*, 2014). Several other review papers catalogue security policy studies into categories within the broader IS security literature. For example, Siponen and Oinas-Kukkonen (2007) classified a sample of early IS security studies according to research approach and security-related topic (e.g., security management, secure information system development). Similarly, Zafar & Clark (2009) classified IS security studies according to predefined themes established by the IBM Security Capability Reference Model. More recently, Soomro *et al* (2016) reviewed the IS security literature and classified studies into categories related to information security management. Collectively, these extant reviews provide descriptive accounts of security policy research (or aspects of it), aimed at classifying studies into isolated categories based on research topics, theories, or methodological approaches. Appendix A summarizes several extant reviews of the security policy literature and describes how the current study differs in terms of scope and purpose.

Notably absent from the prior literature is a detailed and comprehensive account of how the larger body of research on the drivers of security policy compliance behavior fits with the study of the inputs and consequences of security policies. Our aim is to address this issue by synthesizing the multiple streams of security policy research, gaining a holistic understanding of this work, and developing a research framework that explicates relationships among security policy constructs. Through this exercise, we seek to contribute to theory building efforts in IS security research, as well as identify areas where future research is needed due to gaps or inconsistent findings. We next describe the methodological approach for our review of the security policy literature.

Methodology

Our review approach aligns with Rowe's (2014) concept of a review for understanding, which aims at synthesizing a stream of research, identifying problems, gaps, and research opportunities within it, and providing a foundation for future theorizing within this domain. Alternative forms of literature reviews are either seen to be less systematic and comprehensive or are intended to analyze a particular theory or methodological issue within the context of a single topic or theory (Paré *et al*, 2015; Rowe, 2014). None of these approaches were seen by the authors to be compatible with the existing body of security policy literature or the goals of this study. In particular, given the dearth of original theory (see Appendix F) within much of the security policy literature, we opted for an incremental approach that focused on a pre-theoretical structure (i.e., a research framework derived from our literature review) as opposed to conducting a literature review aimed at pure theoretical explanation. Our approach is in accord with the recommendations of IS scholars who promote pre-theoretical structures as critical elements in the steps toward strong theory (Hassan, 2014; Hassan and Lowry, 2015).

Past guidance has advocated that high-quality literature reviews in IS should contain a clear articulation of the review boundaries, the steps taken to collect the relevant literature, and how the literature was analyzed (Paré *et al*, 2016; Rowe, 2014; Schryen, 2015; vom Brocke *et al*, 2015; Webster and Watson, 2002). Clearly describing how the review was conducted can translate to a high degree of transparency to the reader, repeatability of the findings for future researchers, and a greater sense of reliability in the overall results (Paré *et al*, 2016). Details of these key components are described below and are further elaborated in the appendices.

Review boundaries

Defining boundaries is an important component of a literature review that establishes the areas to be included and excluded from the study's scope. This review focuses broadly on security policies in organizations, including their design, implementation, compliance/non-compliance, and monitoring. As noted in the Conceptual Foundations section, we follow the definitions used in past research by viewing security policies as the standards, boundaries, and responsibilities for users of information and technology resources in order to facilitate the prevention, detection, and response to security incidents (Bulgurcu *et al*, 2010; Lowry & Moody, 2015). Papers were excluded from our review when they did not directly consider organizational security policy issues (e.g., general government policies, legal policies, political policies, or industry policies), were not specific to the organizational context (e.g., security-related behaviors at home), were primarily technical in nature (e.g., software or hardware design and configuration), or were oriented toward enterprise-level security strategies (e.g., an exclusive focus on the higher-level aspects of managing a security program).

We restricted our focus to empirical and conceptual publications within peer-reviewed journals published through the first half of 2017. Due to the varying degrees of quality and independent review, our review excluded books and conference publications, as well as opinion and commentary pieces. This practice is consistent with other reviews of the IS security literature (e.g., Soomro *et al*, 2016; Wall *et al*, 2015; Zafar & Clark, 2009). Because of the interdisciplinary nature of IS security research, we follow Rowe's (2014) guidance by establishing no boundaries in regard to either the methodological approach employed or the research discipline. We did not exclude articles from our scope based on the operational area of the security policy being studied (e.g., anti-virus policy versus network security policy), provided that the focus of the research was oriented around some element of the policy itself.

Literature search

We conducted a sequential search for relevant literature, whereby a majority of the papers were collected prior to analysis (vom Brocke *et al*, 2015). The criteria for selecting articles to be included in the review utilized a keyword search that was based on a range of possible terms and a variety of distinct research databases to achieve a broad scope of coverage. We referred to the seminal security policy literature, as well as practitioner publications, for the most commonly used terms to guide our search (vom Brocke *et al*, 2015). As a result, we searched for the terms "security policy," "cybersecurity policy," "information security policy," or "security compliance" within the abstracts of publications indexed in the ABI/Inform, ACM Digital Library, Business Source Complete, JSTOR, and Google Scholar databases. These databases are among those most commonly used for the collection of publications for literature reviews in IS (Bandara *et al*, 2015; Schryen, 2015). We sought to collect a comprehensive set of papers, not only those published in a small sample of journals or those viewed as being seminal papers (vom Brocke *et al*, 2015). Based on the results from this initial search, the first and second author examined the identified papers in terms of the boundary criteria specified in the preceding section. Where both authors agreed that the paper fell within the defined boundaries, it was added to the review scope. In cases where one author questioned the inclusion of a potential manuscript (e.g., the centrality of security policy was ambiguous or the paper dealt with technical security policies to some degree), the content of the paper was discussed by the first and second authors until consensus was reached on its inclusion or exclusion. The third author independently reviewed the papers being considered, and a consensus was reached for all included and excluded papers.

Next, a backward search was conducted for works cited within the identified "in-scope" papers, as well as a forward search to identify other sources that cited these publications (Bandara *et al*, 2015; vom Brocke *et al*, 2015; Webster and Watson, 2002). In particular, backward searches within recent and oft-cited papers (e.g., Bulgurcu *et al*, 2010; D'Arcy *et al*, 2009; Goel and Chengalur-Smith, 2010; Hsu *et al*, 2015; Lee *et al*, 2016; Siponen & Vance, 2010; Spears & Barki, 2010) identified several additional papers for inclusion. The decision-making approach to paper inclusion/exclusion described above was employed with this supplementary collection of papers. In total, 114 articles published within 35 journals were selected for inclusion in our review (see Appendix B and C for a complete listing). Appendix D provides a listing of journal articles that were excluded due to the criteria outlined above.

Literature analysis

A systematic analysis of the articles was conducted using an inductive approach. We chose this technique as it enables themes and concepts to emerge from the literature in order to create a research framework (Bandara *et al*, 2015). Past literature reviews in IS, such as Aksulu and Wade (2010), have used a similar technique. We employed a concept-centric approach in our examination of the literature (Webster and Watson, 2002), which focused on highlighting the key constructs and construct relationships identified in each article, as well as key characteristics, such as the methodology and theory base. By organizing the review around the concepts studied in the literature, concept-centric reviews enable an enhanced synthesis of the literature, whereas reviews that favor a more author-centric approach tend to focus on the summarization of a series of articles (Rowe, 2014). Throughout the course of the analysis, the authors met periodically to discuss patterns that were beginning to emerge from the literature. A comprehensive table was created during the authors' initial examination of the literature to record this information, the major components of which are presented in Appendices B, E, F, and G.

In order to synthesize the broader patterns that were emerging from the literature, we relied on visual tools such as "mind mapping" software (XMind) and simple PowerPoint diagrams to form a preliminary conceptual framework and identify key constructs. As additional papers were reviewed, the authors discussed both online and in person how new concepts and patterns should be integrated into the framework. We created ten distinct iterations of our research framework over a period of seven months. As we reached the end of our analysis, the framework and underlying constructs had stabilized and were viewed as being consistent with the full collection of articles within the scope of our review. Formal definitions were established for the terminology used in referring to the framework constructs (refer to Appendix E).

All papers were then re-reviewed by the first author and coded into one or more categories representing the relationship between two of the identified constructs. The second and third authors reviewed these categorizations. Where inconsistencies in coding arose, the relevant papers were re-reviewed and were discussed among the authors. In some cases, papers were coded to an additional construct that had been overlooked. In other cases, where there was a misinterpretation of a construct or a definition, refinements were made to the terminology that provided clearer boundaries. All conflicts were satisfactorily resolved. Due to the inductive nature of the coding process, we achieved reliability in our results through author discussion and iterative refinement of the resulting categories. Our analysis aimed to identify a complete collection of the core, high-level themes and concepts within the literature. However, despite the range of patterns that we explicitly identified, we recognize that there may be additional, lower-level patterns from some subsets of the literature that are only implicitly recognized. Although techniques such as inter-rater reliability might be appropriate for reviews that begin with a theory-driven selection of dimensions or categories, our approach of building on themes found within the literature is consistent with past literature reviews published in top IS journals, including Grahlmann *et al* (2012), Leidner and Kayworth (2006), and Wiener *et al* (2016). Following Rowe's (2014) guidance, a summary of coding results is provided in Appendix F.

The resulting research framework, which is outlined in detail in the following section, consists of ten distinct constructs and five groups of corresponding relationships. The design of the framework follows the guidance of Sabherwal and Robey (1995) and Burton-Jones *et al* (2015), who suggest that a joint application of both variance and process approaches has the potential to more thoroughly address complex questions than one approach could alone. Whereas a variance approach examines relationships between variables at a point in time, a process approach considers how sequences of events contribute to changing phenomena (Langley, 1999). Because of the wide range of approaches adopted within studies included in our review (see Appendix B), choosing to structure our framework using a purely variance or process approach would have excluded valuable insights. As such, the resulting framework is structured in a temporal order, while simultaneously highlighting the cross-sectional factors that introduce variability into the relationship outcomes. By adopting this combined approach, we aim to clarify both the sequence of events that are used to design, implement, and monitor security policies over time, while also providing insights into point-in-time relationships that impact these policy-related outcomes.

Results

Based on our analysis of the 114 papers within the scope of the review, this section presents the resulting research framework that details the key constructs and relationships identified, as well as what we know and areas where

Table 2 Research framework relationships

Relationship	*Description and core constructs*	*Key factors*	*Commonly used theories*
R1: Influences on the design and implementation of security policies	The influence of security standards, guidelines and regulations; desired policy format/structure; and internal/external risk management considerations on the design and implementation of a security policy	Creation of a new security standard for an industry Confusion over current policy format/structure Increase or decrease in internal or external risks	Systems theory Grounded theory
R2: Influence of policy on the organization and individual employees	The implications that a security policy has on both the organization (i.e., information security awareness and culture) and individual employees (i.e., socioemotional well-being)	A new security policy is implemented An existing security policy is significantly revised	Critical social theory Actor-network theory Social cognitive theory
R3: Influence of the organization and individual employees on policy compliance	The influence of information security culture, awareness, and support; socioemotional consequences for employees; personality and dispositional traits; and security policy legitimacy, fairness, and justice on employee compliance with a security policy	Employees have a significant socioemotional reaction to a new or revised policy New employees are hired A new management team is introduced	Deterrence theory Protection Motivation theory Theory of planned behavior Rational choice theory
R4: Influence of policy compliance on organizational objectives	The impact that security policy compliance has on organizational security performance	Employees comply (or do not comply) with security policies	Control theory Deterrence theory
R5: Adjustments to policy design	The adjustments and fine-tuning of security policies during the design and implementation process	Identification of policy shortcomings during design and implementation	Deterrence theory Theory of organizational learning

we need to learn more about the relationships. In total, ten core constructs were identified during our analysis: security standards, guidelines, and regulations; desired policy format and structure; internal and external risk management considerations; security policy design and implementation; information security culture, awareness, and support; socioemotional consequences for employees; personality and dispositional traits; security policy legitimacy, fairness, and justice; compliance with security policy; and organizational security objectives. We define each of these constructs and provide illustrative examples in Appendix E. However, rather than focusing on the constructs in isolation, our analysis indicated a series of five core relationships among them, as well as a series of corresponding key factors. These relationships are identified in Table 2 and Figure 1 and are discussed in detail below.

As the five identified relationships draw on various theoretical bases (see Table 2), which are each accompanied by their own assumptions, we follow the work of Cairney (2013) and Langley (1999) who provide guidance on combining multiple theories. By using a complementary approach, we can uncover new insights by simultaneously considering different theories, while maintaining a separation between each of the theoretical lenses. For example, past research within relationship 3 includes extensive use of deterrence theory, protection motivation theory, and the theory of planned behavior. By combining studies that use one or more of these theories together in our framework, we do not argue that these perspectives are compatible (or incompatible), but instead suggest that they share a common pattern in the concepts that they study. As every theory has inherent limitations, this complementary approach can aid in facilitating an understanding of the different perspectives that can be used to study the same phenomenon. Our proposed research framework seeks to synthesize these conceptual relationships, while recognizing that each study provides a unique and valuable point of view. As such, our framework stops short of attempting to reconcile all possible theories within each of the fields into a single, integrated theory. Similar approaches to the combination of multiple theories has been employed in past literature reviews, such as Cram *et al* (2016b).

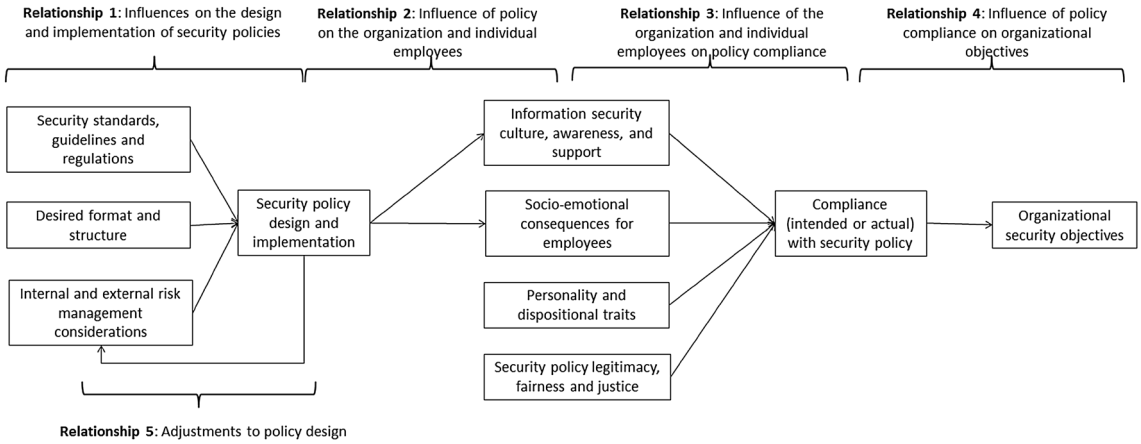

Figure 1 Security policy research framework.

Relationship 1: policy design and implementation factors

The first relationship identified in the literature examines the influences on the design and implementation characteristics of a security policy. Three groups of factors emerged from our analysis. The first factor examines the role of security standards, guidelines, and regulations in shaping how security policies are put into place. A variety of options have been established to guide organizations on best-practice approaches to managing information security. For example, the International Organization for Standardization released the 27000 series of information security management guidelines (International Organization for Standardization, 2016). Organizations of varying sizes and types can adopt one or more specific standards, including ISO 27001 (Information Security Management) and ISO 27002 (Code of Practice for Information Security Controls), in order to comply with best practices and provide assurance to customers (Susanto *et al*, 2011). This guidance can help to provide a standardized level of security to organizations that can then be customized based on particular circumstances (von Solms, 1999). In some cases, such frameworks are required by legal or regulatory guidelines (Knapp *et al*, 2009). Although such guidance can be useful in advocating for the creation of security policies, it can sometimes fall short of the specific, practical details that aid employees in actually tailoring, implementing, and understanding the policies (Siponen, 2006; Siponen & Willison, 2009). To address this challenge, frameworks are adopted that provide more tangible, step-by-step advice in designing and implementing security policies. Rees *et al* (2003) and Knapp *et al* (2009) provide policy frameworks for information security that propose a life cycle model spanning the stages of assessment, planning, delivery, and operation. Such an approach can aid organizations in understanding the most salient factors to consider when designing a security policy and suggests that significant customization of policies is necessary to tailor a policy to a particular organization's circumstances.

The second factor that is viewed as influencing security policy design and implementation is the consideration of policy format and structure. Distinct from the previous factor that draws policy content from preexisting tools, this consideration is instead driven by the aims and objectives of creating a policy that employees are able to read and understand. For example, Goel and Chengalur-Smith (2010) argue that decisions made by security policy creators around brevity (e.g., length), clarity (e.g., ease of understanding), and breadth (e.g., level of detail on violation ramifications) are all contributing factors to the overall quality of the policy. Where practitioners struggle to understand the design of policies, difficulties can arise during implementation (Pathari & Sonar, 2012).

The final factor influencing security policy design and implementation is the role of risk management considerations. Research in this area considers the internal and external characteristics that influence particular security policy design decisions. For example, elements such as organization type, size, information technology (IT) infrastructure, business objectives, legal requirements, economic environment, and internal/external threats are viewed as factors that drive security policy creation (Hong *et al*, 2006; Karyda *et al*, 2005; Knapp *et al*, 2009; Warman, 1992). Wall (2013) argues that insider threats are a key risk and that many organizations fail to install sufficient procedures to ensure that insiders protect data. In response, security policy development activities should increasingly consider the potential risks of the well-meaning, but negligent insider (Wall, 2013).

Unexplored opportunities: policy design and implementation factors Most research within this subset of the literature does not draw heavily on theory (refer to Appendix F for details) and is instead oriented around the practical considerations of managers responsible for the design and implementation of policies. An opportunity may exist in the study of policy design and implementation factors by adopting a control theory-oriented viewpoint. Within IS, such

research has been applied primarily within a systems development context, but some high-level references have been made within the security policy literature as well (e.g., Pathari & Sonar, 2012; Rees *et al*, 2003). By employing a more control theory-centric approach that includes concepts such as control style (i.e., the degree of employee participation and agreement with controls) and control degree (i.e., the amount and frequency of control), future research investigating drivers for policy creation and implementation could build on the work of Kirsch (1997), Gregory *et al* (2013), and Tiwana & Keil (2009) to consider in more depth the rationale behind the controls underlying security policies and what choices managers have in structuring security policies. Recent research, such as Moody *et al* (2016), considers novel applications of control concepts to information security issues, but room still remains to customize this line of inquiry to policy design and implementation.

Another area of development is in regard to the range of security standards and guidelines that drive policy creation. Although studies such as Siponen (2006) outline a selection of the relevant tools, there remains a degree of uncertainty for practitioners in how the standards compare with one another and when one should be followed over another (Ross, 2015). Past studies on de jure standards, such as Backhouse *et al* (2006) and Smith *et al* (2010), have examined the patterns associated with standards adoption and accreditation, but more work remains to be done on newly emerging industry standards and guidelines. Future research could provide clarity in this regard by examining the core objectives, scope, and overlaps in the security standards and guidance that are relied on by managers creating security policies.

Finally, despite the practitioner-oriented nature of this area of the security policy literature, we found very little empirical work that draws on real organizational experiences [some exceptions exist, such as Puhakainen & Siponen (2010)]. Although the conceptual studies that make up this section are valuable to organizations, an opportunity exists to grow the field's knowledge by collecting data via case studies, action research, and surveys to uncover if there are additional process steps or factors that drive the design and implementation of security policies in organizations.

Relationship 2: influence of policy on the organization and individual employees

The second relationship in our research framework examines the impact that an implemented security policy has on the organization and its employees. Interestingly, a sizable proportion of research within this relationship provides empirical insights into the healthcare industry (e.g., Renaud & Goucher, 2012; Stahl *et al*, 2012; Vaast, 2007). This is an area of growing interest within the field that is unique in its security risks (e.g., personal health information) and broad collection of employee representatives (e.g., physicians, administrators, IS staff).

Two factors emerged from our analysis: information security culture and awareness, and socioemotional consequences for employees. The first factor considers how the implementation of a security policy influences broadly held beliefs and values related to security within an organization. Security awareness generally refers to the values and attitudes that individual employees hold in regard to secure information practices (Tsohou *et al*, 2015b), while security culture is commonly framed in terms of the shared assumptions, values, and beliefs held by a group of employees (Karlsson *et al*, 2015; Knapp *et al*, 2006). Although the implementation of a policy that specifies acceptable behaviors and provides specific guidelines for operational activities should be clearly communicated to employees [in order to inform them of the importance of security (Knapp *et al*, 2009)], past research highlights the disconnect between security policy implementation and employee awareness of security issues. This view suggests that policy implementation is only one component of a larger initiative necessary to cultivate awareness and develop a security-oriented culture. Such additional activities can include extensive training and development programs (Chen *et al*, 2015; Karyda *et al*, 2005; Tsohou *et al*, 2015b) and the establishment of strong top management support (Knapp *et al*, 2006). Differences across employee groups can also lead to distinctions in security policy awareness and culture. For example, Johnston *et al* (2013) find that remote employees are less aware of security policy elements compared to onsite employees due to lower levels of managerial oversight and situational support. Similarly, Vaast (2007) notes that unique social representations between different groups in the same organization (e.g., physicians versus IS professionals) can lead to misunderstandings and communication issues related to security.

The second factor considers the impact that the implementation of a security policy has on the socioemotional well-being of employees. This subset of the literature considers how a security policy can shape employee feelings such as trust and motivation. Past IS and management research has noted that managerial actions can bring about either positive consequences for employees, such as perceptions of satisfaction, but can also lead to negative feelings, such as stress and intentions to leave the organization (Jaffee, 1991; Santana and Robey, 1995). Within the context of security policies, the approach used to implement a policy has been found to influence the social and emotional consequences for employees. For example, where compliance with policies is perceived to be mandatory, employees are more likely to adopt the necessary precautions (Boss *et al*, 2009); however, this may lead to feelings of suppression and a lack of fairness (Lowry & Moody, 2015; Renaud & Goucher, 2012). Further, security policy compliance activities can, at times, be catalysts for employee stress (Lee *et al*, 2016). In order to create a positive reception by employees, past research suggests that a security policy should be viewed as truthful, clear, and equitable (Renaud & Goucher, 2012; Siponen, 2000; Stahl *et al*, 2012).

Unexplored opportunities: influence of policy on the organization and individual employees Although researchers would be well served to continue to focus on the important and unique elements of the healthcare industry, future studies could also apply the identified insights on how security policies impact awareness/culture and socioemotional well-being to other industries as well. By comparing the current results to other highly regulated industries such as financial services and aerospace, technology-intensive industries such as telecommunications and web services, or evolving industries such as publishing and retail, new and interesting insights could be uncovered that could be compared to healthcare. Since many of the related constructs tend to be slow to change over time (e.g., organizational culture, employee perceptions), such research may be particularly valuable where it takes a longitudinal perspective.

Another area for development is the link between security policies and their perceived legitimacy by employees. Much of the current literature considers the positive or negative views that employees have in regard to a particular security initiative, but few consider the underlying drivers that lead to those perceptions. Willison and Warkentin (2013) make a similar point in promoting the study of organizational justice perceptions as drivers of employee computer abuse. By drawing on past frameworks, such as Bijlsma-Frankema and Costa's (2010) model of control legitimacy (comprised of justice, autonomy, competence development, and group identification), the factors that drive why employees view a security policy as being legitimate at a particular point in time can be clarified. This could provide useful insights for practitioners intent on cultivating support and avoiding resistance for security policies within their organizations.

Relationship 3: organizational and individual employee factors driving policy compliance

The third relationship considers the influences on security policy compliance. This category of research comprises approximately seventy percent of the studies within the scope of this review (81 of 114 papers), and as shown in Appendix F and based on our discussion in the Security Policy Research Overview section, draws heavily on established theory from several reference disciplines. In establishing this relationship, we recognize the existence of papers that address two categories of lower-level themes. First, 50 papers focused on policy *compliance* (e.g., factors that lead to an employee complying with a policy), while 29 papers examined *non-compliance* (e.g., factors that lead to an employee violating a policy). Separately, 57 papers consider the *intended* behavior of employees (e.g., I plan to comply with the policy in the future), while 26 papers examine *actual* behavior (e.g., I currently comply with the existing policy). The sum of papers examining intended and actual behavior is greater than the total papers under examination, as eight papers examined both intended and actual behavior, while two papers did not clarify the type of behavior under investigation.

However, because of the significant overlap in the topics examined within the policy compliance/non-compliance and actual/intended behavior literature, we chose to investigate the broader organizational and individual factors that drove the behavior. In doing so, we recognize the methodological and conceptual differences between the elements of these two categories. For example, some scholars contend that security policy compliance and non-compliance are distinct behaviors and, therefore, should be studied separately (Guo, 2013). This position is most relevant in cases where deterrence theory is applied, as empirical evidence indicates that deterrence-based sanctions are much stronger predictors of policy compliance as compared to non-compliance (D'Arcy and Herath, 2011; Sommestad *et al*, 2014). However, Sommestad *et al* (2014) found that the relative influences of many non-sanction-based predictor variables were consistent across both compliant and non-compliant (misuse) security behaviors. This finding aligns with our view of security policy compliance/non-compliance as a singular concept, and we suggest that other literature review techniques, such as a meta-analysis, would be better suited to unravel the relevant quantitative differences (King and He, 2005). Rather, we focus on four factors that emerged from our analysis that crossover the compliance/non-compliance, intended/actual behavior boundaries: information security culture, awareness, and support; the socioemotional consequences of the security policy; personality and dispositional traits; and security policy legitimacy, fairness, and justice.

Information security culture, awareness, and support includes the organizational and managerial characteristics that drive employee compliance with a security policy. A series of characteristics are examined in the literature that are shown to have a positive relationship with security policy compliance, including organizational values, climate, and norms (Chan *et al*, 2005; Goo *et al*, 2014; Hu *et al*, 2012), as well as security training, awareness, and visibility (Bulgurcu *et al*, 2010; Lowry *et al*, 2015; Puhakainen & Siponen, 2010; Siponen *et al*, 2010). However, other characteristics show inconsistent results. For example, managerial commitment and support was commonly found to be positively associated with compliance (Chan *et al*, 2005; Herath & Rao, 2009b; Hu *et al*, 2012), but D'Arcy and Greene (2014) and Ng *et al* (2009) found that perceived organizational support had either a negative or insignificant relationship to security behaviors. Similarly, Al-Mukahal & Alshare (2015) found no significant relationship between security policy awareness and the number of policy violations.

The use of managerial controls is examined as a means to encourage employees to comply with security policy guidelines. These controls are primarily behavioral in nature, relying on managers to monitor employee activities and discipline behavior that is inconsistent with

organizational objectives (Kirsch, 1997). Findings suggest that where employees believe policy compliance to be mandatory (Boss *et al*, 2009; Lowry & Moody, 2015), managers are monitoring their actions (Vance *et al*, 2015, 2013), and non-compliance will be detected (Foth, 2016; Herath & Rao, 2009b; Li *et al*, 2010), they are increasingly accountable and will more readily follow security guidelines (Vance *et al*, 2013). Empirical studies also suggest that sanctions have some influence on employees' policy compliance decisions (Bulgurcu *et al*, 2010; Herath & Rao, 2009a, b; Hu *et al*, 2012, 2011), although the findings are mixed at best (D'Arcy and Herath 2011; D'Arcy *et al*, 2009; Guo *et al*, 2011; Hu *et al*, 2011).

Informal controls, which increasingly rely on social values and beliefs (Chua *et al*, 2012; Kirsch, 1997; Kirsch *et al*, 2010), are also found to positively link to employee compliance with security policies. This includes normative beliefs (i.e., "others think I should comply") (Bulgurcu *et al*, 2010; Cheng *et al*, 2013; Guo *et al*, 2011; Herath & Rao, 2009a, b), as well as descriptive norms (i.e., "others are complying, so I will too") (Cheng *et al*, 2013; Herath & Rao, 2009b).

Socioemotional consequences of the security policy examine how the socioemotional impact of security policies can contribute to policy compliance. Although one element of Relationship 2 examines how security policies can shape an employee's social and emotional well-being (e.g., feelings of stress associated with the introduction of a new security policy), this stream of research extends the concept by examining the subsequent consequences to compliance. For example, where a security policy can generate positive social and emotional outcomes, such as happiness (Siponen & Iivari, 2006), job satisfaction (D'Arcy and Greene, 2014), and organizational commitment (Aurigemma & Leonard, 2015; Teh *et al*, 2015), these factors impact the degree that employees will comply with the guidelines. In contrast, security policies that contribute to stress (D'Arcy *et al*, 2014) and role conflict/ambiguity (Teh *et al*, 2015) are found to lead to non-compliance.

Personality and dispositional traits encompass the inherent individual employee characteristics associated with security policy compliance. The factors and theoretical perspectives employed in this category largely stem from the rationality-based view of human behavior, such as security policy compliance being driven by a cognitive evaluation of its costs and benefits, along with other relatively stable security-related attitudes and beliefs. Some commentators argue that this purely cognitive-rational viewpoint may be an oversimplification and that affective factors such as moods and emotions may influence security policy compliance (for examples of these factors, see the socioemotional category above and the legitimacy category below). The most prominent factors examined in the security policy research include aspects of an individual's ethical standards, such as personal norms (Ifinedo, 2014), morality (Hu *et al*, 2011; Myyry *et al*, 2009; Vance & Siponen, 2012), and virtuousness (Siponen & Iivari, 2006). Findings from this research suggest that personality and dispositional traits have either a direct link to security policy compliance (or compliance intentions) or a link that is mediated by other constructs such as attitude. Other research, such as Johnston *et al* (2016), finds that dispositional factors (e.g., conscientiousness, extraversion, agreeableness) moderate the link between an employee's perception of a situation (e.g., sanction severity, threat vulnerability) and their intention to comply with a security policy. Links between attitude and policy compliance are established in works such as Bulgurcu *et al* (2010), Foth (2016), Hu *et al* (2012), and Moquin & Wakefield (2016); however, some research shows that the strength of this link varies by country (Dinev *et al*, 2009), while others find that no significant link exists at all (Guo *et al*, 2011).

Other research in this area focuses around aspects of an individual's general disposition. Although findings linking organizational commitment to policy compliance are inconclusive (Goo *et al*, 2014; Lee *et al*, 2004), or show that it has an indirect influence on policy compliance (Posey *et al*, 2015), traits such as low self-control (Guo & Yuan, 2012; Hu *et al*, 2011, 2015; Ifinedo, 2014) and risk/reward-seeking nature (Guo *et al*, 2011; Vance & Siponen, 2012; Vance *et al*, 2012) are found to link negatively to policy compliance.

Finally, past studies considering employee traits also consider the role that rationalizations play in complying with security policies. Results in this area are again contrasting. For example, although self-efficacy is generally found to positively relate to policy compliance (Herath & Rao, 2009b; Ifinedo, 2012, 2014; Siponen *et al*, 2009, 2014; Siponen *et al*, 2010; Vance *et al*, 2012), no significant relationship was found by Wall *et al* (2013). Similarly, response efficacy (i.e., the belief that employees can make a difference in security) is commonly found to link to compliance (Herath & Rao, 2009b; Ifinedo, 2012; Siponen *et al*, 2009; Vance *et al*, 2012), but contrasting results are also found (Siponen *et al*, 2014, 2010). Finally, a relatively new approach to examining the employee policy compliance rationalizations is the study of neutralization techniques (e.g., "no one will be hurt if I violate the policy"), which have found positive links with policy violations (Siponen & Vance, 2010; Teh *et al*, 2015), as well as evidence of only partial support (Barlow *et al*, 2013).

Security policy legitimacy, fairness and justice consider how compliance is driven by employee perceptions of the policy itself. This collection of factors is distinct from personality and dispositional traits in that it focuses on the fundamental security policy characteristics that influence employee compliance, rather than inherent traits of the employees themselves. Past research outside of IS security finds that employees are more likely to follow organizational guidelines that they perceive to be legitimate, where legitimacy results from feelings of justice, autonomy, group identification, and competence development (Bijlsma-Frankema and Costa, 2010). This concept has been applied to the security policy literature,

where past studies have highlighted the positive links between compliance and perceptions of policy legitimacy (Hu *et al*, 2012; Son, 2011), fairness (Lowry *et al*, 2015), freedom (Lowry & Moody, 2015), justice (Li *et al*, 2014), user participation in policy development (Spears & Barki, 2010), and voluntariness (Siponen & Iivari, 2006). Other related studies in this area are oriented around employee perceptions that a policy (or a policy-mandated behavior) is necessary to combat legitimate threats (Herath & Rao, 2009b; Johnston & Warkentin, 2010a; Ng *et al*, 2009). However, even in situations where employees perceive policies as necessary, the existence of barriers, personal costs, or other inconveniences have also been shown to impede compliance (Bulgurcu *et al*, 2010; Ifinedo, 2012; Ng *et al*, 2009; Vance *et al*, 2012).

Unexplored opportunities: organizational and individual employee factors driving policy compliance The research examining compliance has considered a wide variety of important factors that can be of assistance to organizations wishing to improve compliance with security policies. Although a number of clear theoretical relationships have been established, inconsistent results in some areas have clouded the field's understanding of the organizational and individual employee characteristics that drive policy compliance. One factor that may contribute to these inconsistent results is the confounding of proximal constructs (i.e., those that have a direct influence on compliance) and distal constructs (i.e., those that affect compliance indirectly via their influence on the proximal constructs). Research in other fields, such as Van Iddekinge *et al* (2009), suggests that the effects of personality on performance are partially mediated by other variables, such as motivation. Future research on security policy compliance could seek to clarify the extent that such findings apply in a security policy compliance setting.

Another factor may be that nearly all studies in this area are cross-sectional in nature and do not consider the ongoing adjustments that are made to policies over time. The literature in other areas of IS control highlights the importance of adjustments, as this provides opportunities for managers to identify and correct problems that occur (Choudhury and Sabherwal, 2003; Cram *et al*, 2016a). The binary nature of the security policy compliance literature (i.e., employees either comply or they do not), mixed with the contrasting results in many areas, presents a confusing picture for practitioners, as well as an uncertain direction for research. These challenges are compounded by not only the wide range of existing theories that are applied within this body of research (see Appendix F), but also the scarcity of new theory that is developed as a result of these studies. Indeed, there is an opportunity to supplement the empirical literature with an increasing attention to either pure theory development (e.g., Wall *et al*, 2016) or broader consideration of alternative research approaches (e.g., process versus variance approaches), as a means to move beyond referencing the same theoretical bases to consider new avenues for theoretical insight. In particular, since most studies in this relationship adopt a cross-sectional, variance approach, future studies could consider the ongoing process changes that occur to policies over time as a result of compliance problems and violations. This could include investigations of the most effective way to adjust a policy to encourage compliance and how organizations learn from compliance failures. Adding an increasingly iterative perspective to security policy development, implementation, monitoring, and adjustment may allow for valuable new insights to be uncovered.

Additionally, a focus in security policy research is the implementation of policy enforcement monitoring mechanisms and evaluations of the impact of employees' awareness of these mechanisms on compliance. This research has yet to account for malicious organizational insiders who can employ countermeasures to mitigate these controls, or simply circumvent policy enforcement mechanisms, when employees are enlightened about these controls in an effort to improve compliance. Future research should investigate the risk/reward trade-off between gains in compliance due to employees' awareness of monitoring controls and the potential for malicious insiders to exploit this knowledge.

Relationship 4: security policy influence on organizational objectives

The fourth relationship explores the extent to which security policies aid in achieving organizational objectives, such as reducing security breaches. Compared to the previous relationship, the quantity of studies in this area is limited and the existing results are somewhat surprising. For example, Doherty & Fulford (2005) and Wiant (2005) find no significant relationship between security policy adoption and the incidence of security breaches or the seriousness of those incidents. However, this is in contrast to other studies, such as Spears & Barki (2010), who find that fewer security deficiencies result from organizational awareness, user participation, and perceived improvement in security control development, which includes policies.

Other research in this area considers the specific factors that contribute to security policy effectiveness, such as the goals being achieved, the perception that the organization is protected, and that security losses are minimized. Using this concept, Hsu *et al* (2015) finds that effectiveness is influenced by both extra-role (security behaviors that benefit the organization but are not specified in policies and not dependent on rewards or punishment) and in-role (those specified or associated with security policies) behaviors. Similarly, Knapp & Ferrante (2012) find evidence to support policy awareness and enforcement to relate positively to policy effectiveness.

Unexplored opportunities: security policy influence on organizational objectives The relatively limited focus on demonstrating the tangible benefits of

employing a security policy, as well as the conflicting results, presents an important opportunity for future research. Even though a notable research effort has been dedicated to understanding how organizations can more effectively influence employee compliance with security policies (see Relationship 3, above), there is a paucity of empirical studies that clearly establish that compliance directly results in desirable organizational objectives. Although this relationship is widely assumed to exist, few studies investigate the tangible benefits that can result. Future work could attempt to clarify the specific organizational security objectives that can be achieved through security policy compliance, as well as the negative impacts on objectives where non-compliance is common (e.g., quantity and severity of security incidents). Such investigations could also consider the consequences of security policy compliance on the broader organization (e.g., corporate governance, regulatory penalties), as well as a possible relationship between the degree of security policy compliance and compliance with other organizational policies (e.g., record retention, health and safety, etc.).

Another area for future inquiry is the examination of factors that can influence the achievement of security-related objectives. Since policies are typically one of many internal controls that work together to prevent and detect security incidents, it remains possible that even if employees comply with security policies, the actual organizational benefits of doing so may be diluted by other factors. These factors could moderate the relationship between policy compliance and the achievement of organizational security objectives or could influence the achievement of organizational security objectives directly. For example, Doherty & Fulford (2005) suggest that enforcement difficulties and inadequate resourcing could lead to sub-optimal organizational outcomes, even when security policies are being complied with. Future research could seek to specify a comprehensive list of constructs that could influence the achievement of organizational security objectives, including the relevant links to security policy compliance.

Finally, the achievement of broader objectives that stem from security policy compliance may take time to emerge and develop. For example, similar to the lag effect that has been shown with respect to certain technical security controls (Angst *et al*, 2017), the implementation of a revised security policy may result in an initial decline in compliance as employees struggle to understand their responsibilities; however, following communication and training activities, compliance with the policy may subsequently rise. On the other hand, employees may exhibit a surge in compliance with the deployment of a new, more rigorous policy; however, employees may become fatigued with these more rigorous controls and compliance may suffer over time. By considering these temporal aspects of the link between policy compliance and organizational benefits, managers may be able to better understand the benefits received through employee adherence to security policies. However, future research is needed to clarify these compliance-related factors that change over time and how this can result in delays in achieving organizational security benefits.

Relationship 5: adjustments to policy design

Finally, the fifth relationship investigates the process of updating and maintaining security policies. Much of the research in this area, such as Knapp & Ferrante (2012) and Doherty & Fulford (2005), focuses primarily on examining the frequency of policy updates. The sources for why the policies are being updated include issues of age (e.g., the same policy has been in place for two years), policy scope (e.g., the technology changes), and best practices (e.g., compliance and standards guidelines are updated). Although these updates would appear to be beneficial to the overall information security of the organizations, some research finds no link between the frequency of policy updates and the downstream incidents or severity of security incidents (Doherty & Fulford, 2005). However, other findings dispute this result and argue that policy maintenance does contribute positively to security effectiveness (Knapp & Ferrante, 2012).

Other studies in this area adopt a more conceptual approach to policy design updates, by modeling the steps that should lead to adjustments. Knapp *et al* (2009) suggest that an iterative process of risk assessment, policy development, and policy review should be in place. As part of this approach, aspects of policy training, implementation, monitoring, and enforcement contribute to identifying opportunities for policy improvement. Rees *et al* (2003) propose a similar model that includes four core life cycle steps: plan (development, definition), deliver (implementation), operation (review trends, monitor operations), and access (policy assessment, risk assessment).

Unexplored opportunities: adjustments to policy design based on changing organizational factors Despite the past research in this area that outlines the conceptual factors that should be considered when adjusting security policies over time, little empirical research has been conducted that examines how these changes are managed in practice. It is possible that one managerial technique may be effective for bringing an old policy up to date, while a different technique is effective to adjust a policy to account for a new best practice. Similarly, many organizations have developed a collection of security-related policies (e.g., acceptable use policy, network security policy, data classification policy) that cover a variety of systems and apply to a range of stakeholders. In such cases, a more complex system of governance is required to effectively oversee, monitor, review, update, and approve the collection of security policies. Future research could make a useful contribution to the field by clarifying the most effective managerial and governance techniques used to make security policy adjustments.

Although most research examining security policy adjustments assumes that factors such as age, scope, and emerging best practices drive policy changes, future research could also consider the additional factors that may be relevant. For example, rather than approaching security policies as primarily static documents that undergo occasional, significant changes, researchers could consider the potential benefits of security policies that undergo periodic, small-scale adjustments in response to employee feedback, industry trends, and emerging security threats. By adopting a more agile approach to security policy adjustments, organizations may be able to more effectively guide the behavior of employees and protect information assets. Additionally, extant research on security policy adjustments focuses on the content of the policies, rather than other possible changes that could be made, such as how a policy is communicated to employees (e.g., adjusted from a newsletter to a video) or how employees are trained in regard to a new policy (e.g., adjusted from in-class learning to an online tutorial). These aspects of security policy adjustments have the potential to impact employee compliance, as well as the downstream organizational benefits, and would be worthwhile paths of future research.

However, by focusing only on the events that directly drive security policy changes, we may be limited in understanding the full scope of the policy management process. An opportunity exists to more fully integrate the concept of a policy life cycle into the study of policy maintenance. For example, where managers find a low policy compliance rate for employees, changes could be made to the policy to improve compliance. Likewise, where organizational security performance is below expectations, policy improvements could commonly be made. These considerations have not yet been fully addressed by the security policy literature, but it would be valuable to adopt an increasingly process-focused, longitudinal viewpoint that can help the field better understand the full range of steps that are undertaken to facilitate a security policy change and how these steps relate to one another.

This section has outlined five core relationships that have been examined within the current security policy literature. Publications within each relationship have highlighted important insights and underlying constructs. A variety of gaps and opportunities for future research are also noted, which we turn our attention to in the following section.

Discussion

The aim of this section is to develop the gaps identified above into a tangible, specific collection of opportunities for future research, consistent with characteristics of a review for understanding (Rowe, 2014). To do so, we outline a series of theoretical relationships not yet applied within the initial framework (Figure 1) in order to construct a revised framework (Figure 2) that proposes new links between security policy constructs, while also highlighting specific future research directions. In order to aid in framing these opportunities for researchers, we further develop a series of possible research directions that could be explored. We recognize that other gaps may exist in the security policy literature and that there are research directions other than the ones we note. As well, since our framework is based on an analysis of what research has been conducted in the past, the emergence of future innovations and technological trends may introduce additional elements that could be relevant to future research. However, this exercise is intended to directly address the gaps highlighted in our review and provide specific guidance on how these issues can be examined in the future. Table 3 summarizes the gaps noted in our findings, the proposed relationships, informing theories or approaches, and possible research directions. Supplementary details on the theories, including their boundary conditions, assumptions, and limitations are noted in Appendix G. This is complemented by Figure 2, which builds on the initial framework by depicting the proposed constructs and relationships using dashed lines and shaded numerals. Each revised area is discussed in more detail below.

Revision 1: control mode, degree and style relating to security policy design and implementation

Control refers to the attempt to affect the behavior of another person or group as a means to achieve goals (Davis, 1940; Flamholtz *et al*, 1985; Tannenbaum, 1962) and encompasses mechanisms such as policies, procedures, and managerial oversight. Much of the past research on control within IS is oriented around the factors that controllers (e.g., managers) consider when selecting controls, such as behavior observability and outcome measurability (Cram *et al*, 2016b; Wiener *et al*, 2016). Traditionally, the resulting controls have been categorized as one of four modes (behavioral, outcome, clan, and self), but additional considerations of control degree (i.e., the frequency and intensity of control) and style (i.e., the degree of mutual controller–controlee agreement) have been introduced (Gregory *et al*, 2013; Kirsch, 1997).

Although control-related factors are examined in other areas of the security policy literature, primarily around compliance (e.g., Boss *et al*, 2009), little consideration is given to the topic in the actual construction of a security policy. By employing a more control theory-centric approach related to security policy design and implementation, researchers could gain insights into the different ways that a policy can be constructed, which could lead to downstream compliance impacts. For example, an organization that employs a unilateral control style to design its security policy (i.e., a one-sided, authoritative approach) may have a very different experience than an organization that uses a bilateral control style (i.e., mutual agreement and discussion

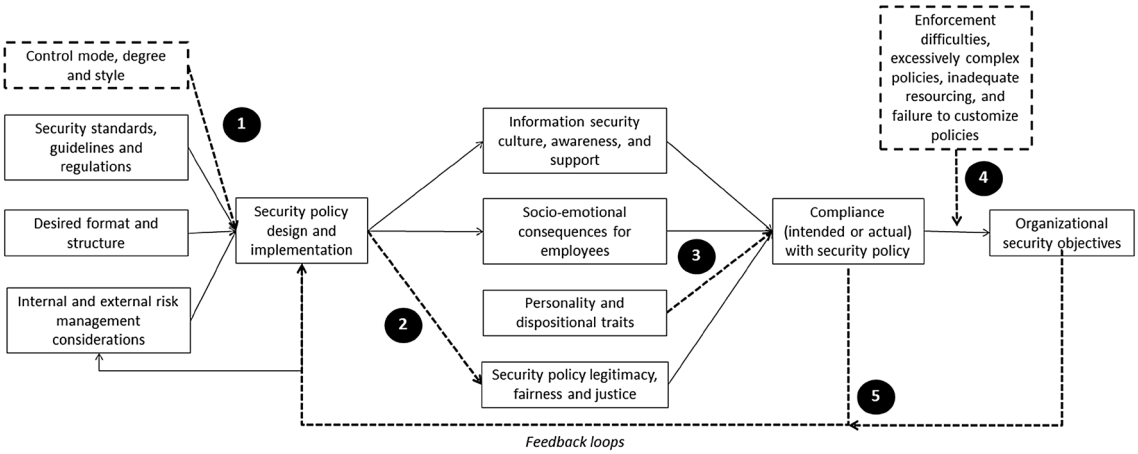

Figure 2 Security policy research framework – revised.

Table 3 Revised research framework relationship descriptions and future research directions

Revision #	*Gap noted in results*	*Proposed relationship*	*Informing theory or approach*	*Possible research direction*
1	Consideration of control factors when constructing security policies	Control mode, control style, and control degree → Security policy design and implementation	Control theory	How do tight/relaxed control degrees and unilateral/bilateral control styles translate into security policy design?
2	Consideration of legitimacy, fairness, and justice during policy design and implementation	Security policy design and implementation → Security policy legitimacy, fairness, and justice	Institutional theory	How can security policies be more effectively designed to take into account employee perceptions of legitimacy, fairness, and justice?
3	Inconsistent findings in regard to the personality and dispositional traits that lead to policy compliance	Personality and dispositional traits → Compliance with security policy	Replication and longitudinal research	How do the personality traits of the increasing number of Generation Y employees influence compliance with security policies?
4	Ambiguous link between employee compliance and organizational security benefits	Enforcement difficulties, excessively complex policies, inadequate resourcing, and failure to customize policies MODERATES Compliance with security policy → Organizational security objectives	Agency theory	What factors, individually or in combination, reduce the positive relationship that security policy compliance has on organizational security performance?
5	Consequences of a policy that is not complied with or does not achieve organizational security objectives	Compliance with security policy → Security policy design and implementation Organizational security objectives → Security policy design and implementation	Work systems theory, cybernetics	How do organizations adjust security policies following a data breach?

between managers and staff on policy components). Comparable research has been conducted in the systems development field that links control design antecedents to the performance of such controls in influencing employee behavior (Gopal and Gosain, 2010; Maruping *et al*, 2009).

When applied to a security policy context, researchers could ask questions such as: *How do tight/relaxed control degrees and unilateral/bilateral control styles translate into security policy design?* The results from such research could provide valuable insight into comparing the alternatives in designing security policies, as well as the downstream consequences that particular control choices can have on constructs such as socioemotional impacts.

Revision 2: security policy links to legitimacy, fairness, and justice

The concept of legitimacy draws on institutional theory, which considers the norms, processes, and routines within organizations associated with social behavior (Meyer and Rowan, 1977; Scott, 1987). Recent studies within management that have examined particular

elements of the theory have argued that employee perceptions of justice, competence development, autonomy, and group identification contribute to views of legitimacy (Bijlsma-Frankema and Costa, 2010). Where organizational structures are viewed as being legitimate, fair, and just, employees are more likely to perform their responsibilities more effectively, including complying with rules and regulations (Jaffee, 1991; Niehoff and Moorman, 1993; Schnedler and Vadovic, 2011; Workman, 2009).

As noted in our initial framework (Figure 1), the "Security policy legitimacy, fairness and justice" construct relates to the "Compliance with security policy" construct, including research by Son (2011) and Hu *et al* (2012). This work explores how the existence of employee perceptions of security policies impacts the degree that they are complied with. However, as we note above, despite the valuable insights on how legitimacy impacts compliance, current research does not establish a clear picture of the security policy characteristics that contribute to first shaping legitimacy, fairness, and justice perceptions. For example, research by Li *et al* (2014) links perceptions of unjust policies to compliance consequences, but it remains unclear what aspects of the policy lead to justice perceptions in the first place and how the policy could be better designed to take this into account.

Future research in this area could pose questions such as: *how can security policies be more effectively designed to take into account employee perceptions of legitimacy, fairness, and justice?* Such studies could aid managers in considering a wider range of employee-centric factors when designing and tailoring security policies. In doing so, organizations could gain a mechanism that could be adjusted to enhance subsequent policy compliance.

Revision 3: personality and dispositional links to security policy compliance

As noted in the Results section, a notable collection of studies have examined the role that personality and dispositional traits have in influencing compliance with security policies. However, a variety of inconsistent results linking personality, commitment, efficacy, and neutralization to policy compliance present challenges to both practitioners and academics. One option to address these inconsistent results is to increasingly conduct replication research, which refers to studies that seek to obtain the same results as previous studies by either reproducing similar conditions or deliberately introducing variations to the conditions (e.g., data set, population) of the original study (Lindsay and Ehrenberg, 1993; Tsang and Kwan, 1999). Although replication studies have traditionally comprised less than 10% of research in most business disciplines, valuable theory development opportunities do exist, including the opportunity to aid in the support or discrediting of theory (Tsang and Kwan, 1999). Past commentators suggest that a proportion of replication research isn't explicitly acknowledged as such, but rather is presented as extensions or challenges of past work (Salterio, 2014). We suggest that much of the research on personality and dispositional links to compliance falls into this category, but that the results that question past findings have yet to follow replication research guidelines (e.g., Evanschitzky and Armstrong, 2013; Mezias and Regnier, 2007) to the extent necessary to pose a challenge to the theoretical links established in previous studies. An opportunity exists to re-evaluate the theory and relationships in this subset of the security policy literature by deliberately replicating past work in order to determine the factors that may account for the current discrepancies.

Another alternative within this area of research is to increasingly conduct studies of a longitudinal nature, in order to better understand how changes in personality and dispositional traits may help to explain the inconsistent findings. The current literature adopts a heavily cross-sectional approach, which, although valuable, provides limited insight into how the personality–compliance relationship can change over time. Although past research in the social psychology literature supports the assertion that personality characteristics are malleable (Helson *et al*, 2002; Roberts *et al*, 2006; Twenge *et al*, 2008), little focus within the security policy research has considered how this evolution may impact compliance. For example, organizations with an aging workforce may experience a different pattern of compliance issues (due to personality characteristics for that age group) compared to organizations with predominantly younger employees. Future research could consider questions such as: *How do the personality traits of the increasing number of Generation Y employees influence compliance with security policies?*

Revision 4: compliance–performance moderator

As noted in our results, we suggest that there is lack of empirical studies that clearly establish a link between compliance and the achievement of organizational objectives (e.g., reduced security incidents). Past commentators, including Doherty & Fulford (2005), have suggested possible factors that could influence this relationship, including excessively complex policies or inadequate resourcing. Our revised framework draws on elements of agency theory to propose the consideration of a moderator to the compliance–performance relationship. Although widely used in a variety of business disciplines, agency theory was surprisingly cited within only 3 of the 114 papers in our review. The theory is based around the relationship between two parties, the principal and agent, and the challenges that arise from their conflicting goals and the limited ability of the principal to oversee the agent's work (Eisenhardt, 1989). Past research drawing on agency theory is commonly oriented around the contract governing the principal–agent relationship and the mechanisms that can be used to limit the self-serving behavior of agents (Jensen and Meckling, 1976; Sharma, 1997; Zsidisin and Ellram,

2003). Where such a mechanism is framed as a policy that guides the behavior of employees to act in line with organizational objectives, agency theory can contribute to better understanding the compliance–performance relationship. In particular, although some limited research examines how policy compliance contributes positive organizational benefits, it is but one of the mechanisms available to principals in driving such benefits.

By employing agency concepts more broadly, future research could consider not only the factors other than security policies that aid in achieving security-oriented benefits (e.g., penetration testing, security audits), but also the factors that can moderate the relationship between a policy that is complied with at an organization and the resulting benefits. For example, where policies are in place, but are difficult to monitor and enforce, employees may be engaging in risky security behaviors without the knowledge of managers. This could include how such policies can be increasingly monitored (i.e., addressing the agency challenge of principals overseeing agent work), as well as alternative mechanisms that should be employed in such situations to supplement security policies, such as desktop monitoring (i.e., addressing the agency challenge of mechanisms to limit self-serving agent behavior). Research in this area could pose questions such as: *What factors reduce the positive relationship that security policy compliance has on organizational security performance?*

Revision 5: feedback loops

Past studies have considered the iterative nature of security policies to the extent that they are created and fine-tuned prior to and following implementation (see Relationship 1). However, as we note above, a gap exists in understanding how policies are changed following compliance problems (e.g., employees refusing to abide by a policy) or failed security objectives (e.g., a significant insider security breach). Although part of this gap is attributable to the cross-sectional focus noted in Revision 3, further theoretical viewpoints that can aid in addressing this gap are that of work systems theory (WST) and cybernetics. WST considers the circumstances where humans and machines perform work using information and technology, while accounting for the planned and unplanned changes that occur within such systems (Alter, 2013). Similarly, a cybernetic process is one that uses a feedback loop to set goals, determine achievement against those goals, and make ongoing corrections (Hofstede, 1978). Often associated with the study of budgeting, performance evaluation, and management accounting (Eisenhardt, 1985; Macintosh, 1994), cybernetics can be a simple and effective mechanism to iteratively identify and fix issues. The concept of work systems and cybernetics can apply to a wide range of business and technology activities within organizations, including the management of security policies. Past studies have proposed a life cycle model consisting of four steps, beginning with initiation, then followed by development, implementation, and finally operation and maintenance (Alter, 2008a, b). The steps flow sequentially, but rather than ending with operation and maintenance, the flow instead: (a) feeds back into initiation; (b) continues operating; or (c) terminates. Although the initiation, development, and implementation steps are captured within our Relationship 1, the remaining elements are largely unaccounted for within the security policy literature.

This potential research direction represents an important opportunity to examine more than just how policies are set up and adhered to by employees, but also how they are modified, updated, and customized based on experience and results. Such research could pose questions such as: *How do organizations adjust security policies following a data breach?*

Summary

The revised security policy research framework specified above outlines a series of opportunities to address gaps and inconsistencies in the current literature. We identify five proposed revisions that draw on unique theory foundations or approaches to add new constructs (e.g., control mode, degree, and style; compliance–performance moderator), relationships (e.g., the link between security policy design/implementation and legitimacy, fairness, and justice; feedback loops from compliance and organizational security objectives), and research approaches (e.g., replication and longitudinal research for personality links to compliance).

Conclusion

The objective of this research was to synthesize what we know and what remains to be learned about security policies by means of an overarching research framework that explains the key construct relationships, identifies knowledge gaps, and highlights future research directions. We follow Rowe's (2014) notion of a literature review for understanding by creating a concept-centric framework presented in temporal order that synthesizes current security policy research into five sets of relationships: (1) influences on the design and implementation of policies; (2) the influence of security policies on the organization and individual employees; (3) the influence of the organization and individual employee factors on policy compliance; (4) the influence of policy compliance on organizational objectives; and (5) adjustments to policy design. Based on gaps and inconsistencies identified in this framework, we propose a revised framework that highlights five key opportunities for future research directions. Although our results do not highlight an exhaustive listing of opportunities for future research, they represent a series of notable examples of gaps and ambiguities that currently exist in the field.

Our research makes several contributions. First, we establish the key constructs and relationships studied within the security policy research by means of an

updated review of the literature and a resultant research framework. Our security policy research framework synthesizes the wide range of topics, theories, and relationships between information security concepts, which can aid practitioners in more effectively designing, implementing, and overseeing security policies. From a research perspective, by focusing on interrelationships between key constructs, as opposed to the mainly descriptive and categorical approaches of extant reviews, we create structure in the security policy research domain and facilitate theory building efforts in this space. Notably, a distinguishing feature of our research framework is that it is structured in a temporal order, while simultaneously highlighting the cross-sectional factors that introduce variability into the relationship outcomes. By adopting this combined approach, we provide an important building block for future theory building that brings both process and variance perspectives to the study of security policies in organizations. We also highlight the gaps and inconsistencies from the existing security policy literature in our review. Although the current body of research has been valuable in shaping what we currently know about security policies in organizations, these gaps and inconsistencies highlight the areas where researchers can continue to make useful discoveries. Finally, we introduce a series of new directions that future research can focus on in the revised policy framework. The five identified areas provide specific directions that subsequent studies could adopt in order to address current gaps and continue to move the security policy research field forward.

About the Authors

W. Alec Cram is an Assistant Professor of Information and Process Management at Bentley University. He received a Ph.D. from Queen's University. Alec previously worked as an IT Audit Manager at Deloitte, where he received a CISSP and CISA. Alec 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. His work has been published or is forthcoming in outlets including the *Information Systems Journal*, *European Journal of Information Systems*, *Journal of the Association for Information Systems* and *Information and Management*.

Jeffrey G. Proudfoot is an Assistant Professor in the Information and Process Management Department at Bentley University. Jeff's research centers on information security and privacy with emphases on automated credibility assessment and insider threat detection. Jeff has contributed to over $1 million in Department of Homeland Security (DHS), Center for Identification Technology Research (CITeR), and National Science Foundation (NSF) grants, of which over $500 k was awarded with Jeff operating as a PI or a co-PI. His work has been published or is forthcoming in journals including the *Journal of Management Information Systems*, *Information Technology for Development*, *Journal of Nonverbal Behavior*, and *International Journal of Sociology and Social Policy*.

John D'Arcy is an Associate Professor in the Department of Accounting and MIS, Lerner College of Business and Economics, at the University of Delaware. He received his Ph.D. in Management Information Systems from Temple University. His research interests include information assurance and security, IT risk management, and computer ethics. His work appears in journals such as *Information Systems Research*, *Decision Sciences Journal*, *European Journal of Information Systems*, *Journal of Management Information Systems*, *MIT Sloan Management Review*, *Decision Support Systems*, and *Computers and Security*.

References

Aksulu A and Wade M (2010) A comprehensive review and synthesis of open source research. *Journal of the Association for Information Systems* 11(11), 576–656.

Al-Mukahal HM and Alshare K (2015) An examination of factors that influence the number of information security policy violations in qatari organizations. *Information and Computer Security* 23(1), 102–118.

Albrechtsen E (2007) A qualitative study of user's view on information security. *Computers and Security* 26(4), 276–289.

Alter S (2008a) Defining information systems as work systems: Implications for the IS field. *European Journal of Information Systems* 17(5), 448–469.

Alter S (2008b) Service system fundamentals: Work system, value chain, and life cycle. *IBM Systems Journal* 47(1), 71–85.

Alter S (2013) Work system theory: Overview of core concepts, extensions, and challenges for the future. *Journal of the Association for Information Systems* 14(2), 72–121.

Anderson CL and Agarwal R (2010) Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly* 34(3), 613–643.

Angst C, Block E, D'arcy J and Kelley K (2017) When do IT security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches. *MIS Quarterly* Forthcoming.

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), 201–222.

Backhouse J, Hsu CW and Silva L (2006) Circuits of power in creating de jure standards: Shaping an international information systems security standard. *MIS Quarterly* 30(Special Issue), 413–438.
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 Association for Information Systems* 34(8), 154–204.
Banerjee D, Cronan TP and Jones TW (1998) Modeling IT ethics: A study in situational ethics. *MIS Quarterly* 22(1), 31–60.
Barlow JB, Warkentin M, Ormond D and Dennis AR (2013) Don't make excuses! Discouraging neutralization to reduce IT policy violation. *Computers and Security* 39(Part B), 145–159.
Basin D, Jugé V, Klaedtke F and Zălinescu E (2013) Enforceable security policies revisited. *ACM Transactions on Information and System Security* 16(1), 1–26.
Baskerville R, Park EH and Kim J (2014) An emote opportunity model of computer abuse. *Information Technology and People* 27(2), 155–181.
Baskerville R and Siponen M (2002) An information security meta-policy for emergent organizations. *Logistics Information Management* 15(5/6), 337–346.
Bauer JM and Van Eeten MJG (2009) Cybersecurity: Stakeholder incentives, externalities, and policy options. *Telecommunications Policy* 33(10–11), 706–719.
Bauer L, Ligatti J and Walker D (2009) Composing expressive runtime security policies. *ACM Transactions on Software Engineering and Methodology* 18(3), 1–43.
Bijlsma-Frankema KM and Costa AC (2010) Consequences and antecedents of managerial and employee legitimacy interpretations of control: A natural open system approach. In Organizational Control (SITKIN SB, CARDINAL LB and BIJLSMA-FRANKEMA KM, Eds), pp 396–433, Cambridge University Press, Cambridge.
Boss SR, Galletta D, Moody GD, Lowry PB 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), 837–864.
Boss SR, Kirsch LJ, Angermeier I, Shingler RA and Boss RW (2009) If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. *European Journal of Information Systems* 18(2), 151–164.
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), 523–548.
Burns AJ, Roberts TL, Posey C and Lowry PB (2017) Examining the influence of organisational insiders' psychological capital on information security threat and coping appraisals. *Computers in Human Behavior* 68, 190–209.
Burton-Jones A, Mclean ER and Monod E (2015) Theoretical perspectives in IS research: From variance and process to conceptual latitude and conceptual fit. *European Journal of Information Systems* 24(6), 664–679.
Cairney P (2013) Standing on the shoulders of giants: How do we combine the insights of multiple theories in public policy studies? *The Policy Studies Journal* 41(1), 1–21.
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 and Security* 1(3), 18–41.
Chatterjee S, Sarker S and Valacich JS (2015) The behavioral roots of information systems security: Exploring key factors related to unethical IT use. *Journal of Management Information Systems* 31(4), 49–87.
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), 157–188.
Chen Y, Ramamurthy K and Wen K-W (2015) Impacts of comprehensive information security programs on information security culture. *The Journal of Computer Information Systems* 55(3), 11–19.
Chen Y and Zahedi FM (2016) Individuals' internet security perceptions and behaviors: Polycontextual contrasts between the United States and China. *MIS Quarterly* 40(1), 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 and Security* 39, 447–459.
Choudhury V and Sabherwal R (2003) Portfolios of control in outsourced software development projects. *Information Systems Research* 14(3), 291–314.
Chu AMY, Chau PYK and So MKP (2015) Developing a typological theory using a quantitative approach: A case of information security deviant behavior. *Communications of the AIS* 37(25), 510–535.
Chu MY, So MKP and Chung RSW (2016) Applying the randomized response technique in business ethics research: The misuse of information systems resources in the workplace. *Journal of Business Ethics* Online Early, 1–18.
Chua CEH, Lim W-K, Soh C and Sia SK (2012) Enacting clan control in complex IT projects: A social capital perspective. *MIS Quarterly* 36(2), 577–600.
Cram WA, Brohman MK and Gallupe RB (2016a) Hitting a moving target: A process model of information systems control change. *Information Systems Journal* 26(3), 195–226.
Cram WA, Brohman MK and Gallupe RB (2016b) Information systems control: A review and framework for emerging information systems. *Journal of the Association for Information Systems* 17(4), 216–266.
Cronan TP and Douglas DE (2006) Toward a comprehensive ethical behavior model for information technology. *Journal of Organizational and End User Computing* 18(1), 1–11.
Crossler RE and Bélanger F (2009) The effects of security education training and awareness programs and individual characteristics on end user security tool usage. *Journal of Information System Security* 5(3), 3–22.
Crossler RE, Johnston AC, Lowry PB, Hu Q, Warkentin M and Baskerville R (2013) Future directions for behavioral information security research. *Computers and Security* 32, 90–101.
Crossler RE, Long JH, Loraas TM and Trinkle BS (2014) Understanding compliance with bring your own device policies utilizing protection motivation theory: Bridging the intention-behavior gap. *Journal of Information Systems* 28(1), 209–226.
Culnan MJ and Williams CC (2009) How ethics can enhance organizational privacy: Lessons from the Choicepoint and TJX data breaches. *MIS Quarterly* 33(4), 673–687.
Cuppens F, Cuppens-Boulahia N and Elrakaiby Y (2013) Formal specification and management of security policies with collective group obligations. *Journal of Computer Security* 21(1), 149–190.
D'arcy J and Devaraj S (2012) Employee misuse of information technology resources: Testing a contemporary deterrence model. *Decision Sciences* 43(6), 1091–1124.
D'arcy J and Greene G (2014) Security culture and the employment relationship as drivers of employees' security compliance. *Information Management and Computer Security* 22(5), 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), 643–658.
D'arcy J, Herath T and Shoss MK (2014) Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of Management Information Systems* 31(2), 285–318.
D'arcy J and Hovav A (2007) Deterring internal information systems abuse. *Communications of the ACM* 50(10), 113–117.
D'arcy J, Hovav A and Galletta D (2009) User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research* 20(1), 79–98.
David J (2002) Policy enforcement in the workplace. *Computers and Security* 21(6), 506–513.
Davis RC (1940) Industrial Organization and Management. Harper, New York.
Dhillon G (1997) Managing Information Security. Macmillan, London.
Dhillon G and Backhouse J (2000) Information system security management in the new millennium. *Communications of the ACM* 43(7), 125–128.
Dhillon G and Backhouse J (2001) Current directions in IS security research: Towards socio-organizational perspectives. *Information Systems Journal* 11(2), 127–153.
Di Modica G and Tomarchio O (2016) Matchmaking semantic security policies in heterogeneous clouds. *Future Generation Computer Systems* 55, 176–185.

DIMAGGIO PJ (1988) Interest and agency in institutional theory. In Institutional patterns and organizations (ZUCKER LG, Ed), pp 3–21, Ballinger, Cambridge.

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), 391–412.

DINEV T and HU Q (2007) The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems* 8(7), 386–408.

DOHERTY NF, ANASTASAKIS L and FULFORD H (2009) The information security policy unpacked: A critical study of the content of university policies. *International Journal of Information Management* 29(6), 449–457.

DOHERTY NF and FULFORD H (2005) Do information security policies reduce the incidence of security breaches: An exploratory analysis. *Information Resources Management Journal* 18(4), 21–39.

DOHERTY NF and FULFORD H (2006) Aligning the information security policy with the strategic information systems plan. *Computers and Security* 25(1), 55–63.

EISENHARDT KM (1985) Control: Organizational and economic approaches. *Management Science* 31(2), 134–149.

EISENHARDT KM (1989) Agency theory: An assessment and review. *Academy of Management Review* 14(1), 57–74.

EVANSCHITZKY H and ARMSTRONG JS (2013) Research with in-built replications: Comment and further suggestions for replication research. *Journal of Business Research* 66(9), 1406–1408.

FLAMHOLTZ EG, DAS TK and TSUI AS (1985) Toward and integrative framework of organizational control. *Accounting, Organizations and Society* 10(1), 35–50.

FLOWERDAY SV and TUYIKEZE T (2016) Information security policy development and implementation: The what, how and who. *Computers and Security* 61, 169–183.

FOLEY SN and FITZGERALD WM (2011) Management of security policy configuration using a semantic threat graph approach. *Journal of Computer Security* 19(3), 567–605.

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), 91–109.

FULFORD H and DOHERTY NF (2003) The application of information security policies in large UK-based organizations: An exploratory investigation. *Information Management & Computer Security* 11(3), 106–114.

GAUNT N (1998) Installing an appropriate information security policy. *International Journal of Medical Informatics* 49(1), 131–134.

GOEL S and CHENGALUR-SMITH IN (2010) Metrics for characterizing the form of security policies. *Journal of Strategic Information Systems* 19(4), 281–295.

GOO J, YIM M-S and KIM DJ (2014) A path to successful management of employee security compliance: An empirical study of information security climate. *IEEE Transactions on Professional Communication* 57(4), 286–308.

GOPAL A and GOSAIN S (2010) The role of organizational controls and boundary spanning in software development outsourcing: Implications for project performance. *Information Systems Research* 21(4), 1–23.

GRAHLMANN KR, HELMS RW, HILHORST C, BRINKKEMPER S and VAN AMERONGEN S (2012) Reviewing enterprise content management: A functional framework. *European Journal of Information Systems* 21(3), 268–286.

GREGORY RW, BECK R and KEIL M (2013) Control balancing in information systems development offshoring projects. *MIS Quarterly* 37(4), 1211–1232.

GRITZALIS D (1997) A baseline security policy for distributed healthcare information systems. *Computers and Security* 16(8), 709–719.

GUO KH (2013) Security-related behavior in using information systems in the workplace: A review and synthesis. *Computers and Security* 32, 242–251.

GUO KH and YUAN Y (2012) The effects of multilevel sanctions on information security violations: A mediating model. *Information and Management* 49(6), 320–326.

GUO KH, YUAN Y, ARCHER NP and CONNELLY CE (2011) Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems* 28(2), 203–236.

HAN J, KIM YJ and KIM H (2017) An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective. *Computers and Security* 66, 52–65.

HARRINGTON SJ (1996) The effect of codes of ethics and personal denial of responsibility on computer abuse judgements and intentions. *MIS Quarterly* 20(3), 257-278.

HASSAN NR (2014) Useful products in theorizing for information systems. In *Thirty Fifth International Conference on Information Systems* pp 1–21, Auckland.

HASSAN NR and LOWRY PB (2015) Seeking middle-range theories in information systems research. In *Thirty Sixth International Conference on Information Systems* pp 1–19, Fort Worth.

HEDSTRÖM K, KOLKOWSKA E, KARLSSON F and ALLEN J (2011) Value conflicts for information security management. *Journal of Strategic Information Systems* 20(4), 373–384.

HELSON R, JONES C and KWAN VSY (2002) Personality change over 40 years of adulthood: Hierarchical linear modeling analyses of two longitudinal samples. *Journal of Personality and Social Psychology* 83(3), 752–766.

HERATH T, CHEN R, WANG J, BANJARA K, WILBUR J and RAO HR (2014) Security services as coping mechanisms: An investigation into user intention to adopt an email authentication service. *Information Systems Journal* 24(1), 61–84.

HERATH T and RAO HR (2009a) Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems* 47(2), 154–165.

HERATH T and RAO HR (2009b) Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems* 18(2), 106–125.

HICKS B, RUEDA S, ST. CLAIR L, JAEGER T and MCDANIEL P (2010) A logical specification and analysis for SELinux MLS policy. *ACM Transactions on Information and System Security* 13(3), 1–31.

HOFSTEDE G (1978) The poverty of management control philosophy. *Academy of Management Review* 3(3), 450–461.

HÖNE K and ELOFF JHP (2002a) Information security policy—what do international information security standards say? *Computers and Security* 21(5), 402–409.

HÖNE K and ELOFF JHP (2002b) What makes an effective information security policy? *Network Security* 20(6), 14–16.

HONG K-S, CHI Y-P, CHAO LR and TANG J-H (2006) An empirical study of information security policy on information security elevation in Taiwan. *Information Management and Computer Security* 14(2), 104–115.

HORCAS J-M, PINTO M, FUENTES L, MALLOULI W and MONTES DE OCA E (2016) An approach for deploying and monitoring dynamic security policies. *Computers and Security* 58, 20–38.

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 and Management* 49(2), 99–110.

HSU JS-C, SHIH S-P, HUNG YW and LOWRY PB (2015) The role of extra-role behaviors and social controls in information security policy effectiveness. *Information Systems Research* 26(2), 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), 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), 6–48.

HU Q, XU Z, DINEV T and LING H (2011) Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM* 54(6), 54–60.

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), 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 and Security* 31(1), 83–95.

IFINEDO P (2014) Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information and Management* 51(1), 69–79.

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), 30–41.
International Organization For Standardization (2016) ISO/IEC 27000:2016. https://www.iso.org, accessed 30 January 2016.
Jaffee D (1991) Organization Theory: Tension and Change. McGraw-Hill, New York.
Jajodia S, Samarati P, Sapino ML and Subrahmanian VS (2001) Flexible support for multiple access control policies. *ACM Transactions on Database Systems* 26(2), 214–260.
Jensen M and Meckling W (1976) Theory of the firm: Managerial behavior, agency costs, and ownership structure. *Journal of Financial Economics* 3(4), 305–360.
Johnston AC and Warkentin M (2010a) Fear appeals and information security behaviors: An empirical study. *MIS Quarterly* 34(3), 549–566.
Johnston AC and Warkentin M (2010b) The influence of perceived source credibility on end user attitudes and intentions to comply with recommended IT actions. *Journal of Organizational and End User Computing* 22(3), 1–21.
Johnston AC, 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), 231–251.
Johnston AC, 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), 113–134.
Johnston AC, Wech B and Jack E (2013) Engaging remote employees: The moderating role of "remote" status in determining employee information security policy awareness. *Journal of Organizational and End User Computing* 25(1), 1–23.
Kadam AW (2007) Information security policy development and implementation. *Information Systems Security* 16(5), 246–256.
Kankanhalli A, Teo H-H, Tan BCY and Wei K-K (2003) An integrative study of information systems security effectiveness. *International Journal of Information Management* 23(2), 139–154.
Karjalainen M and Siponen M (2011) Toward a new meta-theory for designing information systems (IS) security training approaches. *Journal of the Association for Information Systems* 12(8), 518–555.
Karlsson F, Åström J and Karlsson M (2015) Information security culture—state-of-the-art review between 2000 and 2013. *Information and Computer Security* 23(3), 246–285.
Karyda M, Kiountouzis E and Kokolakis S (2005) Information systems security policies: A contextual perspective. *Computers and Security* 24(3), 246–260.
Khoury R and Tawbi N (2012) Corrective enforcement: A new paradigm of security policy enforcement by monitors. *ACM Transactions on Information and System Security* 15(2), 1–27.
Kiel JM, Ciamacco FA and Steines BT (2016) Privacy and data security: HIPAA and HITECH. In Healthcare information management systems (WEAVER CA, BALL MJ, KIM GR and KIEL JM, Eds), pp 437–449, Springer, New York.
Kim J, Park EH and Baskerville R (2016) A model of emotion and computer abuse. *Information and Management* 53(1), 91–108.
King NJ and Raja VT (2012) Protecting the privacy and security of sensitive customer data in the cloud. *Computer Law and Security Review* 28(3), 308–319.
King WR and He J (2005) Understanding the role and methods of meta-analysis in IS research. *Communications of the Association for Information Systems* 16(32), 665–696.
Kirsch LJ (1997) Portfolios of control modes and IS project management. *Information Systems Research* 8(3), 215–239.
Kirsch LJ, Ko D-G and Haney MH (2010) Investigating the antecedents of team-based clan control: Adding social capital as a predictor. *Organization Science* 21(2), 469–489.
Knapp KJ and Ferrante CJ (2012) Policy awareness, enforcement and maintenance: Critical to information security effectiveness in organizations. *Journal of Management Policy and Practice* 13(5), 66–80.
Knapp KJ, Marshall TE, Rainer RK and Ford FN (2006) Information security: Management's effect on culture and policy. *Information Management and Computer Security* 14(1), 24–36.
Knapp KJ, Morris RFJ, Marshall TE and Byrd TA (2009) Information security policy: An organizational-level process model. *Computers and Security* 28(7), 493–508.
Koops B-J (2014) The trouble with European data protection law. *International Data Privacy Law* 4(4), 250–261.
Landoll DJ (2016) Information Security Policies, Procedures, and Standards. CRC Press, Boca Raton.
Langley A (1999) Strategies for theorizing from process data. *Academy of Management Review* 24(4), 691–710.
Lebek B, Uffen J, Breitner MH, Neumann M and Hohler B (2013) Employees' information security awareness and behavior: A literature review. In *46th Hawaii International Conference on System Sciences* pp 2978–2986, Maui, Hawaii.
Lebek B, Uffen J, Neumann M, Hohler B and Breitner MH (2014) Information security awareness and behavior: A theory-based literature review. *Management Research Review* 37(12), 1049–1092.
Lee C, Lee CC and Kim S (2016) Understanding information security stress: Focusing on the type of information security compliance activity. *Computers and Security* 59(1), 60–70.
Lee J and Lee Y (2002) A holistic model of computer abuse within organizations. *Information Management and Computer Security* 10(2), 57–63.
Lee SM, Lee S-G and Yoo S (2004) An integrative model of computer abuse based on social control and general deterrence theories. *Information and Management* 41(6), 707–718.
Lee Y and Larson KR (2009) Threat or coping appraisal: Determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems* 18(2), 177–187.
Leidner DE and Kayworth T (2006) A review of culture in information systems research: Toward a theory of information technology culture conflict. *MIS Quarterly* 30(2), 357–399.
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), 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), 635–645.
Li N and Wang Q (2008) Beyond separation of duty: An algebra for specifying high-level security policies. *Journal of the ACM* 55(3), 1–46.
Liang H and Xue Y (2009) Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly* 33(1), 71–90.
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), 394–413.
Liang H, Xue Y and Wu L (2013) Ensuring employees' IT compliance: Carrot or stick? *Information Systems Research* 24(2), 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), 49–59.
Lindsay RM and Ehrenberg ASC (1993) The design of replicated studies. *The American Statistician* 47(3), 217–222.
Liu C-C (2015) Types of employee perceptions of information security using Q methodology: An empirical study. *European Journal of Information Systems* 10(4), 557–575.
Liu J, Li Y, Wang H, Jin D, Su L, Zeng L and Vasilakos T (2016) Leveraging software-defined networking for security policy enforcement. *Information Sciences* 327, 288–299.
Lowry PB and Moody GD (2015) Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies. *Information Systems Journal* 25(5), 465–488.
Lowry PB, Posey C, Bennett RJ and Roberts TL (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), 193–230.
Lowry PB, Posey C, Roberts TL and Bennett RJ (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), 385–401.
Macintosh NB (1994) Management Accounting and Control Systems: An Organizational and Behavioral Approach. Wiley, New York.
Maruping LM, Venkatesh V and Agarwal R (2009) A control theory perspective on agile methodology use and changing user requirements. *Information Systems Research* 20(3), 377–399.

Mcdaniel P and Prakash A (2006) Methods and limitations of security policy reconciliation. *ACM Transactions on Information and System Security* 9(3), 259–291.

Mehra SK (2010) Law and cybercrime in the United States today. *The American Journal of Comparative Law* 58, 659–685.

Meyer JW and Rowan B (1977) Institutional organizations: Formal structure as a myth and ceremony. *American Journal of Sociology* 83(2), 340–363.

Mezias SJ and Regnier MO (2007) Walking the walk as well as talking the talk: Replication and the normal science paradigm in strategic management research. *Strategic Organization* 5(3), 283–296.

Montanari M, Chan E, Larson K, Yoo W and Campbell RH (2013) Distributed security policy conformance. *Computers and Security* 33, 28–40.

Moody GD, Kirsch LJ, Slaughter SA, Dunn BK and Weng Q (2016) Facilitating the transformational: An exploration of control in cyber-infrastructure projects and the discovery of field control. *Information Systems Research* 27(2), 324–346.

Moores TT and Chang JC-J (2006) Ethical decision making in software piracy: Initial development and test of a four-component model. *MIS Quarterly* 30(1), 167–180.

Moquin R and Wakefield RL (2016) The roles of awareness, sanctions, and ethics in software compliance. *The Journal of Computer Information Systems* 56(3), 261–270.

Muthaiyah S and Kerschberg L (2007) Virtual organization security policies: An ontology-based integration approach. *Information Systems Frontiers* 9(5), 505–514.

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), 126–139.

Ng B-Y, Kankanhalli A and Xu Y (2009) Studying users' computer security behavior: A health belief perspective. *Decision Support Systems* 46(4), 815–825.

Niehoff BP and Moorman RH (1993) Justice as a mediator of the relationship between methods of monitoring and organizational citizenship behavior. *Academy of Management Journal* 36(3), 527–556.

Osenga K (2013) The internet is not a super highway: Using metaphors to communicate information and communications policy. *Journal of Information Policy* 3(1), 30–54.

Padayachee K (2012) Taxonomy of compliant information security behavior. *Computers and Security* 31(5), 673–680.

Paré G, Tate M, Johnstone D and Kitsiou S (2016) Contextualizing the twin concepts of systematicity and transparency in information systems literature reviews. *European Journal of Information Systems* 25(6), 493–508.

Paré G, Trudel M-C, Jaana M and Kitsiou S (2015) Synthesizing information systems knowledge: A typology of literature reviews. *Information and Management* 52(2), 183–199.

Pathari V and Sonar R (2012) Identifying linkages between statements in information security policy, procedures and controls. *Information Management and Computer Security* 20(4), 264–280.

Peace AG, Galletta DF and Thong JYL (2003) Software piracy in the workplace: A model and empirical test. *Journal of Management Information Systems* 20(1), 153–177.

Perrow C (1986) Complex Organizations. Random House, New York.

Phelps DC, Gathegi JN, Workman M and Heo M (2012) Information system security: Self-efficacy and implementation effectiveness. *Journal of Information System Security* 8(1), 3–21.

Posey C, Bennett RJ and Roberts TL (2011a) Understanding the mindset of the abusive insider: An examination of insiders' causal reasoning following internal security changes. *Computers and Security* 30(6–7), 486–497.

Posey C, Bennett RJ, Roberts TL and Lowry PB (2011b) When computer monitoring back-fires: Privacy invasions and organizational injustice as precursors to computer abuse. *Journal of Information System Security* 7(1), 24–47.

Posey C, Roberts TL and Lowry PB (2015) The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems* 32(4), 179–214.

Posey C, Roberts TL, Lowry PB, Bennett RJ and Courtney JF (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), 1189–1210.

Puhakainen P and Siponen M (2010) Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly* 34(4), 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, accessed 30 January 2017.

Rees J, Bandyopadhyay S and Spafford EH (2003) PFIRES: A policy framework for information security. *Communications of the ACM* 46(7), 101–106.

Remus U, Wiener M, Mähring M, Saunders C and Cram WA (2015) Why do you control? The concept of control purpose and its implications for IS project control research. In *Thirty Sixth International Conference on Information Systems* pp 1–19, Fort Worth.

Renaud K and Goucher W (2012) Health service employees and information security policies: An uneasy partnership? *Information Management and Computer Security* 20(4), 296–311.

Rhee H-S, Kim C and Ryu YU (2009) Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers and Security* 28(8), 816–826.

Roberts BW, Walton KE and Viechtbauer W (2006) Patterns of mean-level change in personality traits across the life course: A meta-analysis of longitudinal studies. *Psychological Bulletin* 132(1), 1–25.

Ross SJ (2015) Cybersecurity for a "simple" auditor. *ISACA Journal* 6(6), 1–2.

Rowe F (2014) What literature review is not: Diversity, boundaries and recommendations. *European Journal of Information Systems* 23(3), 241–255.

Sabherwal R and Robey D (1995) Reconciling variance and process strategies for studying information systems development. *Information Systems Research* 6(4), 303–327.

Safa NS, Von Solms R and Furnell S (2016) Information security policy compliance model in organizations. *Computers and Security* 56(1), 70–82.

Salterio SE (2014) We don't replicate accounting research—or do we? *Contemporary Accounting Research* 31(4), 1134–1142.

Santana M and Robey D (1995) Perceptions of control during systems development: Effects on job satisfaction of systems professionals. *Computer Personnel* 16(1), 20–34.

Schmerken I (2015) Morgan Stanley data theft exposes insider threat & need for more restrictions. http://www.wallstreetandtech.com/security/morgan-stanley-data-theft-exposes-insider-threat-and-need-for-more-restrictions, accessed 30 January 2015.

Schnedler W and Vadovic R (2011) Legitimacy of control. *Journal of Economics and Management Strategy* 20(4), 985–1009.

Schneider FB (2000) Enforceable security policies. *ACM Transactions on Information and System Security* 3(1), 30–50.

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), 286–325.

Scott WR (1987) The adolescence of institutional theory. *Administrative Science Quarterly* 32(4), 493–511.

Sharma A (1997) Professional as agent: Knowledge asymmetry in agency exchange. *Academy of Management Review* 22(3), 758–798.

Shephard MM and Mejias RJ (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), 557–567.

Shirtz D and Elovici Y (2011) Optimizing investment decisions in selecting information security remedies. *Information Management and Computer Security* 19(2), 95–112.

Shropshire J, Warkentin M and Sharma S (2015) Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers and Security* 49, 177–191.

Silva L, Hsu C, Backhouse J and Mcdonnell A (2016) Resistance and power in a security certification scheme: The case of c:Cure. *Decision Support Systems* 92, 68–78.

Siponen M (2000) A conceptual foundation for organizational information security awareness. *Information Management and Computer Security* 8(1), 31–41.

Siponen M (2006) Information security standards focus on the existence of process, not its content. *Communications of the ACM* 49(8), 97–100.

Siponen M and Iivari J (2006) Six design theories for IS security policies and guidelines. *Journal of the Association for Information Systems* 7(7), 445–472.
Siponen M, Mahmood MA and Pahnila S (2009) Are employees putting your company at risk by not following information security policies? *Communications of the ACM* 52(12), 145–147.
Siponen M, Mahmood MA and Pahnila S (2014) Employees' adherence to information security policies: An exploratory field study. *Information and Management* 51(2), 217–224.
Siponen M and Oinas-Kukkonen H (2007) A review of information security issues and respective research contributions. *The DATA BASE for Advances in Information Systems* 38(1), 60–80.
Siponen M, Pahnila S and Mahmood MA (2010) Compliance with information security policies: An empirical investigation. *Computer* 43(2), 64–71.
Siponen M and Vance A (2010) Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly* 34(3), 487–502.
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), 289–305.
Siponen M and Willison R (2009) Information security management standards: Problems and solutions. *Information and Management* 46(5), 267–270.
Siponen M, Willison R and Baskerville R (2008) Power and practice in information systems security research. In *International Conference on Information Systems* pp 1–13, Association for Information Systems, Paris.
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), 463–486.
Sommestad T, Hallberg J, Lundholm K and Bengtsson J (2014) Variables influencing information security policy compliance: A systematic review of quantitative studies. *Information Management and Computer Security* 22(1), 42–75.
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), 200–217.
Son J-Y (2011) Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information and Management* 48(7), 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), 309–321.
Soomro ZA, Shah MH and Ahmed J (2016) Information security management needs more holistic approach: A literature review. *International Journal of Information Management* 36(2), 215–225.
Spears JL and Barki H (2010) User participation in information systems security risk management. *MIS Quarterly* 34(3), 503–522.
Stahl BC, Doherty NF and Shaw M (2012) Information security policies in the uk healthcare sector: A critical evaluation. *Information Systems Journal* 22(1), 77–94.
Stanton J, Stam K, Mastrangelo P and Jolton J (2005) Analysis of end user security behaviors. *Computers and Security* 24(2), 124–133.
Straub DW (1990) Effective IS security: An empirical study. *Information Systems Research* 1(3), 255–276.
Straub DW and Nance WD (1990) Discovering and disciplining computer abuse in organizations: A field study. *MIS Quarterly* 14(1), 45–62.
Straub DW and Welke RJ (1998) Coping with systems risk: Security planning models for management decision making. *MIS Quarterly* 22(4), 441–469.
Susanto H, Almunawar MN and Tuan YC (2011) Information security management system standards: A comparative study of the big five. *International Journal of Electrical and Computer Sciences* 11(5), 23–29.
Tang M, Li M and Zhang T (2016) The impacts of organizational culture on information security culture: A case study. *Information Technology and Management* 17(2), 179–186.
Tannenbaum AS (1962) Control in organizations: Individual adjustment and organizational performance. *Administrative Science Quarterly* 7(2), 236–257.
Teh P-L, Ahmed PK and D'arcy J (2015) What drives information security policy violations among banking employees? Insights from neutralization and social exchange theory. *Journal of Global Information Management* 23(1), 44–64.
Thomson K-L (2010) Information security conscience: A precondition to an information security culture? *Journal of Information System Security* 6(4), 3–19.
Thong JYL and Yap CS (1998) Testing an ethical decision-making theory: The case of softlifting. *Journal of Management Information Systems* 15(1), 213–237.
Tiwana A and Keil M (2009) Control in internal and outsourced software projects. *Journal of Management Information Systems* 26(3), 9–44.
Tsang EWK and Kwan K-M (1999) Replication and theory development in organizational science: A critical realist perspective. *Academy of Management Review* 24(4), 759–780.
Tsohou A, Karyda M and Kokolakis S (2015a) Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs. *Computers and Security* 52, 128–141.
Tsohou A, Karyda M, Kokolakis S and Kiountouzis E (2010) Aligning security awareness with information system security management. *Journal of Information System Security* 6(1), 36–54.
Tsohou A, Karyda M, Kokolakis S and Kiountouzis E (2015b) Managing the introduction of information security awareness programmes in organizations. *European Journal of Information Systems* 24(1), 38–58.
Twenge JM, Konrath S, Foster JD, Campbell WK and Bushman BJ (2008) Egos inflating over time: A cross-temporal meta-analysis of the narcissistic personality inventory. *Journal of Personality and Social Psychology* 76(4), 875–902.
Unal D and Caglayan MU (2013) A formal role-based access control model for security policies in multi-domain mobile networks. *Computer Networks* 57(1), 330–350.
Uzunov AV, Fernandez EB and Falkner K (2015) Security solution frames and security patterns for authorization in distributed, collaborative systems. *Computers and Security* 55(1), 193–234.
Vaast E (2007) Danger is in the eye of the beholders: Social representations of information systems security in healthcare. *Journal of Strategic Information Systems* 16(2), 130–152.
Van Iddekinge CH, Ferris GR and Heffner TS (2009) Test of a multistage model of distal and proximal antecedents of leader performance. *Personnel Psychology* 62(3), 463–495.
Vance A, Anderson BB, Kirwan CB and Eargle D (2014) Using measures of risk perception to predict information security behavior: Insights from electroencephalography (EEG). *Journal of the Association for Information Systems* 15(10), 679–722.
Vance A, Lowry PB and Eggett D (2013) Using accountability to reduce access policy violations in information systems. *Journal of Management Information Systems* 29(4), 263–289.
Vance A, Lowry PB 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), 345–366.
Vance A and Siponen M (2012) IS security policy violations: A rational choice perspective. *Journal of Organizational and End User Computing* 24(1), 21–41.
Vance A, Siponen M and Pahnila S (2012) Motivating IS security compliance: Insights from habit and protection motivation theory. *Information and Management* 49(3–4), 190–198.
Verizon (2016) 2016 data breach investigations report. http://www.verizonenterprise.com/DBIR/2015/, accessed 25 February 2017.
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 Association for Information Systems* 37(9), 205–224.
Von Dran GM, Guynes CS and Prybutok VR (1996) The information infrastructure: Policy and security considerations. *Computers and Society* 26(1), 13–15.
Von Solms R (1999) Information security management: Why standards are important. *Information Management and Computer Security* 7(1), 50–57.
Vroom C and Von Solms R (2004) Towards information security behavioural compliance. *Computers and Security* 23(3), 191–198.
Wall DS (2013) Enemies within: Redefining the insider threat in organizational security policy. *Security Journal* 26(2), 107–124.
Wall JD, Lowry PB and Barlow JB (2016) Organizational violations of externally governed privacy and security rules: Explaining and

predicting selective violations under conditions of strain and excess. *Journal of the Association for Information Systems* 17(1), 39–76.
Wall JD, Palvia P and Lowry PB (2013) Control-related motivations and information security policy compliance: The role of autonomy and efficacy. *Journal of Information Privacy and Security* 9(4), 52–79.
Wall JD, Stahl BC and Salam AF (2015) Critical discourse analysis as a review methodology: An empirical example. *Communications of the Association for Information Systems* 37(1), 257–285.
Warkentin M, Johnston AC 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), 267–284.
Warkentin M, Johnston AC, Shropshire J and Barnett WD (2016a) Continuance of protective security behavior: A longitudinal study. *Decision Support Systems* 92, 25–35.
Warkentin M, Walden E, Johnston AC and Straub DW (2016b) Neural correlates of protection motivation for secure IT behaviors: An fMRI examination. *Journal of the Association for Information Systems* 17(3), 194–215.
Warman AR (1992) Organizational computer security policy: The reality. *European Journal of Information Systems* 1(5), 305–310.
Webster J and Watson RT (2002) Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly* 26(2), xiii–xxiii.
Weldon D (2015) Are your biggest security threats on the inside? http://www.cio.com/article/2985790/security/are-your-biggest-security-threats-on-the-inside.html, accessed 1 December 2015.
Whitman ME (2008) Security policy: From design to maintenance. In Information security: Policy, processes, and practices (Straub DW, Goodman SE and Baskerville R, Eds), pp 123–151, M. E. Sharpe, New York.
Whitman ME, Townsend AM and Aalberts RJ (2001) Information systems security and the need for policy. In Information security management: Global challenges in the new millennium (DHILLON G, Ed), pp 10–20, IGI Global, Hershey PA.
Wiant TL (2005) Information security policy's impact on reporting security incidents. *Computers and Security* 24(6), 448–459.
Wiener M, Mähring M, Remus U and Saunders C (2016) Control configuration and control enactment in information systems projects: Review and expanded theoretical framework. *MIS Quarterly* 40(3), 741–774.
Willison R (2006) Understanding the perpetration of employee computer crime in the organisational context. *Information and Organization* 16(4), 304–324.
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), 403–414.
Willison R and Warkentin M (2013) Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly* 37(1), 1–20.
Wood CC (1982) Policies for deterring computer abuse. *Computers and Security* 1(2), 139–145.
Workman M (2009) A field study of corporate employee monitoring: Attitudes, absenteeism, and the moderating influences of procedural justice perceptions. *Information and Organization* 19(4), 218–232.
Workman M, Bommer WH and Straub DW (2008) Security lapses and the omission of information securitymeasures: A threat control model and empirical test. *Computers in Human Behavior* 24(6), 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), 212–222.
Xue Y, Liang H and Wu L (2011) Punishment, justice, and compliance in mandatory IT settings. *Information Systems Research* 22(2), 400–414.
Yazdanmehr A and Wang J (2016) Employees' information security policy compliance: A norm activation perspective. *Decision Support Systems* 92, 36–46.
Zafar H and Clark JG (2009) Current state of information security research in IS. *Communications of the AIS* 24(34), 557–596.
Zhang J, Reithel BJ and Li H (2009) Impact of perceived technical protection on security behaviors. *Information Management and Computer Security* 17(4), 330–340.
Zhang X, Parisi-Presicce F, Sandhu R and Park J (2005) Formal model and policy specification of usage control. *ACM Transactions on Information and System Security* 8(4), 351–387.
Zsidisin GA and Ellram LM (2003) An agency theory investigation of supply risk management. *Journal of Supply Chain Management* 39(3), 15–27.

Appendix A: Security policy research literature reviews

The following is not an exhaustive list of IS security research literature reviews, as there are additional reviews that are only tangentially related to security policy research and/or appear in lower-tier journals and conference proceedings.

Article	*Coverage*	*Description/key findings*	*How our review differs in scope**
Crossler *et al* (2013)	Overview of behavioral IS security literature; not a systematic review paper	Using the extant literature as a base, proposed the following topics for future behavioral IS security research: separating insider deviant behavior from insider misbehavior; unmasking the mystery of the hacker world; improving information security compliance; cross-cultural information security research	We review the broader body of security policy literature
D'Arcy and Herath (2011)	17 empirical studies in the IS literature that used deterrence (sanction) constructs, published through 2010 (approximately); specific time period not provided	Reviewed empirical studies that used deterrence theory in the IS literature; in an attempt to explain the contradictory findings in this literature, identified contingency variables, and methodological and theoretical issues specific to the application of deterrence theory in the IS context	We review the broader body of security policy literature
Dhillon and Backhouse (2001)	IS security literature through 2000 (approximately); specific number of articles and time period not provided	Classified IS security literature into Burrell and Morgan's sociological paradigms (functionalist, interpretive, radical humanist, radical structuralist); one of the earliest papers to identify the preponderance of purely technical IS security research and called for a socioorganizational perspective	We review the more specific body of security policy literature

Article	*Coverage*	*Description/key findings*	*How our review differs in scope**
Guo (2013)	Not a systematic review paper; literature on employees' security-related behavior; specific number of articles and time period not provided	Provided a classification/taxonomy of employees' security-related behavior, based on the extant literature	We review the broader body of security policy literature
Karlsson *et al* (2015)	72 information security culture research articles published between 2000 and 2013	Classified the papers in terms of theories, research methods, and research topics	We review the security policy literature, which is distinct from security culture research
Lebek *et al* (2013); Lebek *et al* (2014)	113 articles on employees' information security awareness and behavior published between 2000 and mid 2012 (both the 2013 and 2014 publications cover the same scope)	Classified 54 different theories used in behavioral IS security studies; based on the results, provided a taxonomy of antecedents of information security behavior	We review the broader body of security policy literature
Padayachee (2012)	Not a systematic review paper; overview of selected literature on employees' security policy compliance; specific number of articles and time period not provided	Provided a taxonomy of factors that influence employees' security policy compliance, which was derived from the literature and grounded in self-determination theory	We review the broader body of security policy literature
Siponen and Oinas-Kukkonen (2007)	IS security literature through 2000; specific number of articles not provided	Classified the papers based on research approaches, reference disciplines, and security issues (access to information systems, secure communication, security management, secure information systems development)	We review the more specific body of security policy literature
Siponen & Vance (2014)	19 empirical, survey studies of employees' security policy compliance, published between 1990 and 2011	Provided methodological guidelines for survey studies of security policy compliance behavior in organizations; the guidelines were applied to the reviewed articles, and no study met more than three of the five proposed guidelines.	We review the broader body of security policy literature
Siponen *et al* (2008)	1280 IS security research articles published between 1990 and 2004	Classified the papers in terms of theories, research methods, and research topics	We review the more specific body of security policy literature
Sommestad *et al* (2014)	29 empirical studies of employees' security policy compliance published through 2012 (approximately); specific time period not provided	Meta-analyzed the literature on employees' security policy compliance; showed the relative strength of the various predictor variables used in the literature (60 total predictor variables)	We review the broader body of security policy literature
Soomro *et al* (2016)	67 articles on management role in information security published between 2004 and September 2014	Classified the papers into the following categories: information security and management; information security policy awareness and training; integration of technical and managerial activities for information security management; human aspects of information security management; information security as a business issue	We review the more specific body of security policy literature
Wall *et al* (2015)	24 empirical studies of employees' security-related behavior published between 2002 and 2012	Evaluated the philosophical underpinnings (using critical review methods) of empirical studies of employees' security-related behavior	We review the broader body of security policy literature
Willison and Warkentin (2013)	Overview of selected IS and general literature on neutralization, deterrence and expressive motivations, and organizational justice; specific number of articles and time period not provided; not a systematic review paper	Proposed the following topics for future empirical investigations of employee computer abuse: techniques of neutralization (rationalizations), expressive/instrumental criminal motivations, disgruntlement as a result of perceptions of organizational justice	We review the broader body of security policy literature
Zafar & Clark (2009)	137 IS security research articles published through 2007; start date not provided	Classified the papers according to themes established by the IBM Information Security Capability Reference Model (e.g., Governance, Identity and Access Management, Personnel Security)	We review the more specific body of security policy literature

* Our review also differs from each of these based on the time frame (ours is through the first half of 2017), and the identification of linkages among the constructs in the literature (as opposed to primarily a classification of articles based on research topic, theory, method, etc.).

Appendix B: Articles included in review (sorted by author)

The issue of which articles constitute security policy research is not entirely straightforward, particularly when it comes to the vast literature on employees' security policy compliance. Within this subset of the security policy literature, there exist many different conceptualizations of compliance behavior (Chu *et al*, 2015; Guo, 2013), and not all behaviors contain an explicit security policy labeling. We follow the criteria of past reviews (Siponen & Vance, 2014; Sommestad *et al*, 2014) and include policy-related behaviors in organizational contexts, such as computer abuse and IS misuse, within our conceptualization of security policy compliance. Including these behaviors is based on the notion that they mainly involve the unauthorized use of information and technology resources within organizations, and, therefore, constitute security policy violations (Chu *et al*, 2015).

Article	*Journal*	*Empirical/Conceptual*	*Methodology*
Al-Mukahal & Alshare (2015)	*Information and Computer Security*	Empirical	Survey
Aurigemma & Leonard (2015)	*Journal of Information System Security*	Empirical	Survey
Barlow *et al* (2013)	*Computers and Security*	Empirical	Survey
Baskerville *et al* (2014)	*Information Technology and People*	Conceptual	–
Boss *et al* (2009)	*European Journal of Information Systems*	Empirical	Survey
Bulgurcu *et al* (2010)	*MIS Quarterly*	Empirical	Survey
Chan *et al* (2005)	*Journal of Information Privacy and Security*	Empirical	Survey
Chen *et al* (2012)	*Journal of Management Information Systems*	Empirical	Experiment
Chen *et al* (2015)	*The Journal of Computer Information Systems*	Empirical	Survey
Cheng *et al* (2013)	*Computers and Security*	Empirical	Survey
Chu *et al* (2016)	*Journal of Business Ethics*	Empirical	Survey
Crossler *et al* (2014)	*Journal of Information Systems*	Empirical	Survey
D'Arcy and Hovav (2007)	*Communications of the ACM*	Empirical	Survey
D'Arcy & Devaraj (2012)	*Decision Sciences*	Empirical	Survey
D'Arcy and Greene (2014)	*Information Management and Computer Security*	Empirical	Survey
D'Arcy *et al* (2009)	*Information Systems Research*	Empirical	Survey
D'Arcy *et al* (2014)	*Journal of Management Information Systems*	Empirical	Survey
Dinev & Hu (2007)	*Journal of the Association for Information Systems*	Empirical	Survey
Dinev *et al* (2009)	*Information Systems Journal*	Empirical	Survey
Doherty & Fulford (2005)	*Information Resources Management Journal*	Empirical	Survey
Doherty & Fulford (2006)	*Computers & Security*	Conceptual	–
Doherty *et al* (2009)	*International Journal of Information Management*	Empirical	Archival
Flowerday & Tuyikeze (2016)	*Computers and Security*	Empirical	Survey
Foth (2016)	*European Journal of Information Systems*	Empirical	Survey
Fulford & Doherty (2003)	*Information Management and Computer Security*	Empirical	Survey
Gaunt (1998)	*International Journal of Medical Informatics*	Empirical	Observation, Survey
Goel and Chengalur-Smith (2010)	*Journal of Strategic Information Systems*	Empirical	Survey
Goo *et al* (2014)	*IEEE Transactions on Professional Communication*	Empirical	Survey
Gritzalis (1997)	*Computers and Security*	Conceptual	–
Guo & Yuan (2012)	*Information and Management*	Empirical	Survey
Guo *et al* (2011)	*Journal of Management Information Systems*	Empirical	Survey
Han *et al* (2017)	*Computers and Security*	Empirical	Survey
Harrington (1996)	*MIS Quarterly*	Empirical	Survey
Hedström *et al* (2011)	*Journal of Strategic Information Systems*	Empirical	Case studies
Herath & Rao (2009a)	*Decision Support Systems*	Empirical	Survey
Herath & Rao (2009b)	*European Journal of Information Systems*	Empirical	Survey
Höne and Eloff (2002a)	*Computers and Security*	Conceptual	–
Höne and Eloff (2002b)	*Network Security*	Conceptual	–
Hong *et al* (2006)	*Information Management and Computer Security*	Empirical	Survey
Hovav & D'Arcy (2012)	*Information and Management*	Empirical	Survey
Hsu *et al* (2015)	*Information Systems Research*	Empirical	Survey
Hu *et al* (2011)	*Communications of the ACM*	Empirical	Scenario, Survey
Hu *et al* (2012)	*Decision Sciences*	Empirical	Survey
Hu *et al* (2015)	*Journal of Management Information Systems*	Empirical	Experiment
Hwang *et al* (2017)	*Online Information Review*	Empirical	Survey
Ifinedo (2012)	*Computers and Security*	Empirical	Survey
Ifinedo (2014)	*Information and Management*	Empirical	Survey
Ifinedo (2016)	*Information Systems Management*	Empirical	Survey

Article	*Journal*	*Empirical/Conceptual*	*Methodology*
Johnston & Warkentin (2010a)	*MIS Quarterly*	Empirical	Experiment
Johnston & Warkentin (2010b)	*Journal of Organizational and End User Computing*	Empirical	Experiment
Johnston *et al* (2013)	*Journal of Organizational and End User Computing*	Empirical	Survey
Johnston *et al* (2015)	*MIS Quarterly*	Empirical	Experiment, Interviews
Johnston *et al* (2016)	*European Journal of Information Systems*	Empirical	Survey
Kadam (2007)	*Information Systems Security*	Conceptual	–
Karyda *et al* (2005)	*Computers & Security*	Empirical	Case studies
Kim *et al* (2016)	*Information & Management*	Empirical	Survey
Knapp *et al* (2006)	*Information Management and Computer Security*	Empirical	Interviews, Survey
Knapp *et al* (2009)	*Computers & Security*	Empirical	Survey, Content Analysis
Knapp & Ferrante (2012)	*Journal of Management Policy and Practice*	Empirical	Survey
Lee and Larson (2009)	*European Journal of Information Systems*	Empirical	Survey
Lee and Lee (2002)	*Information Management and Computer Security*	Conceptual	–
Lee *et al* (2004)	*Information and Management*	Empirical	Survey
Lee *et al* (2016)	*Computers and Security*	Empirical	Survey
Li *et al* (2010)	*Decision Support Systems*	Empirical	Survey
Li *et al* (2014)	*Information Systems Journal*	Empirical	Survey
Liao *et al* (2009)	*Journal of Computer Information Systems*	Empirical	Survey
Liang *et al* (2013)	*Information Systems Research*	Empirical	Survey
Lowry & Moody (2015)	*Information Systems Journal*	Empirical	Scenario, Survey
Lowry *et al* (2015)	*Information Systems Journal*	Empirical	Survey
Moquin & Wakefield (2016)	*Journal of Computer Information Systems*	Empirical	Survey
Myyry *et al* (2009)	*European Journal of Information Systems*	Empirical	Survey
Ng *et al* (2009)	*Decision Support Systems*	Empirical	Survey
Padayachee (2012)	*Computers & Security*	Conceptual	–
Pathari & Sonar (2012)	*Information Management and Computer Security*	Conceptual	Modeling
Posey *et al* (2011a)	*Computers and Security*	Empirical	Survey
Posey *et al* (2015)	*Journal of Management Information Systems*	Empirical	Survey
Puhakainen & Siponen (2010)	*MIS Quarterly*	Empirical	Survey, Interviews
Rees *et al* (2003)	*Communications of the ACM*	Conceptual	–
Renaud & Goucher (2012)	*Information Management and Computer Security*	Empirical	Interviews
Safa *et al* (2016)	*Computers & Security*	Empirical	Survey
Shephard & Mejias (2016)	*International Journal of Human–Computer Interaction*	Empirical	Experiment
Shropshire *et al* (2015)	*Computers and Security*	Empirical	Survey
Siponen (2000)	*Information Management and Computer Security*	Conceptual	–
Siponen (2006)	*Communications of the ACM*	Conceptual	–
Siponen & Iivari (2006)	*Journal of the Association for Information Systems*	Conceptual	–
Siponen & Vance (2010)	*MIS Quarterly*	Empirical	Scenario, Survey
Siponen & Willison (2009)	*Information and Management*	Empirical	Archival
Siponen *et al* (2009)	*Communications of the ACM*	Empirical	Survey
Siponen *et al* (2010)	*Computer*	Empirical	Survey
Siponen *et al* (2014)	*Information and Management*	Empirical	Survey
Sommestad *et al* (2015)	*Information and Computer Security*	Empirical	Survey
Son (2011)	*Information and Management*	Empirical	Survey
Park & Son (2016)	*International Journal of Information Management*	Empirical	Survey
Spears & Barki (2010)	*MIS Quarterly*	Empirical	Interviews, Survey
Stahl *et al* (2012)	*Information Systems Journal*	Empirical	Archival
Straub (1990)	*Information Systems Research*	Empirical	Survey
Teh *et al* (2015)	*Journal of Global Information Management*	Empirical	Survey
Tsohou *et al* (2015b)	*European Journal of Information Systems*	Empirical	Action, Case Study
Vaast (2007)	*Journal of Strategic Information Systems*	Empirical	Interviews
Vance & Siponen (2012)	*Journal of Organizational and End User Computing*	Empirical	Scenario, Survey
Vance *et al* (2012)	*Information and Management*	Empirical	Survey
Vance *et al* (2013)	*Journal of Management Information Systems*	Empirical	Scenario, Survey
Vance *et al* (2015)	*MIS Quarterly*	Empirical	Scenario, Survey
von Solms (1999)	*Information Management and Computer Security*	Conceptual	–
Wall (2013)	*Security Journal*	Empirical	Archival
Wall *et al* (2013)	*Journal of Information Privacy and Security*	Empirical	Survey

Article	*Journal*	*Empirical/Conceptual*	*Methodology*
Warkentin *et al* (2011)	*European Journal of Information Systems*	Empirical	Survey
Warman (1992)	*European Journal of Information Systems*	Empirical	Survey, Interview
Wiant (2005)	*Computers and Security*	Empirical	Survey
Wood (1982)	*Computers and Security*	Conceptual	–
Workman *et al* (2008)	*Computers in Human Behavior*	Empirical	Archival, Survey
Xue *et al* (2011)	*Information Systems Research*	Empirical	Survey
Yazdanmehr & Wang (2016)	*Decision Support Systems*	Empirical	Survey
Zhang *et al* (2009)	*Information Management and Computer Security*	Empirical	Survey

A similar issue exists with respect to protection motivation theory (PMT)-based studies on how to achieve secure behavior (e.g., Boss *et al*, 2009, 2015; Johnston & Warkentin, 2010a; Posey *et al*, 2015). Within this work, some papers explicitly describe secure behaviors in response to security policies (e.g., using anti-spyware, backing up data, changing passwords), whereas others are vague on this issue, or are specific to the personal/home usage context. Again, following past reviews of the security compliance literature (Siponen & Vance, 2014; Sommestad *et al*, 2014), we include only those PMT-based studies that involve secure behavior in organizational contexts. Adhering to these criteria means that a study meets at least one of the following conditions: (1) a description of secure behavior in which the user is interacting with an organizational information system, (2) a description of the direct relevance of the secure behavior to the organizational context, or (3) the use of organizational respondents. PMT-based studies where the population is personal/home computer users or the context is otherwise not work-related are excluded, because in such cases individuals are not subject to security policies and must acquire information about security threats and tools on their own (Anderson & Agarwal, 2010; Chen and Zahedi, 2016). Appendix D further details our exclusion criteria, as it pertains to a specific list of excluded articles.

In making the preceding points, we emphasize that the PMT-based studies of how to achieve secure behavior often use similar constructs, regardless of whether the context is organizational or personal/home usage. Likewise, studies of employees' security compliance use many similar theoretical bases and constructs across the variety of behaviors being investigated (e.g., security policy compliance/non-compliance, computer abuse, IS misuse, etc.). Consequently, we have captured the key constructs and themes within these subsets of the security policy literature, even if a particular study may have been excluded based on our criteria.

Regarding the overall security policy literature, we do not claim to have captured every (peer-reviewed) published article for this review, but we do have a relatively complete consensus of the literature, to the point where the constructs and interrelationships in our research framework are supported and no new concepts emerged from the literature. In this manner, we followed Rowe's (2014) guidance that reviews for understanding should strive for strong coverage of the domain rather than absolute completeness.

Appendix C: Articles included in review (sorted by article frequency)

Journal	*Number of articles included in review*
Computers and Security	17
Information Management and Computer Security	10
European Journal of Information Systems	9
Information and Management	9
MIS Quarterly	8
Journal of Management Information Systems	6
Communications of the ACM	5
Information Systems Journal	5
Information Systems Research	5
Decision Support Systems	4
Journal of Computer Information Systems	3
Journal of Organizational and End User Computing	3
Journal of Strategic Information Systems	3
Decision Sciences	2

Journal	*Number of articles included in review*
Information and Computer Security	2
International Journal of Information Management	2
Journal of Information Privacy and Security	2
Journal of the Association for Information Systems	2
Computer	1
Computers in Human Behavior	1
IEEE Transactions on Professional Communication	1
International Journal of Human–Computer Interaction	1
International Journal of Medical Informatics	1
Information Resources Management Journal	1
Information Systems Management	1
Information Systems Security	1
Information Technology and People	1
Journal of Business Ethics	1
Journal of Global Information Management	1
Journal of Information Systems	1
Journal of Information System Security	1
Journal of Management Policy and Practice	1
Network Security	1
Online Information Review	1
Security Journal	1

Appendix D: Articles excluded from the review

The following table lists articles that were excluded from our review, including details of our rationale. Obviously, this list is not exhaustive, but our aim is to provide transparency into our exclusion process, particularly with respect to the exclusion of certain well-known articles that appear in top-tier IS journals. We refer the reader back to the Methodology section, as well as Appendix B, for additional details on our inclusion/exclusion criteria.

Notes: the term "not security policy centric" is used to describe an article that we deemed as not directly addressing the design, implementation, compliance/non-compliance, or monitoring of security policies in organizations. Many such articles address information security issues or information security management in a general sense. The remaining descriptions of our rationale for exclusion are self-explanatory.

Article	*Journal*	*Rationale for Exclusion*
Albrechtsen (2007)	Computers and Security	Not security policy centric
Anderson & Agarwal (2010)	MIS Quarterly	Not security policy centric; personal/home usage context
Backhouse *et al* (2006)	MIS Quarterly	Oriented toward industry policy
Basin *et al* (2013)	ACM Transactions on Information and System Security	Oriented toward technical policy
Bauer and van Eeten (2009)	Telecommunications Policy	Not security policy centric
Bauer *et al* (2009)	ACM Transactions on Software Engineering and Methodology	Oriented toward technical policy
Boss *et al* (2015)	MIS Quarterly	Not security policy centric; personal/home usage context
Burns *et al* (2017)	Computers in Human Behavior	Not security policy centric
Chen and Zahedi (2016)	MIS Quarterly	Not security policy centric; personal/home usage context
Crossler and Bélanger (2009)	Journal of Information System Security	Not security policy centric
Culnan and Williams (2009)	MIS Quarterly	Not security policy centric; issues and opinion paper
Cuppens *et al* (2013)	Journal of Computer Security	Oriented toward technical policy

Article	*Journal*	*Rationale for Exclusion*
David (2002)	Computers and Security	Issues and opinion paper
Dhillon and Backhouse (2000)	Communications of the ACM	Not security policy centric
Di Modica and Tomarchio (2016)		
Foley and Fitzgerald (2011)	Journal of Computer Security	Oriented toward technical policy
Herath *et al* (2014)	Information Systems Journal	Not security policy centric; personal/home usage context
Hicks *et al* (2010)	ACM Transactions on Information and System Security	Oriented toward technical policy
Horcas *et al* (2016)	Computers and Security	Oriented toward technical policy
Jajodia *et al* (2001)	ACM Transactions on Database Systems	Oriented toward technical policy
Kankanhalli *et al* (2003)	International Journal of Information Management	Not security policy centric
Karjalainen and Siponen (2011)	Journal of the Association for Information Systems	Not security policy centric
Khoury and Tawbi (2012)	ACM Transactions on Information and System Security	Oriented toward technical policy
Li & Wang (2008)	Journal of the ACM	Not security policy centric
Liang & Xue (2009)	MIS Quarterly	Not security policy centric; personal/home usage context
Liang & Xue (2010)	Journal of the Association for Information Systems	Not security policy centric; personal/home usage context
Liu (2015)	European Journal of Information Systems	Not security policy centric
Liu *et al* (2016)	Information Sciences	Oriented toward technical policy
Lowry *et al* (2014)	Journal of Business Ethics	Not security policy centric
McDaniel and Prakash (2006)	ACM Transactions on Information and System Security	Oriented toward technical policy
Mehra (2010)	The American Journal of Comparative Law	Oriented toward public policy
Montanari *et al* (2013)	Computers & Security	Oriented toward technical policy
Muthaiyah and Kerschberg (2007)	Information Systems Frontiers	Oriented toward technical policy
Osenga (2013)	Journal of Information Policy	Oriented toward public policy
Phelps *et al* (2012)	Journal of Information System Security	Not security policy centric
Posey *et al* (2011b)	Journal of Information System Security	Not security policy centric
Posey *et al* (2013)	MIS Quarterly	Not security policy centric; primarily a methodological article; taxonomy of security-related behaviors
Rhee *et al* (2009)	Computers & Security	Not security policy centric; personal/home usage context
Schneider (2000)	ACM Transactions on Information and System Security	Oriented toward technical policy
Shirtz and Elovici (2011)	Information Management and Computer Security	Not security policy centric
Silva *et al* (2016)	Decision Support Systems	Oriented toward industry policy
Smith *et al* (2010)	MIS Quarterly	Oriented toward industry policy
Stanton *et al* (2005)	Computers and Security	Not security policy centric; taxonomy of security-related behaviors
Straub and Nance (1990)	MIS Quarterly	Not security policy centric
Straub & Welke (1998)	MIS Quarterly	Not security policy centric
Tang *et al* (2016)	Information Technology and Management	Not security policy centric
Thomson (2010)	Journal of Information System Security	Not security policy centric
Tsohou *et al* (2010)	Journal of Information System Security	Not security policy centric
Tsohou *et al* (2015a)	Computers & Security	Not security policy centric
Unal & Caglayan (2013)	Computer Networks	Oriented toward technical policy
Uzunov *et al* (2015)	Computers and Security	Oriented toward technical policy
Vance *et al* (2014)	Journal of the Association for Information Systems	Not security policy centric; personal/home usage context

Article	*Journal*	*Rationale for Exclusion*
Von Dran *et al* (1996)	Computers and Security	Issues and opinion paper
Vroom and von Solms (2004)	Computers and Security	Not security policy centric
Wall *et al* (2016)	Journal of the Association for Information Systems	Oriented toward public policy
Warkentin *et al* (2016b)	Journal of the Association for Information Systems	Not security policy centric; personal/home usage context
Warkentin *et al* (2016a)	Decision Support Systems	Not security policy centric; personal/home usage context.
Willison (2006)	Information and Organization	Not security policy centric
Willison and Backhouse (2006)	European Journal of Information Systems	Not security policy centric
Workman and Gathegi (2007)	Journal of the American Society for Information Science and Technology	Not security policy centric; personal/home usage context
Zhang *et al* (2005)	ACM Transactions on Information and System Security	Oriented toward technical policy

Appendix E: Research framework constructs, definitions, and supporting publications

Construct	*Definition*	*Examples*	*Sample Publications*
Security standards, guidelines and regulations	The formal documents and opinions on security policy recommendations that are published by external bodies, groups, or associations	ISO 27001/02, COBIT, Health Insurance Portability and Accountability Act (HIPPA), Information Technology Infrastructure Library (ITIL), and the Payment Card Industry Data Security Standard (PCI DSS)	Knapp *et al* (2009), Siponen (2006); von Solms (1999)
Desired policy format and structure	The aims and objectives of an organization's security policies, in terms of length, clarity, and level of detail	Management endeavors to design security policies that are concise and easy to understand	Goel and Chengalur-Smith (2010), Pathari & Sonar (2012)
Internal and external risk management considerations	The internal and external factors that pose information security risks to an organization	Organization type, size, IT infrastructure, business objectives, economic environment, and internal/external threats	Hong *et al* (2006), Karyda *et al* (2005), Knapp *et al* (2009), Warman (1992), Wall (2013)
Security policy design and implementation	The actual design characteristics of the completed security policy and the manner in which the policy is implemented at the organization	Creating an internet use policy by defining the purpose, scope, roles/ responsibilities, and expected/prohibited employee behaviors	Karyda *et al* (2005), Knapp *et al* (2009), Wall (2013)
Information security culture, awareness, and support	Security culture consists of the shared assumptions, values, and beliefs help by a group of employees (Karlsson *et al*, 2015; Knapp *et al*, 2006). Security awareness refers to the values and attitudes that individual employees hold in regard to secure information practices (Tsohou *et al*, 2015). Managerial support for information security initiatives represents the financial backing, sponsorship, encouragement, and leadership that management put forth for security initiatives	Management is strongly committed to delivering the funds necessary to enhance employee awareness of security policies	Chen *et al* (2015), Johnston *et al* (2013), Karyda *et al* (2005)
Socioemotional consequences for employees	The interaction between the existence of a security policy and an employee's social and emotional well-being	An employee feels an increased sense of stress in needing to comply with a new anti-malware policy at their organization	Renaud & Goucher (2012), Vaast (2007)

Construct	*Definition*	*Examples*	*Sample Publications*
Personality and dispositional traits	The inherent, individual characteristics of employees, including behavioral, cognitive, and ethical norms	An employee believes that it is their moral responsibility to comply with security policies laid out by the organization	Ifinedo (2014), Myyry *et al* (2009), Vance & Siponen (2012)
Security policy legitimacy, fairness and justice	The perception of an individual that a security policy is desirable, appropriate, and reasonable	An employee considers a new password policy at their organization as an unfair burden on them	Hu *et al* (2012), Siponen & Iivari (2006), Son (2011)
Compliance with security policy	The extent to which employees intend to comply or actually comply with a security policy	Despite a policy stating that data backups should be completed every night, an employee ignores the guideline and only backs up their data on a weekly basis.	Bulgurcu *et al* (2010), Herath & Rao (2009a; b)
Organizational security objectives	The benefits that the implementation of security policies intend to achieve	By implementing a data protection policy, an organization hopes to reduce the number of incidents of personal information being accidentally released.	Hsu *et al* 2015; Knapp & Ferrante (2012), Spears & Barki (2010), Wiant (2005)

Appendix F: Article coding results by relationship

The papers highlighted in the R1–R5 columns below correspond to the findings presented in the Results section. The items listed in the "Main Theoretical/Conceptual Linkages" column represent theories and conceptual models that were referenced in each of the listed papers. The data presented here varies in magnitude and scope, depending on the theoretical orientation of each paper. In some cases, a theory or model was used to construct or extend a research model; in other cases, a broader theory or concept simply informed the direction of the research.

Paper	*R1*	*R2*	*R3*	*R4*	*R5*	*Main Theoretical/Conceptual Linkages*
Al-Mukahal & Alshare (2015)			x			Deterrence theory, neutralization theory, theory of planned behavior
Aurigemma & Leonard (2015)			x			Affective organizational commitment, theory of planned behavior, rational choice theory
Barlow *et al* (2013)			x			Theory of neutralization techniques
Baskerville *et al* (2014)			x			Emote opportunity model of computer abuse
Boss *et al* (2009)		x	x			Social influence theory, organismic integration theory, agency theory, control theory
Bulgurcu *et al* (2010)			x			Theory of planned behavior, rational choice theory, deterrence theory
Chan *et al* (2005)			x			Not applicable or none noted
Chen *et al* (2012)			x			Compliance theory, general deterrence theory
Chen *et al* (2015)		x				Organizational culture theory, security culture framework
Cheng *et al* (2013)			x			General deterrence theory, social bond theory, social control mechanisms
Chu *et al* (2016)			x			General deterrence theory
Crossler *et al* (2014)			x			Protection motivation theory
D'Arcy and Hovav (2007)			x			General deterrence theory
D'Arcy & Devaraj (2012)			x			Deterrence theory
D'Arcy and Greene (2014)			x			Social exchange theory
D'Arcy *et al* (2009)			x			General deterrence theory
D'Arcy *et al* (2014)			x			Coping theory, moral disengagement theory, social cognitive theory
Dinev & Hu (2007)			x			Theory of planned behavior
Dinev *et al* (2009)			x			Theory of planned behavior
Doherty & Fulford (2005)					x	Not applicable or none noted
Doherty & Fulford (2006)	x					Not applicable or none noted
Doherty *et al* (2009)	x					Not applicable or none noted
Flowerday & Tuyikeze (2016)	x	x				Not applicable or none noted
Foth (2016)			x			Theory of planned behavior, general deterrence theory

Paper	*R1*	*R2*	*R3*	*R4*	*R5*	*Main Theoretical/Conceptual Linkages*
Fulford & Doherty (2003)	x					Not applicable or none noted
Gaunt (1998)		x				Not applicable or none noted
Goel & Chengalur-Smith (2010)	x					Not applicable or none noted
Goo *et al* (2014)			x			Safety climate and performance model
Gritzalis (1997)	x					Not applicable or none noted
Guo & Yuan (2012)			x			Deterrence theory, social cognitive theory
Guo *et al* (2011)			x			Composite behavior model
Han *et al* (2017)			x			Rational choice theory
Harrington (1996)			x			Deterrence theory
Hedström *et al* (2011)			x			Value-based compliance model
Herath & Rao (2009a)			x			General deterrence theory, protection motivation theory
Herath & Rao (2009b)			x			General deterrence theory, agency theory
Höne and Eloff (2002a)	x					Not applicable or none noted
Höne and Eloff (2002b)	x					Not applicable or none noted
Hong *et al* (2006)	x					Integrated system theory of information security management
Hovav & D'Arcy (2012)			x			Deterrence theory
Hsu *et al* (2015)			x	x		Social control theory
Hu *et al* (2011)			x			Deterrence theory, rational choice theory, self-control theory
Hu *et al* (2012)			x			Theory of planned behavior
Hu *et al* (2015)			x			Self-control theory
Hwang *et al* (2017)			x			Protection motivation theory
Ifinedo (2012)			x			Theory of planned behavior, protection motivation theory
Ifinedo (2014)			x			Theory of planned behavior, social cognitive theory, social bond theory
Ifinedo (2016)			x			General deterrence theory, rational choice theory, organizational climate perspective
Johnston & Warkentin (2010a)			x			Protection motivation theory, fear appeals model
Johnston & Warkentin (2010b)			x			Not applicable or none noted
Johnston *et al* (2013)		x				Social cognitive theory
Johnston *et al* (2015)			x			Protection motivation theory, deterrence theory
Johnston *et al* (2016)			x			Protection motivation theory, general deterrence theory
Kadam (2007)	x					Not applicable or none noted
Karyda *et al* (2005)	x	x			x	Not applicable or none noted
Kim *et al* (2016)			x			Abuse opportunity structure, emotion process model
Knapp *et al* (2006)		x				Grounded theory
Knapp *et al* (2009)	x	x			x	Grounded theory
Knapp & Ferrante (2012)				x	x	General deterrence theory, theory of organizational learning
Lee and Larson (2009)			x			Protection motivation theory
Lee and Lee (2002)			x			General deterrence theory, social bond theory, social learning theory
Lee *et al* (2004)			x			General deterrence theory, social control theory, theory of planned behavior
Lee *et al* (2016)		x				Person-environment fit theory
Li *et al* (2010)			x			Rational choice theory
Li *et al* (2014)			x			Organizational justice
Liao *et al* (2009)			x			Theory of planned behavior, deterrence theory, theory of ethics
Liang *et al* (2013)			x			Control theory, regulatory focus theory
Lowry & Moody (2015)		x	x			Organizational control theory, reactance theory
Lowry *et al* (2015)			x			Fairness theory, reactance theory
Moquin & Wakefield (2016)			x			Protection motivation theory, theory of planned behavior
Myyry *et al* (2009)			x			Theory of cognitive moral development, theory of motivational types of values
Ng *et al* (2009)			x			Health belief model
Padayachee (2012)			x			Self-determination theory
Pathari & Sonar (2012)	x					Not applicable or none noted
Posey *et al* (2011a)			x			Causal reasoning theory, attribution theory
Posey *et al* (2015)			x			Protection motivation theory, organizational commitment
Puhakainen & Siponen (2010)			x			Universal constructive instructional theory, elaboration likelihood model

Paper	*R1*	*R2*	*R3*	*R4*	*R5*	*Main Theoretical/Conceptual Linkages*
Rees *et al* (2003)	x				x	Not applicable or none noted
Renaud & Goucher (2012)		x				Not applicable or none noted
Safa *et al* (2016)			x			Social bond theory, involvement theory
Shephard & Mejias (2016)			x			General deterrence theory, rational choice theory, agency theory
Shropshire *et al* (2015)			x			Theory of reasoned action, technology acceptance model
Siponen (2000)		x				Theory of reasoned action, theory of planned behavior, intrinsic motivation, technology acceptance model
Siponen (2006)	x					Not applicable or none noted
Siponen & Iivari (2006)			x			Conservative-deontological theory, liberal-intuitive theory, prima-facie theory, virtue theory, utilitarian theory, universalizability theory
Siponen & Vance (2010)			x			Neutralization theory, general deterrence theory
Siponen & Willison (2009)	x					Not applicable or none noted
Siponen *et al* (2009)			x			Theory of reasoned action, protection motivation theory
Siponen *et al* (2010)			x			Protection motivation theory, deterrence theory, theory of reasoned action, innovation diffusion theory
Siponen *et al* (2014)			x			Protection motivation theory, theory of reasoned action, cognitive evaluation theory
Sommestad *et al* (2015)			x			Theory of planned behavior, protection motivation theory
Son (2011)			x			General deterrence theory, intrinsic and extrinsic motivation models
Park & Son (2016)			x			Procedural justice
Spears & Barki (2010)			x	x		Buy-in theory of participation, system quality theory, emergent interactions theory
Stahl *et al* (2012)		x				Critical social theory
Straub (1990)			x			General deterrence theory
Teh *et al* (2015)			x			Social exchange theory
Tsohou *et al* (2015b)		x				Actor-network theory, structuration theory, contextualism
Vaast (2007)		x				Not applicable or none noted
Vance & Siponen (2012)			x			Rational choice theory
Vance *et al* (2012)			x			Protection motivation theory, habit theory
Vance *et al* (2013)			x			Theory of accountability
Vance *et al* (2015)			x			Accountability theory
von Solms (1999)	x					Not applicable or none noted
Wall (2013)	x		x			Not applicable or none noted
Wall *et al* (2013)						Self-determination theory, psychological reactance theory
Warkentin *et al* (2011)			x			Social learning theory
Warman (1992)	x					Not applicable or none noted
Wiant (2005)				x		Deterrence theory
Wood (1982)	x				x	Not applicable or none noted
Workman *et al* (2008)			x			Threat control model, social cognitive theory, protection motivation theory
Xue *et al* (2011)			x			Technology acceptance model
Yazdanmehr & Wang (2016)			x			Norm activation theory, social norms theory
Zhang *et al* (2009)			x			Risk compensation theory, theory of planned behavior
Total articles	20	15	81	4	6	

Appendix G: Overview of Supplementary Theories and Approaches

Informing theory or approach	*Summary*	*Boundary conditions and assumptions*	*Limitations*	*References*
Control theory	Control theory examines the managerial design and implementation of mechanisms that attempt to affect the behavior of another person or group as a means to achieve organizational goals. Key areas of focus include the antecedents to control choice (e.g., behavior observability) and the characteristics of control (e.g., control mode, degree, style)	Control theory assumes a clear division of roles between controllers (e.g., managers) and controllees (e.g., staff) Control theory focuses primarily around the controller's concern for the organization's ability to capture value	Where organizational structure and job roles are ambiguous, control theory is less helpful in clarifying controller–controlee interactions Control research within IS has been largely focused on systems development processes	Cram *et al* (2016b), Davis (1940), Flamholtz *et al* (1985), Remus *et al* (2015), Tannenbaum (1962), Wiener *et al* (2016)
Institutional theory	Institutional theory considers the norms, processes, and routines within organizations associated with social behavior	Where organizational structures are viewed as being legitimate, fair, and just, employees are more likely to perform their responsibilities more effectively, including complying with rules and regulations	Institutional theory deemphasizes the individual interests of actors, in favor of institutional influences	DiMaggio (1988), Jaffee (1991), Meyer and Rowan (1977), Niehoff and Moorman (1993), Schnedler and Vadovic (2011), Scott (1987), Workman (2009)
Replication and longitudinal research	Replication research seeks to obtain the same results as previous studies by either reproducing similar conditions or deliberately introducing variations to the conditions (e.g., data set, population) of the original study Longitudinal research draws on data from multiple points in time	Replication research relies on the prior publication of work that allows for a reproduction of similar study conditions or a deliberate variation of particular study conditions Longitudinal research aims to identify causal factors by uncovering changes that occur over time	Replication research is not always identified as such and comprises only a small proportion of published research Longitudinal research introduces challenges in terms of data collection difficulties (e.g., finding organizations or individuals willing to participate on multiple occasions)	Lindsay and Ehrenberg (1993), Salterio (2014), Tsang and Kwan (1999)
Agency theory	Agency theory examines the relationship between two parties, the principal and agent, and the challenges that arise from their conflicting goals and the limited ability of the principal to oversee the agent's work	Applications of agency theory commonly assume that (1) agents act primarily out of self-interest; (2) the goals of principals and agents conflict; and (3) information asymmetry exists between principals and agents Agency relationships can apply in a variety of settings, including owner-manager and manager-subordinate	Agency theory is most useful in situations where principal–agent goal conflict and/or information asymmetry is high Agency theory has been criticized for being narrow in scope and difficult to test	Eisenhardt (1989), Jensen and Meckling (1976), Perrow (1986), Sharma (1997), Zsidisin and Ellram (2003)
Work systems theory, cybernetics	Work systems theory considers the circumstances where humans and machines perform work using information and technology, while accounting for the planned and unplanned	Systems and processes are standardized and measurable. Where performance variances are identified within the systems, the related information can be used to resolve the problems that	In processes that are unstandardized, difficult to measure, or information isn't available to make corrections, feedback loops may be less helpful	Alter (2013), Hofstede (1978)

Informing theory or approach	*Summary*	*Boundary conditions and assumptions*	*Limitations*	*References*
Work systems theory, cybernetics	Work systems theory considers the circumstances where humans and machines perform work using information and technology, while accounting for the planned and unplanned changes that occur within such systems. A cybernetic process is one that uses a feedback loop to set goals, determine achievement against those goals, and make ongoing corrections	Systems and processes are standardized and measurable. Where performance variances are identified within the systems, the related information can be used to resolve the problems that exist. Work systems theory and cybernetics can apply to both technical processes, as well as sociotechnical systems	In processes that are unstandardized, difficult to measure, or information isn't available to make corrections, feedback loops may be less helpful	Alter (2013), Hofstede (1978)