

2023

## An Adversarial Dance: Toward an Understanding of Insiders' Responses to Organizational Information Security Measures

Puzant Balozian

*James Madison University, balozipx@jmu.edu*

A. J. Burns

*Louisiana State University, ajburns@lsu.edu*

Dorothy E. Leidner

*University of Virginia, dorothy\_leidner@baylor.edu*

Follow this and additional works at: <https://aisel.aisnet.org/jais>

---

### Recommended Citation

Balozian, Puzant; Burns, A. J.; and Leidner, Dorothy E. (2023) "An Adversarial Dance: Toward an Understanding of Insiders' Responses to Organizational Information Security Measures," *Journal of the Association for Information Systems*, 24(1), 161-221.

DOI: 10.17705/1jais.00798

Available at: <https://aisel.aisnet.org/jais/vol24/iss1/4>

This material is brought to you by the AIS Journals at AIS Electronic Library (AISeL). It has been accepted for inclusion in Journal of the Association for Information Systems by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact [elibrary@aisnet.org](mailto:elibrary@aisnet.org).

# An Adversarial Dance: Toward an Understanding of Insiders' Responses to Organizational Information Security Measures

Puzant Baloizian,<sup>1</sup> A. J. Burns,<sup>2</sup> Dorothy E. Leidner<sup>3</sup>

<sup>1</sup>James Madison University, USA, [balozipx@jmu.edu](mailto:balozipx@jmu.edu)

<sup>2</sup>Louisiana State University, USA, [ajburns@lsu.edu](mailto:ajburns@lsu.edu)

<sup>3</sup>University of Virginia, USA, [dorothy@virginia.edu](mailto:dorothy@virginia.edu)

## Abstract

Despite the increased focus on organizational security policies and programs, some employees continue to engage in maladaptive responses to security measures (i.e., behaviors other than those recommended, intended, or prescribed). To help shed light on insiders' adaptive and maladaptive responses to IS security measures, we conducted a case study of an organization at the forefront of security policy initiatives. Drawing on the beliefs-actions-outcomes (BAO) model to analyze our case data, we uncover a potentially nonvirtuous cycle consisting of security-related beliefs, actions, and outcomes, which we refer to as an "adversarial dance." Explaining our results, we describe a novel belief framework that identifies four security belief profiles and uncovers an underexplored outcome of IS security: insiders' lived security experiences. We find that individuals' unfavorable lived security experiences produce counterproductive security-related beliefs that, in turn, lead to maladaptive behaviors. Maladaptive behaviors create new potential for security risk, leading to increased organizational security measures to counter them. Thus, the adversarial dance continues, as the new security measures have the potential to reinforce counterproductive security-related beliefs about the importance and risk of IS security and lead to new maladaptive behaviors. To help situate our findings within the current security literature, we integrate the results with prior research based on extant theories. While this paper is not the first to suggest that security measures can elicit maladaptive behaviors, the emergent belief framework and expanded BAO model of IS security constitute an important contribution to the behavioral IS security literature.

**Keywords:** Information System (IS) Security, Security Beliefs, Beliefs-Actions-Outcomes (BAO) Theory, Belief Framework, Security Adverse Effects

John D'Arcy was the accepting senior editor. This research article was submitted on June 24, 2019 and underwent three revisions. Authors are listed in alphabetical order.

## 1 Introduction

Many organizations are highly connected enterprises with valuable and/or sensitive information being stored, processed, and accessed by organizational insiders at various levels within the organization (Baloizian et al., 2019; Burns et al., 2018; D'Arcy et al., 2009). This means that the protection of organizational information systems (IS) security is increasingly

reliant upon the behaviors of individuals with access to information technology and systems (Crossler et al., 2013; Dinev & Hu, 2007; Stanton et al., 2006). The dispersion of information across various systems and technologies increases the surface area for information security professionals to secure, making it difficult to ensure that organizational insiders exhibit secure behaviors when interacting with sensitive information (Boss et al., 2015).

In today's technologically complex information environments, insiders play an outsized role in maintaining organizational information security. Whether inadvertent, intentional and nonmalicious, or purposeful and malicious, insiders' security-related actions can have serious consequences for organizations (Willison & Warkentin, 2013). Indeed, studies indicate that organizational insiders are responsible for up to half of all reported information security breaches (IBM, 2018; PWC, 2015), and breaches caused by insiders can often be more damaging than those caused by outsiders (IBM, 2021; Miller, 2018). As a recent example, a targeted spear-phishing attack led employees at a Canadian university to believe that a large supplier was changing its bank account details. Over a period of nine days, these employees transferred more than \$11.5 million into a fraudulent bank account. It took more than seven months, as well as undisclosed costs in terms of work hours, legal fees, and fees to outside security consultants, for the university to reclaim roughly 90% of the funds (Canadian Press, 2018).

To help mitigate such insider threats, organizations invest significant resources in developing behavioral as well as technical countermeasures, including protocols, policies, and technologies (PWC, 2015). Yet despite these investments, some employees continue to exhibit organizationally maladaptive responses to security measures (Balozian & Leidner, 2016; D'Arcy & Lowry, 2019; Guo et al., 2011; Willison & Warkentin, 2013). An *organizationally maladaptive response* to security measures is any response other than the organization's recommended, intended, or prescribed response (Burns et al., 2019; Galluch & Thatcher, 2011; Marett et al., 2019; Padayachee, 2012). Maladaptive responses, in part, stem from the plethora of increasing security requirements expected of employees that are sometimes viewed by employees as constraining, demanding, and challenging to understand or follow (Balozian & Leidner, 2016; Posey et al., 2011b; Post & Kagan, 2007). For example, one industry report found the following explanations and justifications for maladaptive responses to IS security measures: "I'm not doing anything wrong," "I need access to programs and applications not sanctioned by my company's IT policy to get my job done," and "I'm too busy to think about my company's IT policy" (Cisco, 2011). In a more recent industry survey, insiders indicated that they "just wanted to get their job done" when engaging in potentially harmful or noncompliant behaviors (Dell, 2017). Academic researchers have found ample evidence that insiders perceive security compliance as burdensome (e.g., Lowry & Moody, 2015), even leading to intentional abuse and/or insider noncompliance (Posey et al., 2011a; Posey et al., 2011b). Thus, the burdens associated with

organizational security measures may induce maladaptive responses.

Although maladaptive responses are not necessarily malicious, they nevertheless pose significant security risks for organizations (Lowry et al., 2015; Posey et al., 2011b; Siponen, 2000; Stanton & Stam, 2006). Because of the substantial threats from maladaptive insider responses, a burgeoning body of behavioral and organizational IS security research has emerged focused on the human actions that influence the security of organizational IS (Burns et al., 2019). Researchers have proposed various theories (e.g., protection motivation theory, deterrence theory, reactance theory, rational choice theory, social information processing theory) to help explain security-related behavior in the workplace. One commonality across these theories is the implication of individuals' beliefs in determining their security behaviors. For example, two of the most widely employed theoretical bases in behavioral and organizational IS security research—protection motivation theory (PMT) and deterrence theory (DT)—both harness beliefs to explain behaviors. PMT-based studies have indicated that beliefs about threat severity and susceptibility influence security-related behaviors such as changing passwords (Johnston et al., 2015) and internet security coping behavior (Chen & Zahedi, 2016). Further, DT-based studies have shown that beliefs about security countermeasures and security sanctions influence IS misuse intentions (D'Arcy et al., 2009). While these influential studies have made substantial contributions to our knowledge of security-related behaviors, the extant research tends to focus more on beliefs about the costs/benefits of compliance, as well as the risks/punishments for noncompliance, than on beliefs about the overarching issue of security per se. Lacking in the IS security literature is the theoretical linkage between beliefs, actions, and individual and organizational outcomes based on the contextualized experiences of insiders themselves.

Thus, although the extant works point to the importance of individuals' beliefs influencing their security-related behaviors (see Table 1 for specific examples), security researchers often limit their examinations to predefined sets of security-related beliefs based on the theoretical framings of their respective studies. This reality potentially hinders our understanding of the full extent to which beliefs may influence employees' security-related behaviors and outcomes. Hence, using an exploratory case study, the current work seeks to expand the set of relevant security-related beliefs through an inductive approach that considers the contextual experiences of employees. Therefore, the research objective of this study is to more comprehensively examine the influence of organizational insiders' beliefs about IS security on their adaptive and maladaptive security-related behaviors. To this end, we employ Melville's (2010) beliefs-actions-outcomes (BAO)

theory of behavior to analyze our qualitative data<sup>1</sup> and develop a novel theoretical framework of insiders' responses to IS security.

Our work extends prior IS security work in three important ways. First, through the lens of BAO, we develop an extended BAO model of insiders' adaptive and maladaptive security behaviors that shows how individual and organizational outcomes, especially individuals' lived security experiences, influence beliefs about IS security. Second, we uncover a novel IS security belief framework that helps explain insiders' responses to IS security based on their beliefs. Third, by engaging organizational insiders in open-ended interviews, we provide a richer, more holistic view of insiders' beliefs about IS security. A primary goal of organizational IS security research is to better understand insiders' security-related behavior. Our study contributes to this goal by revealing four profiles of organizational insiders based upon their security beliefs and tying these beliefs to their security behaviors. Finally, we show a nonvirtuous cycle (i.e., the "adversarial dance"), whereby maladaptive responses lead to new security measures that reinforce negative beliefs and elicit more maladaptive responses. This explains how insiders lived security experiences feed back into their beliefs by fostering new or reinforcing existing beliefs about IS security.

## 2 Related Literature

To help situate our research within the extant body of IS security literature, we next provide a brief discussion of the IS security literature we draw on to develop our study. We then introduce the theoretical frame (BAO theory) for our study.

### 2.1 Background on IS Security Behaviors and Beliefs

A large body of IS security research considers the nature of insiders' IS security behavior in terms of whether it is organizationally adaptive or maladaptive (Marett et al., 2019; Rippetoe & Rogers, 1987). Adaptive responses to IS security measures (e.g., compliant and protective behaviors) are desirable from the organizational perspective. Moreover, the literature takes a distinctly negative view of employees who exhibit maladaptive responses to their organization's IS security measures (Marett et al., 2019). This makes sense because most IS security studies are oriented toward increasing organizational security with adaptive responses (e.g.,

compliant and/or protective behaviors) as the proxy for positive (i.e., more secure) organizational outcomes (Burns et al., 2018). Thus, noncompliant and insecure responses to security measures are viewed as maladaptive from the organization's perspective because they represent responses that differ from the organization's recommended or prescribed responses (Galluch & Thatcher, 2011; Marett et al., 2019; Padayachee, 2012). However, nascent IS security research is starting to expose a potential downside to organizational security measures. For example, D'Arcy et al. (2014) studied stressful encounters with security policies. Labeled *technostress*, this negative outcome experienced by employees trying to adhere to security policies reflects a significant potential cost of security measures (D'Arcy et al., 2014). Further, Lowry and Moody (2015) explain how security policies can create the perception of a threat to freedom in the workplace. Interestingly, autonomy at work constitutes an important psychological requisite of intrinsic motivation (Deci & Ryan, 2000). Thus, when security measures challenge individual freedom at work, resistance (i.e., reactance) is triggered, which relates negatively to organizationally adaptive responses (i.e., compliance intentions) (Lowry & Moody, 2015).

Specific examples of such tensions between insiders' ancillary security responsibilities and their primary organizational role abound. For example, to secure work-related accounts, users are required to create and maintain multiple, complex passwords. This adds cognitive labor to the employees' traditional workload—a problem made worse by the fact that secure passwords should be suitably long, complex, and random (Woods & Siponen, 2018). This reality, more than laziness, apathy, or malice, often explains insecure, maladaptive password behaviors (e.g., password reuse, writing down passwords, sharing passwords, and choosing weak passwords) (Woods & Siponen, 2018, 2019). Thus, many behaviors that are maladaptive from the organizational perspective may appear reasonable from the perspective of the individual. Put another way, some insecure behaviors are actually rational from the users' perspective (Herley, 2009). This is akin to Simon's (1955) "rational man," acting within a context of limited resources and information.

In seeking to understand why employees choose to comply, or not, with security policies, researchers have invoked a variety of theories that identify myriad beliefs relating either to IS compliance and sanctions or to security threats associated with specific IS. In terms of

<sup>1</sup> As common in exploratory case studies, as well as grounded theory and interpretive case studies (See for example Barrett et al., 2012; Fayard et al., 2016; Oshri et al., 2018; Salovaara et al., 2019), we did not begin the study with the objective of studying a theory or applying a theory to an organizational situation but rather entered the study with the

desire to understand an important organizational issue. It is during data analysis that one begins to consider theory to help explain the observations emerging from the data. For the flow of the paper, however, and consistent with prior research, we present an overview of the theory prior to the method in the sections that follow.

compliance beliefs, research has found that rationality-based beliefs such as beliefs about work impediment and vulnerability of resources influence insiders' policy compliance (Bulgurcu et al., 2010) as do beliefs about the use of formal and informal controls by managers to monitor compliance (Hsu et al., 2015). Moreover, deterrence-based beliefs such as the severity of sanction also influence insiders' behaviors such as insider computer abuse (D'Arcy et al., 2009) and justice beliefs about the fairness of detecting and punishing non-work-related internet usage influences employees' use of the internet during work (Li et al., 2014).

Research has also considered beliefs about the threats associated with particular IS. Here the research focuses on beliefs about the potential severity and susceptibility of a specific security threat. Research has found that beliefs about threat severity and susceptibility influence the decision to use anti-spyware software (Liang & Xue, 2010) and beliefs about the risk of internet security attacks influence internet security behaviors (Chen & Zahedi, 2016). Table 1 provides examples of examined beliefs in prior organizational IS security research.

We contend that specific beliefs about one security protocol, policy, or technology may not extrapolate to the larger set of organizational IS security measures. For example, beliefs about the threat from spyware in Liang and Xue (2010) have not been shown to influence beliefs about other IS security measures. Further, the extant literature tends to focus specifically on organizational policy compliance motivations and intentions without considering the broader beliefs about IS security that might guide insiders' security behaviors. We contend that this may partly be a result of the nature of the closed-ended questions studied in prior IS research (Siponen & Vance, 2014).

For example, Bulgurcu et al. (2010) examined the rationality of policy compliance in terms of costs, benefits, and work impediments. However, they did not ascertain the actual impediments. Instead, they relied on employees' responses to statements such as "complying with the requirements of the [policy] holds me back from doing my actual work" (Bulgurcu et al., 2010, p. 537). While it is crucial to understand the influence of impediments, it is challenging to translate this research into action and alleviate those hindrances without a more contextualized understanding of how policies impede work. In addition, both Siponen and Vance (2010) and Lowry and Moody (2015) used vignettes to investigate policy compliance. While vignettes are a widely used technique for eliciting

responses based on carefully constructed but otherwise realistic situations (Siponen & Vance, 2010), they may not necessarily uncover the broader personal beliefs of the respondents about their actual experiences in the workplace. For example, Siponen and Vance (2010) examined the role of neutralization techniques such as denial of injury by capturing individuals' responses to items, including "it is OK to violate the company information security policy if no harm is done." However, qualitative approaches, such as interviews and case analyses, can provide complementary insights into how the user determined whether harm was done, and who or what could be harmed by violating policies. Meanwhile, Lowry and Moody (2015) studied the influence of reactance to proposed policy changes on compliance intentions by asking whether the policy would "trigger a sense of resistance." Qualitative approaches may supplement these findings to better understand users' actual responses to their organizations' security policies.

Lastly, Burns et al. (2018) examined behaviors in terms of expectancies, using items such as "it would be good to protect my organization from information security threats." Here, as in the previous examples, the closed-ended, forced-choice items do not allow researchers to fully capture the rationalization process or underlying beliefs leading to the judgment that protection is good or whether it is good for the organization, the user, or both. These examples are not intended to diminish the contribution of this prior research in any way but to uncover an important research opportunity to complement these prior works with new contextualized theories based on insights derived from insiders in their work setting. To better understand specific IS security beliefs and behaviors, we investigate insiders' general IS security beliefs from their own perspectives and assess how these general beliefs influence their IS security behaviors.

## 2.2 Background on BAO Theory

To understand how individuals relate to IS security measures, we draw upon Melville's (2010) BAO theory as our theoretical lens.<sup>2</sup> BAO theory is well suited to explain the influence of insiders' beliefs about IS security because it provides a framework for understanding how macrofactors such as organizational structures influence individual (microlevel) beliefs which, in turn, influence individuals' actions. In addition, as BAO posits, it is individuals' actions that ultimately bring about organizational (macrolevel) outcomes (Melville, 2010).

<sup>2</sup> As an exploratory case study, we used an inductive approach during our early rounds of data analysis to determine the most appropriate theoretical lens to help derive insights from subsequent rounds of our data analysis. We

present the theory here rather than in the method section to help orient the reader in the analysis that follows.

**Table 1. Examples of Beliefs in Prior Organizational IS Security Research**

Citation	Theoretical frame	Topic	Beliefs	Examples of belief measures
Bulgurcu et al. (2010)	Rational choice theory	Policy compliance	Compliance rationality-based beliefs	<b>Work impediment:</b> <i>Complying with the requirements of the ISP holds me back from doing my actual work</i> <b>Vulnerability of resources:</b> <i>If I don't comply with the requirements of the ISP, my resources will be at risk.</i>
Chen & Zahedi (2016)	Protection motivation theory	Internet security coping behaviors	Internet security beliefs	<b>Susceptibility:</b> <i>my risks of getting Internet security attacks are (very low/very high)</i> <b>Severity:</b> <i>in general, the severity of security attacks for me is (very low/very high)</i> <b>Self-efficacy:</b> <i>my knowledge for taking preventive actions is (not adequate at all/very adequate)</i> <b>Response efficacy:</b> <i>the success rate of protective actions is (very low/very high)</i>
D'Arcy et al. (2009)	Deterrence theory	IS misuse Intention	Security counter-measure beliefs Security sanction beliefs	<b>Monitoring:</b> <i>I believe that my organization monitors any modification or altering of computerized data by employees.</i> <b>Perceived severity:</b> <i>If caught sending the e-mail, Taylor's punishment would be: (not severe at all/very severe)</i>
Hsu et al. (2015)	Social control theory	In-role security behaviors Extra-role security behaviors	Beliefs about information security policies (ISPs) compliance	<b>Formal controls:</b> <i>Managers in my department frequently evaluate my security behaviors.</i> <b>Social controls:</b> <i>Following IS security policies is the right thing to do.</i>
Johnston & Warkentin (2010); Johnston et al. (2015)	Protection motivation theory Fear appeal theory	Changing passwords	Threat-based beliefs	<b>Severity:</b> <i>If my password was stolen, the consequences would be severe</i> <b>Susceptibility:</b> <i>My password is at risk of being stolen</i> <b>Self-efficacy:</b> <i>Changing my password is easy to do</i>
Li et al. (2014)	Deterrence theory Organizational justice theory	Non-work-related internet usage	Organizational justice beliefs	<b>Procedural justice:</b> <i>The security procedures for detecting and punishing non-work-related Internet usage are applied consistently to everyone in my organization.</i> <b>Distributive justice:</b> <i>The increase in my productivity is worth the inconvenience or other loss that I may suffer from restricting nonwork-related Internet usage.</i>
Liang & Xue (2010)	Technology threat avoidance theory	Spyware/Antispyware software	Threat-based beliefs	<b>Susceptibility:</b> <i>My chances of getting spyware are great</i> <b>Severity:</b> <i>Spyware would invade my privacy</i> <b>Threat:</b> <i>Spyware poses a threat to me</i>

Adapting our terminology from Melville (2010), we define *beliefs* as comprising psychic states (e.g., beliefs, desires, and opportunities) about the organizational environment in which an individual interacts. *Actions* are the various ways in which beliefs translate to behaviors and *outcomes* reflect the ultimate organizational states created by and resulting from the actions (Melville, 2010). BAO, like other theories of complex systems (e.g., Choi et al., 2001; Simon, 1996; Waldrop, 1992), explains a coevolutionary system whereby the macrolevel social (including organizational) environment influences beliefs that

precipitate actions, which ultimately then lead to behaviors in the macrolevel social environment.

Although BAO theory was developed specifically in the context of environmental sustainability, we suggest that the model is relevant in other contexts where individual beliefs are shaped by the external environment and, more importantly, where individual actions potentially affect the larger social system. The latter is very much the case with organizational IS security, where the maladaptive behaviors of even one employee can result in significant risk to an organization.

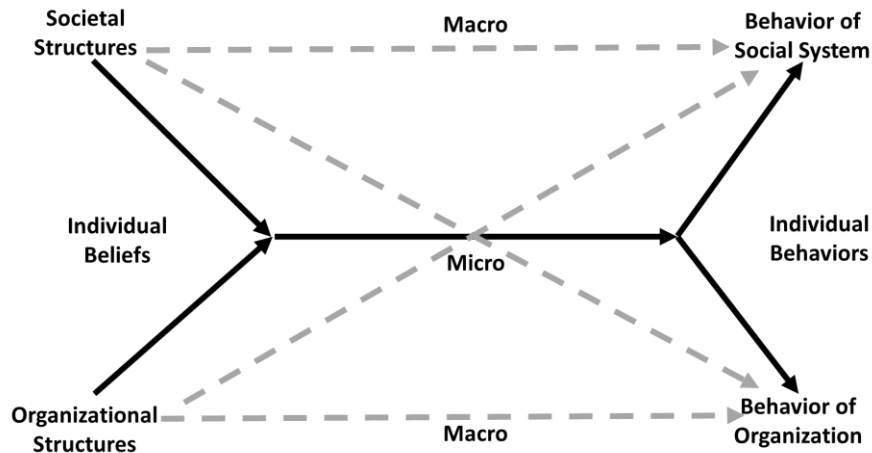


Figure 1. BAO Model Adapted from Melville (2010)

Figure 1 exhibits the adapted BAO model. Because we are interested in employee behaviors, we were particularly interested in the paths that travel through the individual microlevel of the model—that is, the solid rather than the dashed lines in Figure 1. The remainder of our paper will present our method, data analysis uncovering influential security beliefs, and our emergent security belief-response framework.

### 3 Methodology

We employ an exploratory case study using a single revelatory case. Single case studies are common in IS research because they offer researchers the potential to reveal new insights through unique, extreme, or particularly revelatory cases (Yin, 1989). For example, prior IS studies employing single cases have been published in the context of healthcare (Johnston et al., 2019a), energy (Karjalainen et al., 2019), banking (Gregory et al., 2018), government (Koutsikouri et al., 2018), and real estate (Montealegre et al., 2019), among others.

The case site is a southwestern private higher education institution (PHEI) in the United States comprising ten colleges and employing approximately 1,000 staff and faculty. At the time of this research (i.e., 2015-2016), the university had a range of \$250 to \$350 million in operating cash, with total assets between \$2 billion and \$4 billion. Information security is highly valued by the university. The position of chief information security officer (CISO) was created in 2008. The higher education sector is a highly relevant and credible context for information security research because it has become a major target of security breaches in recent years. In 2018, 58% of all higher education institutions in the United States experienced at least one public data breach, over half of which cost the institution \$500,000 or more in remediation (Cisco, 2018). More recently, the

education/research sector sustained the most cyberattacks in 2021 (Brooks, 2022), and the FBI warned of an increase in ransomware attacks targeting colleges (McKenzie, 2021).

To the best of our knowledge, at the time we conducted our study, PHEI had not had any information security breaches reported in the news. The organization is at the forefront of security implementations and serves as a model for other institutions. As examples of some of the security initiatives, in 2014, two-factor authentication VPN was implemented so that those users who were overseas and/or off campus but wanted to access specific systems were not able to access the network without an added factor of authentication. In early 2017, double-factor authentication was enforced on three other commonly used systems. PHEI has also adopted additional security, including encryption, to all institutionally owned computers. All such devices are tracked and remotely accessible by PHEI's IT department and can be wiped if stolen or lost. This strong emphasis on security policies, coupled with the recent security changes (at the time of our research), makes PHEI a good site to analyze users' actual responses to security measures.

#### 3.1 Data Collection

Data collection consisted of conducting 32 semi-structured interviews across the research setting (we provide two tables to preserve respondents' anonymity: see Table 2a for an overview of the respondents' roles, and Table 2b for specific roles). Five types of data were collected: (1) interviews with the IT department, (2) interviews with end-user professionals, including faculty members, administrators, and administrative staff, (3) all internal documents on IS security policies, (4) Q&A emails exchanged with IT security specialists, and (5) notes taken during attendance at a security awareness meeting designed for end users.

**Table 2a. Overview of Respondents' Roles**

Resp #	Position	Resp #	Position (cont.)
1	IT Director	16 & 23	IT director (2 interviews)
2	Faculty	17	Non-IT director
3	Faculty	18	Academic support staff
4	IT Staff	19	Faculty
5	IT Client services (staff)	20	IT director
6	IT Director	21 & 22	IT director (2 interviews)
7	IT Staff	24	Faculty
8	IT Client services (staff)	25	Non-IT director
9	IT Staff	26	Academic support staff
10	IT Client services (staff)	27	Faculty
11	IT Director	28	Faculty
12	IT Director	29	Non-IT director
13	IT Client services (director)	30	Non-IT director
14	IT Staff	31	Academic support staff
15	IT Staff	32	Academic support staff
IT Positions: 16 7 IT directors 5 IT staff members 4 IT client services staff members		Non-IT Positions: 14 5 Non-IT directors 6 Faculty members 4 Academic support staff members	
Note: Total respondents: 30 (32 total interviews); 37% female			

**Table 2b. Specific Roles**

Position	Position (cont.)
Advanced technology repair specialist	Director of online teaching and learning services
Assistant director, academic and research computing services	Director, client support services director, graduate business degree programs
Assistant professor—tenure track	Director, undergraduate programs
Assistant vice president and chief information security officer	Office manager 1
Assistant vice president for client services	Office manager 2
Associate librarian	Professor 1
Coordinator, academic support services in a school	Professor 2
Desktop configuration specialist	Professor and chair 1
Director of a computer center	Professor and chair 2
Director of budget management	Project manager, instructional technology
Director of IT client services	Senior academic consultant
Director of communications and marketing	Senior academic consultant, faculty technology
Director of hardware support and technology systems consultant	Senior analyst/programmer
	Software support specialist 1
	Software support specialist 2
	Temporary full-time lecturer

The interviews ranged in length from 20 minutes to an hour. The semi-structured interview guide (See Appendix A) was designed to elicit the participant's viewpoint rather than superimpose any predetermined viewpoint with appropriate follow-up questions to ensure elaboration and clarification from each respondent (Marshall & Rossman, 2011). We were careful to avoid leading questions that might bias the respondents. The interviews were recorded and transcribed.

### 3.2 Data Analysis

We used an inductive approach to analyze our data, following the guidelines of Gioia et al. (2013). Our approach involved iterating within and across three

orders of analysis. In the first-order analysis, directly extracted quotes established first-order concepts. These concepts are expressed in the words of the respondent and are neither limited by predetermined theory nor forced into distilled categories (Gioia et al., 2013). We thus left these concepts in the precise wording of the respondents in our various tables (see Appendix A). The first-order analysis initially created an extensive list of quotes/concepts from the respondents, which provided an employee perspective on security. Several iterations within the first-order analysis helped us notice similarities and differences in the concepts, reducing the overall number of relevant concepts and triggering the second-order analysis. The concepts beginning to converge in the first-order analysis involved general beliefs about security, the

implications of security for the individual and organization, the security behaviors the individuals engaged in, and the security experiences the individual had encountered.

The second-order analysis focused on inductively abstracting the concepts into themes that helped explain the phenomenon under study (Gioia et al., 2013). Whereas the first-order analysis adhered closely to informants' language and was completed without attention to theory, the second-order analysis sparked attention to existing theory that might serve as an appropriate referent for the emerging themes. We iterated within the second-order analysis several times as we considered various theories in the security literature before eventually determining that BAO theory was the best fit. At this point, BAO became our theoretical lens for the subsequent analyses. From the second-order analysis, we noted four important beliefs (the belief that a security breach is unlikely to seriously harm the organization, the belief that a security breach is likely to seriously harm the organization, the belief that IS security measures are not always important, and the belief that IS security measures are always important) and three security behaviors (avoidance of IS, circumvention of IS security, adaptive IS behavior).

In the third-order analysis, the researchers considered whether the second-order themes could be further distilled into "aggregate" dimensions. When themes from the second order coexist, they may then comprise an even higher-level construct. Figures A1, A2, A3, and A4 in Appendix A show the first-, second, and third-order analyses that resulted in our identification of two broad beliefs—the belief about the risk of a security breach to the organization and the belief about the importance of IS security measures—that influenced IS security behaviors, resulting in favorable and unfavorable lived experiences. The third-order analysis also revealed the relationship between the themes, leading us to note that the coexistence of several beliefs formed a pattern, which then formed the basis for the identification of the four security profiles (Figure 2 in Section 4).

These first-, second, and third-order analyses served as the basis for building a data structure (Figures A1-A4). These data structures not only provided a depiction of the progression from raw data to themes and dimensions but also themselves acted as a theoretical trigger, pushing the researcher to consider existing theoretical explanations of the relationships of the themes and dimensions while also spurring new theoretical insights (Gioia et al., 2013). The ultimate aim was to build an inductive model that is grounded in the data and that theoretically captures the respondents' perspectives (Gioia et al., 2013).

As a means of verifying the four security profiles and three security behaviors that had emerged through our

inductive analysis, we then undertook a fourth-order analysis. This fourth-order analysis involved ensuring that the framework we had developed from the previous three orders of analysis could be verified in the individual transcripts. For this analysis, we recruited four coders (PhD students) who were uninvolved in the first three analyses. Two coders were assigned to each transcript. The two coders independently coded the transcripts according to the framework. They specifically coded according to which profile each respondent represented and which behaviors each respondent exhibited (a table exhibiting the data structure for each respondent is included in Appendix D). The interrater reliability was high (>85%). This final coding stage ensured that our inductive analysis could be deductively applied with high reliability. This is important as a means of verifying that the inductively derived framework was not limited in applicability to a small number of respondents. We further complemented this analysis with additional data collection, namely seven additional interviews and a survey of 120 individuals working in a range of industries, to verify our analysis in other contexts besides higher education (see Appendices B and C). The results of both supplemental analyses lend support to the cross-industry relevance of our findings, confirming that the framework emerging from our qualitative analysis in a single industry is applicable to employees across a range of industries. We randomized and changed the pronouns of the respondents appearing in the findings to preserve anonymity.

## 4 Findings

Informed by BAO theory, our inductive analyses uncovered two important security-related beliefs with associated actions and outcomes. From the two security-related beliefs, we derived a security belief framework consisting of four profiles. Each profile in the framework corresponds to a set of responses (actions) and outcomes. Individual and organizational outcomes recursively influence beliefs, creating the potential for virtuous and nonvirtuous cycles of IS security behavior. We now describe these findings in detail.

### 4.1 IS Security Belief Framework

Two broad security beliefs were expressed by the employees of PHEI: (1) beliefs about the likelihood and impact (i.e., the risk) of a security breach and (2) beliefs about the importance of IS security measures. In terms of the first, insiders varied in their beliefs about the risk of a security breach at their organization, with some employees believing that a security breach poses a serious risk to the organization, as revealed in statements such as "I know that a security breach of social security numbers will affect our reputation" and "I do believe that a 'real' breach of security could hurt

the university.” Other employees, however, believed that a security breach would be unlikely to seriously harm their organization, as exemplified in statements such as, “I don’t think a security breach will affect the reputation of the institution. As far as I know, a security breach is a very common thing. It’s the norm in this century. People are becoming used to it.” Table 3 summarizes these beliefs about the risk to the organization from security breaches with the associated codes/indicators from the interviews (see also Figure A1 in Appendix A for more examples and the data structure).

The second broad belief concerns the importance of the organization’s security measures (e.g., policies, protocols, and technologies). We found that some insiders believe that security measures are always important. For example, when discussing the need for certain IS security policies, one respondent expressed a belief that these policies are universally important:

*I know back last spring when we had a program that IT did for us talking about internet security, keeping our information safe and that type of thing, and some of our users were just really kinda surprised he was telling them that you don’t share your password, you don’t share your information with even your closest contacts because they can do some harmful things to your account if they’ve got that information. I don’t understand why they were surprised. These policies are there for us and they are crucial for our account security.* (Respondent 2)

Other employees do not believe IS security measures are always important. For example, one employee

expressed the belief that some IS security measures should not apply to every employee: “I do not understand AT ALL why my laptop needs to be encrypted” [emphasis added]. Another respondent noted:

*My data in the grand scheme of things is not important data. Top secret data, financial data, that’s important data. Identity data, that’s important data. My application data is important to us. It’s not important outside of us. No Russian hacker wants to get into a learning management system just so they can change the content. So, I don’t see the importance of many of the policies and measures.* (Respondent 10)

Table 4 summarizes these beliefs about the importance of IS security measures (see Figure A2 in Appendix A for more examples and the data structure).

These two broad beliefs were found to exist across all respondents, e.g., no respondent was unaware of security and security measures. From these two beliefs, a security belief framework emerged delineating four employee security profiles—IS security overindulgence, IS security indulgence, IS security disconnect, and IS knows best (Figure 2).

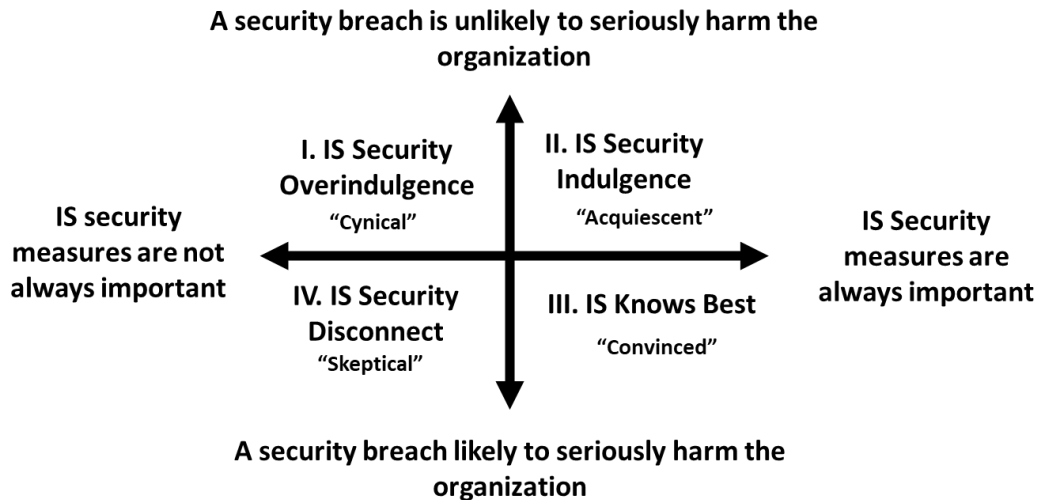
Among our respondents, six employees fit the “IS security overindulgence” quadrant (four IT staff and two professional users), five employees fit the “IS security indulgence” quadrant (one IT and four users), 14 employees fit the “IS knows best” quadrant (eleven IT and three users), and five employees fit the “IS security disconnect” quadrant (all of them users). Appendix D exhibits the profile classification for each respondent in our study. We now describe each profile in detail.

**Table 3. Insiders’ Beliefs about Security Breaches**

Dimension / belief	Definition / meaning	Selected codes / indicators
A security breach is unlikely to seriously harm the organization.	A security breach is unlikely to seriously harm the organization’s operations and reputation.	Security not crucial; security not important; only IT department domain; reason for IS security not related to organization
A security breach is likely to seriously harm the organization.	A security breach is likely to seriously harm the organization’s operations and reputation.	Security very important; security breach consequences harmful; security breach harms reputation; security breach harms operations

**Table 4. Insiders’ Beliefs about the Importance of Security Measures**

Dimension / belief	Definition / meaning	Selected codes / indicators
IS security measures are not always important.	It is not always important for employees to have an organizationally adaptive response to IS security measures.	IS security policies are over and beyond; IS security policies important only for IT department; employees not having sensitive data; no effect of employee laptop breach on organization
IS security measures are always important.	It is always important for employees to have an organizationally adaptive response to IS security measures.	Compliance is crucial; employees as weakest link; noncompliant employees should leave organization



**Figure 2. Insiders' Beliefs about the Importance of Security Measures**

#### 4.1.1 Belief Profile 1: IS Security Overindulgence

The "IS security overindulgence" profile represents a cynical mindset toward IS security. Individuals in this group believe that security breaches do not pose a serious risk to PHEI and that security measures are not always important. A quarter of our respondents, including members of the IS/IT staff as well as professional users, exhibited the IS security overindulgence belief profile. The IT professionals exhibiting this profile are the IT client services staff members serving the faculty, staff, and administrators in their business and functional needs. These respondents are responsible for finding software, solutions, or applications on the market to serve the functional needs of business units. Applications may range from proctoring software to learning management systems and many other applications that support or enhance teaching, research, and administrative productivity in higher educational institutions. These IT professionals are evaluated based on their performance: how many and how fast they find solutions and how successfully these solutions meet business needs. The IT client services staff members expressed pride in the number of solutions they are able to find, suggest, and implement that solve functional problems and expand the university's opportunities in PHEI (Respondents 5, 10, and 13). They reported that their efforts often run counter to the IT security team's focus on minimizing vulnerability, leading the team to reject many of the solutions proposed by the IT client services staff.

We found that the beliefs of these IT client services staff members are driven by their view that industry standards in the marketplace are adequate for the university as well. They may not see security breaches as a severe problem (e.g., "I use my credit card at

Home Depot. Home Depot had a breach. Okay. That's no big deal. You get the credit monitoring. You go on with life." Respondent 10) and tend to feel that IS security measures need not go beyond industry standards.

One IT project manager whose role is to find software solutions on the market and make recommendations for their adoption at PHEI experienced frustration at a solution being rejected on security grounds although "it's a widely used system" among universities and "none of them [the other universities] have any problems with it." He felt as if the university was trying to impose future standards on today's world: "They're trying to get out ahead of it and require what's going to be standard in a few years, but why we're requiring it now, I have no idea ... Okay, if it's [the software] standard in the industry and everybody's okay with that, why are we not? I don't understand it."

Other professionals who are evaluated based on productivity also exhibited the IS security overindulgence belief profile. Specifically, these employees are evaluated based on maintaining a high number of program enrollees (Respondents 25 and 30) and/or a strong focus on research (Respondent 28). These professionals are sensitive to IS security measures and have a low tolerance for protocols, policies, and technologies that impede their productivity. Many reported similar beliefs that IS security measures may be overindulged, aptly summed up by one senior faculty member:

*I think at least in my case that the approach they take to this is over-control, you tend to develop just the impression that they over-control because of the way they handle their security and other things. And so, then they have this reputation for over-control, and not being there to really serve you. You've*

*got to release a little bit of control. You should be more concerned with focusing on the areas that are the biggest threat than focusing so much on the devices and securing the devices and stuff like that.* (Respondent 28)

In summary, we found that some employees exhibit a cynical mindset toward IS security. These insiders often find measures that go beyond what they view as common in other institutions and industries to be inadequately justified in their workplace. For these users, excessive security is viewed as a hindrance to their productivity (Respondents 25, 28, and 30). This IS security belief profile is not surprising given that the productivity of these individuals is often the organizational *raison d'être*.

#### 4.1.2 Belief Profile 2: IS Security Indulgence

The “IS security indulgence” profile characterizes employees who believe that although a breach will not cause significant harm to the organization, security measures are nevertheless always important. This acquiescent perspective of IS security reflects a belief that security measures are important regardless of their instrumentality. Thus, these insiders tend to be acquiescent to security measures despite their belief that security breaches are not a serious risk to the organization. This belief profile may indicate that the insider is a “good soldier,” willing to follow orders, or these individuals might simply find it more expedient to accept IS security measures, as suggested in the following quote:

*I think we just assume that they have the appropriate amount of security to protect the systems that we have, and if they ask us to change passwords every three months or every six months or something, people just do it.* (Respondent 24)

We asked another faculty member about her knowledge and experiences with the virtual private network (VPN) security guidelines. She responded:

*I know that you do have to agree to certain policies as you begin to use things like a VPN, but for the most part, that's fairly standard, so I don't have any problems with agreeing to any of the policies.* (Respondent 27)

As shown in these examples, the indulgent mindset toward IS security is deterministic: security measures should be adopted without regard for instrumentality (i.e., whether a security breach is a serious risk), justification (i.e., whether the IS security group has made its case convincingly), or hindrance (i.e., whether the measure impedes an individual's work). This mindset was seen typically in non-IT professionals who either have solely administrative

duties (Respondent 26) or primarily perform routine work (Respondents 24, 27, and 29). Those exhibiting IS security indulgence profile typically do not bother rationalizing the security measure by assessing whether it is mitigating serious risk; rather, they simply acquiesce to IS security measures.

#### 4.1.3 Belief Profile 3: IS Security Disconnect

The “IS security disconnect” profile depicts employees who believe that a security breach will likely damage the university, but they nevertheless do not consider security measures to always be important. This skeptical mindset toward IS security reflects a disconnect between beliefs about the risk from a breach and the benefit of the organization's security measures. For example, an insider may believe that some devices and accounts should be protected with enhanced security measures but they do not believe that their own account or their own laptop needs these measures because they are not security sensitive. One program director and senior professor expressed these views by saying:

*I do not understand AT ALL why my laptop needs to be encrypted. Even if someone stole my laptop and even if that someone managed to guess my password (both events are unlikely and their simultaneous occurrence even more unlikely), I do not believe that this breaches the university's IT security. I do believe that a “real” breach of security could hurt the university. I just do not believe that a “real” breach can be effectuated through my computer.* (Respondent 19)

Another example of an IS security disconnect is when professionals do not believe that a banned system constitutes a security breach. We observed the IS security disconnect belief profile in the university's recruitment department for graduate programs. Briefly, a recruitment manager purchased and began using an analytics application in 2008. At the time of its initial purchase, the application had been approved by the IT department. Yet after the establishment of the CISO position and the strict focus on security, the application was no longer being approved for use in other departments on campus. Aware of this change in security measures, the recruitment department wanted to keep a low profile to continue using the system, stating:

*I think they go overboard on security. That's another thing. We didn't have any problems using our software, but that was before. I've been using it since 2008. I know another department is trying to add the same software we're using, and PHEI is giving them fits. I got lucky.* (Respondent 30)

One junior faculty member expressed the disconnect between the security measure and the risk: “Why do they need to enforce double authentication on the systems that contain the grades, the course lecture PowerPoints? I don’t understand it. If at all, let them secure the social security numbers and banking information of the students” (temporary lecturer).

#### 4.1.4 Belief Profile 4: IS Knows Best

The “IS knows best” profile represents employees’ beliefs that security measures are always important and that a security breach in the organization is likely to seriously harm the organization. Employees fitting this profile are convinced of the threat of IS security and the importance of security measures. Thus, they are willing to put their organization’s security interests above any personal inconveniences that following security measures might entail. Not surprisingly, IS professionals who are either in senior IS positions (Respondents 1, 12, and 16) and/or whose job roles entail (fully or partly) the enforcement of security measures (Respondent 22) or the configuration and/or support of software implementations (Respondents 9, and 15) exhibited this response. However, a few non-IT/IS staff exhibited this belief profile as well.

The IS knows best profile exhibits a strong positive attitude toward security measures. One respondent explained with pride how the IT department uses a method created by the US Department of Defense to erase all computers prior to recycling them:

*We’ll bring the computer back, wait for two weeks to make sure they (the users) have all their files, and then we use the magnetic storage data sanitization. The department of defense has kind of a method that uses seven passes to wipe a hard drive. We wipe it with that. From there, the computers go to pallets to be sold to recyclers. They have to be certified, basically.* (Respondent 9)

Employees exhibiting the IS knows best profile are quick to dismiss any inconvenience incurred by users resulting from PHEI’s security measures, often indicating a belief that the organization’s IS security measures are justified. When asked about the possible downsides of the mandated encryption on the institutionally provided laptops, the director of the repair shop replied:

*It’s an inconvenience, but I think most people probably understand the need for the security. There is a little bit of delay [in the repair of the institutionally provided laptops], as I mentioned, if we’re trying to recover data or trying to run some utilities on the drive, the drive needs to be unencrypted. But again, I think most people understand why the security is there. Once we explain*

*what we have to do, they’re pretty understanding about that.* (Respondent 1)

The IS knows best profile typifies a belief in the necessity of continuous security improvement. An IT executive summarizes their attitude well:

*People are like, “That’s inconvenient.” I’m not saying it’s not inconvenient. I’d never make that claim. But what I’m saying is that the risk is so high that we have to take some additional action. Most of our, what I would say, changes that we do, absolutely come into place because there’s evidence to back up why we’re doing this.* (Respondent 22)

Unlike the other more cynical, skeptical, and acquiescent mindsets, the IS knows best profile does not express doubts about the decisions of the IS security team but instead fully endorses the IS security measures, believing they are always important and fully justified. For example, an administrative user who also has a background in federal security contracting noted succinctly, “IS security measures at PHEI are not constraining.” She further expressed her positive attitude toward the IS security policies by adding:

*There’s an understanding of why they do what they do, and a thankfulness. I don’t fault them for the layers they put in place, and I don’t find they’re without reason. I think that the way they operate it is quite reasonable, especially for the amount of knowledge, and security, and information they store and maintain. When you think about having to pull transcripts from 15 or 20 years ago, and with the incoming class of freshman of over 3,000 and multiply that. That in and of itself is just massive. Then you have the financials that have to be maintained, tuition records, and everything else. It’s an immense amount of information that’s required. I will never fault them in protecting that knowledge. I’m not saying don’t ever question, but when it comes to things like this, if you have a problem with this, why are you working here? We keep our information more secure than the government does, and I’m happy with that.* (Respondent 31)

In summary, we found that the “IS knows best” mindset toward IS security is characterized by professionals who are fully convinced and consistently endorse IS security measures in the organization. While this might seem obvious coming from the IT staff, we found some ordinary users that had “IS knows best” responses as well. Interestingly though, not all IT staff members fit the “IS knows best” mindset, underscoring the challenges faced by IT security staff in convincing all insiders to take security seriously.

## 4.2 IS Security Response: Actions

Having established the IS security belief framework emerging from our analysis, we now discuss the adaptive and maladaptive responses (actions) observed across the four profiles. While adaptive responses typically resemble IS policy compliance, the maladaptive responses mostly fit into one of two categories: (1) avoidance of IS and (2) circumvention of IS security. Figure A3 in Appendix A shows the data structure for the IS security responses.

### 4.2.1 Organizationally Adaptive Response

Perhaps the most important, if not the most interesting response, is the organizationally adaptive response to IS security. From the perspective of the organization, this is the appropriate and desired response. The reasons for this are almost self-explanatory: an organization enacts protocols, policies, and technologies specifically so that insiders will adapt their behaviors in a way that protects organizational interests. Not surprisingly, we found this response was most prevalent within the IS knows best profile, as illustrated by the following quotes:

*Myself, as a user, I think all of us need to follow the rules even if sometimes we don't understand the "why" behind such rules. (Respondent 2)*

*We had to go through ITS to make that happen and particular through the systems and security group. And it's tedious. I mean, it's cumbersome because now you've got this added layer of bureaucracy to have to deal with. But from an IT perspective, I can see the importance of it. It's a way of catching potential vulnerabilities. (Respondent 11)*

*The fact that ITS chose to implement two-factor authentication to be able to VPN into campus was a good move to strengthen the security without, in my mind, adding a whole lot of burden to people to be able to use that (Respondent 20)*

*I'm not saying don't ever question, but when it comes to things like this, if you have a problem with this, why are you working here? We keep our information more secure than the government does, and I'm happy with that. (Respondent 31)*

We also found that insiders with the security indulgence and security disconnect profiles occasionally exhibited adaptive responses. In the latter case, the insiders behave in an organizationally adaptive manner but they perceive negative consequences, such as reduced productivity or inferior system usage. We will address these individual outcomes after describing the organizationally maladaptive responses.

### 4.2.2 Organizationally Maladaptive Avoidance of IS

One organizationally maladaptive response is the avoidance of impacted systems and technologies. We observed this in insiders' avoidance of the VPN and the avoidance of encrypted devices (laptops, tablets, smartphones, etc.). The coordinator of academic services explained the avoidance of the VPN as follows: "I haven't used it since there's a double authentication. I don't want to use it any more than what I have to. I'd use it more if it was easier for me." Here, the user is acquiescent to the security measure but will avoid the technology if possible in response to IS security. Another professional user described her experience with this additional work and explained why she opted out of VPN use:

*It seemed like every time I went back into it [VPN], it changed. It looked different. It changed the way it did it. It was asking me to put in a different password. I was always having to go online and read the rules to use it again. I just stopped, and just said it would be more productive for me to do it at work where I don't spend all the time getting that set up to use it than trying to use it at home. I quit using it ... I used to be the one who could explain to everybody how to do it at home. Now I don't even know how. I don't think anyone in our office uses that to answer questions at home ... It just got that much more complicated to do. (Respondent 29)*

Another example of avoidance is an employee not wanting to use an institutionally owned laptop because of encryption. PHEI started enforcing encryption on organizationally owned laptops to protect the data on the mobile device in case of loss or theft. Nevertheless, the encryption service does not come without a cost. Encryption places at least two additional burdens on the user. When a laptop has technical problems and is sent to the repair services on campus, the encryption significantly adds to the repair time because decrypting a device with mirroring technology takes time. The user is left without the mobile device for two or three more days. Additionally, the encryption requires that the user add a new passphrase (or password) that is unique to the encrypted device. To be secure, only the owner of the device should know the passphrase. Thus, users will not be able to have their device repaired if the passphrase is forgotten. The only option is to wipe the device and reinstall all applications and any backed-up data, a process that adds considerable time and complication to any repair. One of the staff members explained that he refused a university-provided laptop because of the encryption:

*Like one of the things that IT wants is if you have a laptop, your hard drive has to be encrypted. That's the rule, which is one of the reasons why I don't have a [PHEI issued] laptop. (Respondent 4)*

A leader in a senior position in the IT department summarizes and confirms this phenomenon of avoidance:

*I think the one thing the faculty really did not like was that we required, five years ago, I think we started requiring all laptops to have encryption. And, that seemed to create some issues, because even reimaging a system was no longer easy to do, because you had to spend hours decrypting, before you could work on the computer. So, it slowed us down, basically. It slowed the turnaround time to fix problems, and that kind of thing. The PGP ["pretty good privacy"] password is different from any other password you have. So, that meant that the user had to remember yet another password. The PGP password is much more sensitive, it has a lot more requirements than any other system that we have ... Yeah. So, their way of circumventing that policy is not to use a laptop at all. That was really their only way around it. (Respondent 16)*

Evidence from the interviews suggests that avoidance of IS security was most associated with the IS security indulgence profile. These individuals tend to believe that the IS security measures are important for them to follow, despite feeling that a security breach is unlikely to have a serious impact. Thus, they feel a disconnect between their requisite measures and the outcome of IS security. Rather than violate the IS security measure, they avoid the measure by avoiding the system that it applies to. Because these systems and technologies are usually adopted by the organization for specific purposes (e.g., improved efficiency or productivity), avoidance of them is an organizationally maladaptive response to the IS security measure.

#### **4.2.3 Organizationally Maladaptive Circumvention of IS Security Measures**

Perhaps the most troubling of the responses to IS security is the potential for security measure circumvention. We observed deliberate security measure circumvention by users with the IS security overindulgence and IS security disconnect profiles.

One area where circumvention was widespread was that of password changes, with an increase in a security measure requiring the new password to not have been used in one of the previous four rounds. Symbols (so-called "special characters") are required in passwords

yet certain symbols are not allowed in specific systems: for example, an application system where program directors can review student applications would not validate the user name/password if the password contained a "\$" sign, but users would not know this until after they had changed their password and tried to use that particular system only to have it not allow access. Password change thus created a burden for users because it was never known in advance if the password chosen would be permissible on all the systems the user might need to access. One common method of circumventing the password change security was by changing the password five times consecutively over several minutes so that the original password was always used. Said one faculty user, "I used to change one letter in my password each time, but I'd often forget which letter I'd changed. One time, a friend who works in IT support was in my office and it happened to be time to change my password. I complained about the frequency of these changes and why it was necessary. She suggested that I simply change the password five times until the system allowed me to reuse my original. She said that's what many of the IT staff did." Several faculty and staff reported such password change circumvention behavior.

Other maladaptive password behaviors that respondents reported took the form of using the same (or similar) passwords across personal and work accounts at the same time and writing the password on unsecured devices. PHEI's updated password policy specifically stated that all users should have a password for university systems that was different from any personal passwords that they used for other systems. However, users were widespread in admitting that they used the same passwords and one program director estimated that "50% to 75% percent of my staff reuse passwords." Ironically, tighter security measures made users feel unthreatened even when their passwords had really been hacked. One program director reported that she inadvertently opened an email in her junk mail that looked like it was from the IT department. She clicked the link and entered her ID and password before realizing that it was not really from IT. She called the IT department to ask what to do. They told her to immediately change her password. However, she opted to not change her password. Her reasoning was that "they have so many layers of security. Even if someone has my ID and password, I doubt they can access anything strategic." Her belief that security at PHEI is excessive allowed her to justify behaving in a highly unsecure manner.

Other forms of circumvention included the continual defiant but "underground" use of systems, the emailing of grades to students, and the violation of Dropbox policies. An example of the first was given by the director of the graduate programs whose use of an inexpensive data mining application was subsequently banned:

*Do we really need as much security as they're telling us we need? I don't have details of that. I try to stay under the radar with this program we use so they don't come after me, since it was implemented with PHEI's support, but implemented before some of these extra security layers have been added. (Respondent 30)*

This perception of the IT department as hypervigilant or unrealistic about departments' needs also relates to circumvention by emailing grades to students:

*It's almost impossible not to include grades, but they really don't want us to do that ... We just don't comply [with IS security team policy]. We really have to write the grades in our email correspondence with the students because it may be right before they go to class and take a final. You never know what the situation is. (Respondent 29)*

And a faculty interviewee who claimed that the IT security measures were primarily being done to “give the IT security guys something to do” confessed to circumventing the Dropbox policies. This user also tried, unsuccessfully, to remove the PGP passphrase protection from a laptop and to change the auto-sleep setting on a laptop to never (something that was prohibited by the installed security software). Phrases like “a silly reason,” “unlikely scenario,” “obscure example,” “[IS security team] not being there to really serve you,” and “[IS security team] is all about control” were common among those respondents who circumvented IS security measures. The above findings suggest that increased security measures can, in some cases, reinforce the belief that security measures are not always important and compound maladaptive circumventions.

### 4.3 IS Security Response: Individual Outcomes

In line with BAO theory, we observed that insiders' actions, both adaptive and maladaptive, lead to positive and negative individual and organizational outcomes. We categorize organizational outcomes as positive (beneficial to organizational security) or negative (harmful to organizational security). Novel to our study, we also uncovered a key individual outcome we refer to as “lived IS security experience” (see Figure A4 in Appendix A for the data structure and supporting examples). We found that one's lived IS security experience can be favorable or unfavorable. Favorable lived IS security experiences include factors such as (1) flexibility, (2) sense of security and privacy, (3) positive emotions (e.g., happiness), and (4) enhanced productivity. On the other hand, unfavorable lived IS security experiences typically involve forms of productivity hindrance. Examples of such

unfavorable lived IS security experience are (1) limitations on software choices (e.g., substitution of a superior product with an inferior one, the denial of the use of a system), (2) Information constraints (e.g., limitations on decision making), (3) time inefficiencies (e.g., loss of productive time), and (4) software-defined business decisions (e.g., errors in data integrity from manual processes, loss of business intelligence).

We uncovered a straightforward relationship between insiders' responses to IS security measures and organizational security: maladaptive responses introduced opportunities for security vulnerabilities, while adaptive responses helped to reduce organizational vulnerabilities. This makes sense because security measures are usually created by individuals with specific expertise to help protect the firm from its security threats. However, considering the lived IS security experience in concert with the type of response—adaptive or maladaptive—provides a deeper insight into the relationship between response and outcome as depicted in Figure 3 and explained thereafter.

#### 4.3.1 Unfavorable Maladaptive Experiences

The first quadrant reflects insiders that exhibit a maladaptive response and have an unfavorable experience. While it is possible to have an unfavorable maladaptive experience because the maladaptive response itself leads to an unfavorable outcome (e.g., a breach of security), an unfavorable maladaptive response usually occurs when IS security blocks an insider's maladaptive behavior, creating a negative experience for the insider. Unfortunately, that type of negative lived IS security experience tends to foster or reinforce negative beliefs about IS security.

As an example, one respondent described an unfavorable experience resulting from employees' attempts to integrate unapproved tools. When the integration was denied, these employees became “annoyed and frustrated” with the IS security team. Another respondent explained how they often “butt up against” the IS security team when trying to incorporate advanced systems to do their work. This insider noted how when objectives are not aligned between the IS security team and the functional units they support, an unfavorable experience results. One respondent went so far as to claim that he would not notify PHEI if he lost his laptop. The respondent noted that the remote wiping and encryption capabilities, which are meant to “protect” the organization, would result in his “whole hard disk” being deleted. This perception can lead to an unfavorable maladaptive experience whereby the insider would choose not to report a lost device and would forego the institutional support needed to help get back to work. Meanwhile, the organization is also worse off because it cannot leverage the very security technologies in question.

Observed Response	Maladaptive	<b>I. Unfavorable Maladaptive Experience</b> <b>Explanation:</b> Insider exhibits maladaptive response and has an unfavorable experience, thus fostering/reinforcing negative beliefs about IS security. <b>Example:</b> Insider has their behavior blocked by IS security and has their productivity hindered. <b>Illustrative Quote:</b> <i>They just can't have that... I think they were annoyed and frustrated with that, but ultimately, I guess they went on and did their thing anyway...</i>	<b>II. Favorable Maladaptive Experience</b> <b>Explanation:</b> Insider exhibits maladaptive response and has a favorable experience, thus fostering/reinforcing negative beliefs about IS security. <b>Example:</b> Insider circumvents IS security and successfully completes their task. <b>Illustrative Quote:</b> <i>I share what I want to share on Box with anybody I want, and nobody seems to care...</i>
	Adaptive	<b>III. Unfavorable Adaptive Experience</b> <b>Explanation:</b> Insider exhibits adaptive response and has an unfavorable experience, thus reinforcing negative beliefs about IS security. <b>Example:</b> Insider adopts IS security measure, and it hinders their productivity. <b>Illustrative Quote:</b> <i>We ended up with what I personally feel is a second-best product because the first-best couldn't meet that particular security concern.</i>	<b>IV. Favorable Adaptive Experience</b> <b>Explanation:</b> Insider exhibits adaptive response and has a favorable experience, thus reinforcing positive beliefs about IS security. <b>Example:</b> Insider adopts IS security measure and feels pride at protecting the organization. <b>Illustrative Quote:</b> <i>...when it comes to things like this... We keep our information more secure than the government does, and I'm happy with that.</i>

Unfavorable                      Favorable

**Individual Security Lived Experiences**

**Figure 3. Insider Response: Lived IS Experience Framework**

#### 4.3.2 Favorable Maladaptive Experiences

The second quadrant describes a favorable experience resulting from a maladaptive response. Most often, we found that this occurs when insiders circumvent or otherwise undermine an IS security measure and find that doing so makes their job easier. Interestingly, we observed favorable maladaptive experiences among insiders from only one belief profile: IS security overindulgence. The positive feedback (favorable experience) on a negative organizational behavior (maladaptive response) confirms their already cynical suspicions about IS security, creating a reinforcing cycle whereby individuals matching the IS security overindulgence profile exhibit a maladaptive response and find the result favorable. The most expressed maladaptive response with a favorable outcome concerned the various circumventions of the password policies where insiders experienced no negative personal consequences from violating the password policies. Other favorable maladaptive experiences concerned the use of prohibited software or the continued use of software that was no longer compliant with security protocols. For example, an employee described continuing to use a software package that did not meet the current security standards of the organization but was instrumental in getting her work done:

*I try to stay under the radar with this program we use so they don't come after me, since it was implemented with PHEI's*

*support, but implemented before some of these extra security layers have been added.*  
(R30 – Disconnect)

While the behavior is maladaptive, the experience for the insider remains favorable, since the employee continues to benefit from the use of the system, hence reinforcing the maladaptive behavior.

#### 4.3.3 Unfavorable Adaptive Experiences

The third quadrant of the insider response—the lived IS security experience framework—describes the outcome observed when an insider exhibits an adaptive response that results in an unfavorable lived experience. Most often, we found that this occurs when insiders follow a new security measure that, in their assessment, hinders their productivity or performance. We found that insiders fitting the IS security disconnect and IS security indulgence profiles demonstrated this outcome. The following two quotes illustrate insiders who complied with an IS security measure and found it to be too cumbersome, leading to an unfavorable lived experience.

*I haven't used it since there's a double authentication. I don't want to use it any more than what I have to. I'd use it more if it was easier for me.* (R26 – Indulge)

*I used to be the one who could explain to everybody how to do it at home. Now I don't even know how. I don't think anyone in our office uses that to answer questions at home*

... It just got that much more complicated to do. (R29 – Indulge)

In the end, these two employees decided to avoid using the system, a maladaptive response. In this way, an unfavorable adaptive lived experiences may trigger or reinforce negative beliefs about IS security, leading to subsequent maladaptive responses.

#### 4.3.4 Favorable Adaptive Experiences

The fourth quadrant of the insider response—the lived IS security experience framework describes the outcome observed when an insider exhibits an adaptive response that results in a favorable lived experience. We found that insiders fitting the IS knows best profile typically demonstrated this lived IS security experience. From the organization’s perspective, this is the ideal response because it works to create and/or reinforce positive beliefs about IS security. Some insiders reacted positively about the decision to move toward two-factor authentication for all systems, seeing it as “a good move to strengthen security without adding a whole lot of burden to people.” In this case, the employee’s favorable experience stems from the fact that the IS security measures make the organization safer from security threats. Some appreciated the laptop encryption policy, noting that they “don’t have to worry” about their laptop being “lost or stolen.” And in another case, an employee expressed a favorable experience with the security review process for new databases, feeling comfortable using a new database with the assurance that it has been through a rigorous “review process before we subscribe to them.”

Another respondent in the IT workforce experienced enhanced productivity. The software support specialist got “the ability to meet with that patch management group, and it’s a lot easier to deploy out patches with the more policies that we add” because with increased awareness “people see the significance of needing to get their devices updated and patched.” Finally, one professional user experienced an enhanced work environment because of the single sign-on VPN system. He stated that the institution is providing a “fairly high level of security but also making it fairly user friendly.” So, via the VPN, he has “all these multiple entry points into a variety of different software tools or places where you can go and do the things you need to do, but it’s through a unitary log-in ID and password, so that’s kind of nice. So, I’m accessing everything from very simple email to, you know, I access financial data, personnel data, so a variety of different kinds of data and *it always is very easy for me.*”

#### 4.4 IS Security Response: Organizational Outcomes

In addition to individual outcomes from IS security responses, there are both positive and negative

organizational outcomes. The positive organizational outcome—enhanced organizational IS security—occurs when insiders exhibit adaptive responses to IS security. This is not surprising given that IS security measures are developed expressly to help improve organizational security. However, even adaptive behaviors can lead to a negative organizational security outcome—increased security risk—over time as insiders exhibiting adaptive behaviors experience unfavorable outcomes and subsequently engage in maladaptive behaviors. Indeed, a vicious cycle may ensue when the IS security team realizes that maladaptive actions such as avoidance and circumvention are putting systems at risk and establishes new security measures to counteract the risk. When these new measures foster or reinforce negative beliefs about IS security, new maladaptive responses may emerge. Thus, a nonvirtuous cycle—or an “adversarial dance” as one respondent described it—is established whereby maladaptive responses lead to new security measures that reinforce negative beliefs and elicit maladaptive responses. This was observable in the continuing problems related to passwords—with users finding ways to circumvent the policies and the IT security team responding with stricter measures—as well as in the decisions by insiders to use prohibited systems to avert the VPN, such as when insiders collaborated via Dropbox instead of PHEI’s securely maintained content management system but in so doing increased the security risk to PHEI. The move to the VPN itself was a response to the maladaptive behavior of insiders who, despite security awareness campaigns, continued to click phishing links. In the words of an IT executive:

*So, you’ve seen them, I’m sure. “Your PHEI webmail account is about to expire. Please click on this link and give us your username, password, and social security number.” I’ve had them so crazy; you click the link; they’ve set up a pharming website with our logo that looks legit. You sign in via the phishing site in China and then they log in our servers, and you never know. If you need to go somewhere, open a web browser and type where you need to go. But since they continue [clicking on phishing links], enforcing double authentication is the way to go. (Respondent 21)*

However, as explained earlier, the implementation of dual authentication on the VPN led to maladaptive responses for some insiders, reverting to less secure alternatives such as saving files to insecure mediums rather than accessing the security systems directly via the VPN, hence continuing the adversarial dance. Taken together, our findings suggest that outcomes—both individual and organizational—influence beliefs even as they are influenced by them through actions. We depict this in a general IS Security BAO model (Figure 4).

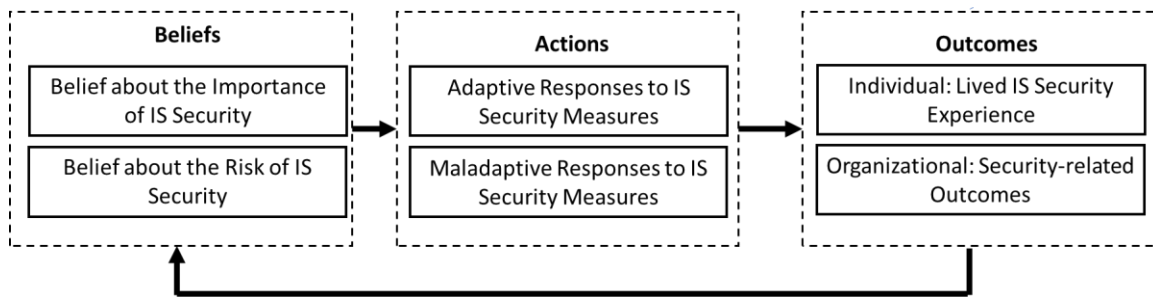


Figure 4. BAO Model of IS Security

#### 4.5 Additional Data Collections and Analyses for Generalizability

To help ensure generalizability and further enhance the validity of our findings, we conducted two additional rounds of data collection (one qualitative and one quantitative) from different industries outside the educational sector. First, we interviewed a total of seven managers, including four from the finance/banking sector (a financial exchange stock market agent, a financial manager from a wholesaler, a senior business development manager from Western Union, and a deputy head of the collection unit in a big bank), one from the medical industry (an ENT doctor working in a large medical center), one from the technology sector (a project manager in an IT company), and one from consumer goods (a senior digital merchandiser for a multinational company). These managers were randomly sampled from a pool of 32 professionals enrolled in an executive MBA program and were interviewed during the Spring of 2021. Importantly, we found that the four previously discovered profiles (with their beliefs and actions) were also supported in this pool of seven managers. Appendix B details the results of this additional round of data.

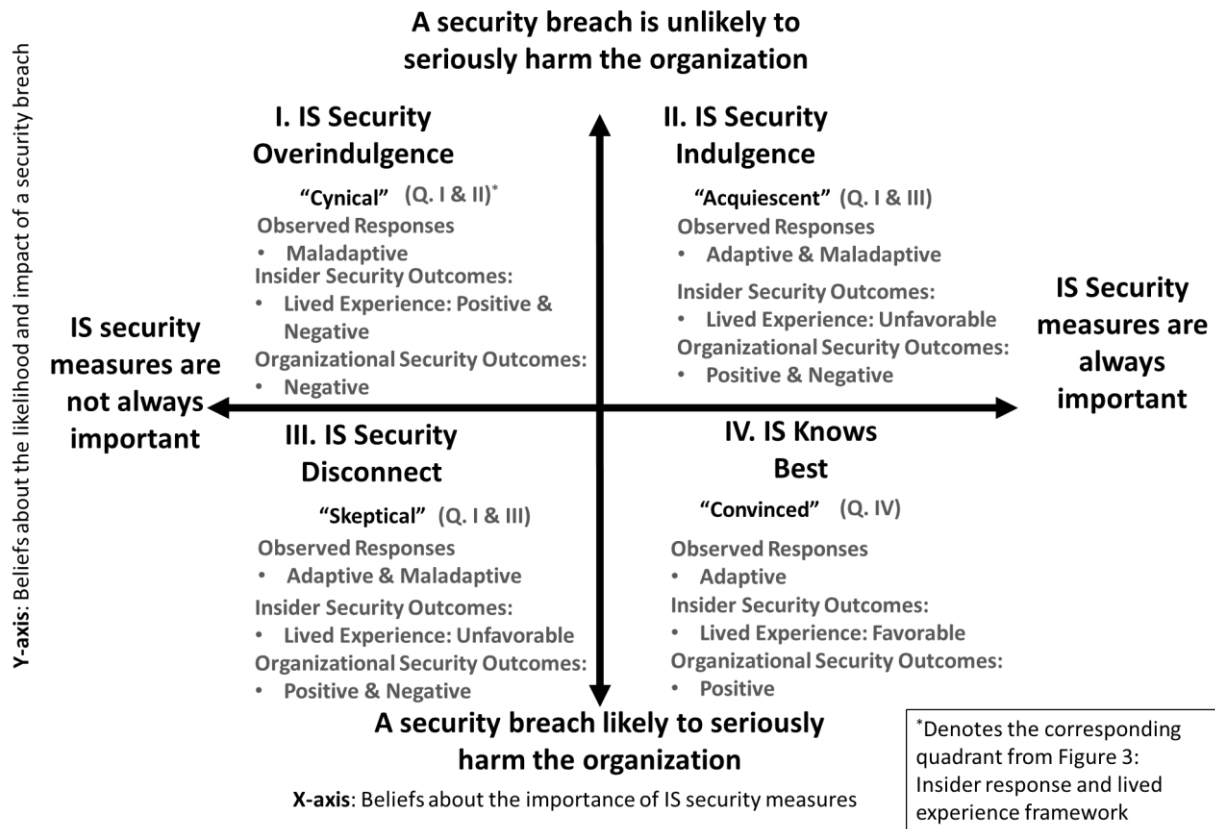
Next, we surveyed 120 individuals working full-time across a variety of industries to ascertain their security-related beliefs, actions, and organizational outcomes. Again, in support of our prior findings, we found evidence of each of the four profiles in our sample. Respondents in each of these profiles represent different industries such as healthcare, manufacturing, retail, and finance, among others. In addition to forced-choice responses, we also allowed our survey participants to provide open-ended responses to better understand their beliefs and subsequent actions and outcomes. For example, we asked respondents who were classified as belonging to the IS security disconnect or IS security overindulgence profiles to explain why they ignored or evaded a security measure at work, which elicited a familiar response: “to get the job done.” We also asked individuals classified as belonging to the IS security indulgence profile to explain a system they avoided at work. A sample response was “I didn’t use the company’s Wi-Fi on my personal phone.” Finally,

we asked respondents from the IS knows best profile to explain why they do or do not comply with all the security measures at work. As expected, this was the largest group and displayed a variety of reasons for compliance, including “because I do not want to compromise my company” and “I don’t want to lose my job.” Appendix C provides more details regarding our supplemental quantitative analyses, including sample demographic details and a discussion of our findings.

### 5 Theoretical Integration and Contributions to Research

Figure 5 synthesizes our findings, integrating the two major beliefs, four belief profiles, three responses, and the individual and organizational outcomes. We found that the belief profiles helped explain both adaptive and maladaptive responses (actions), which led to favorable and unfavorable experiences and organizational outcomes that were both positive and negative for information security. In addition, we found that individual outcomes can be explained by a novel insider response and lived IS security experience framework that lays the foundation for an adversarial dance with the organization’s IS security.

Some existing IS security research resonates with and complements our uncovered beliefs about IS security and the security belief framework, although our contributions depart from the prior security work in several key areas. The literature on policy compliance (e.g., Bulgurcu et al., 2010; Chen et al., 2012; D’Arcy & Lowry, 2019; Herath & Rao, 2009; Johnston et al., 2015; Vance et al., 2013) provides ample evidence that organizationally maladaptive security behaviors increase security risk (Marett et al., 2019). This extensive body of policy compliance work draws upon rational choice theory (e.g., Bulgurcu et al., 2010), neutralization theory (e.g., Siponen & Vance, 2010), reactance theory (e.g., Lowry & Moody, 2015), and organizational justice theory (e.g., Li et al., 2014). While we found specific integration points between our findings and prior works based on these extant theories, we also found specific theoretical linkages that were absent in the prior works.



**Figure 5. Novel Belief Framework with Associated Actions and Outcomes**

Table 5 summarizes our integration with several key theories used in prior IS security studies. To help integrate our findings, we show key departures and complementary findings between our research and these prior works.

Building on the prior security research, we uncovered specific costs that insiders attribute to security measures. For example, they often find that security measures inhibit productivity. However, unlike prior research (Bulgurcu et al., 2010), we were able to ascertain these productivity hindrances. Specifically, we uncovered several distinct types of productivity hindrances: (1) limitations on software choices, (2) time inefficiencies, (3) information constraints, and (4) software-defined business decisions. We are among the first to detail these discrete forms of productivity hindrances that can be associated with security measures. This is important because, as we found, such unfavorable lived IS security experiences may foster or reinforce negative beliefs about IS security.

While we are not the first to uncover beliefs that relate to maladaptive actions, we are among the first to uncover a cogent belief framework by studying the actual beliefs, actions, and outcomes in an organization. Prior research has found that related beliefs and actions such as apathy (Boss et al., 2009), psychological distancing (Burns et al., 2019), and

security awareness (Bulgurcu et al., 2010) impact insiders' security-related behaviors, but none of this research has explained how these fit within a framework or relate to each other. Our research extracts beliefs directly from the reactions of employees and integrates them into belief profiles that explain employee security behaviors. With this knowledge, researchers can now study how beliefs (and their associated belief profiles) relate to maladaptive IS security responses and the resulting lived experiences of employees. This new understanding should allow us to find new theoretically sound ways to improve insiders' lived experience with IS security and reduce the potentially nonvirtuous cycle, or adversarial dance, of IS security.

Finally, significant research has examined the influence of organizational communication on information security behaviors, primarily in terms of threat communications and fear appeals (e.g., Boss et al., 2015; Johnston & Warkentin, 2010; Johnston et al., 2019b; Marett et al., 2019). However, relatively few studies have focused on organizations' use of communication to justify security measures. This is a crucial point because we found that maladaptive responses can arise when security measures inhibit productivity.

**Table 5. Theoretical Integration**

Theory	Example study	Example of theoretical findings	Integration with our findings	Contributions of our work
Rational choice theory (RCT)	Bulgurcu et al. (2010)	Found that employees often engage in a cost-benefit analysis among available behavioral options when forming policy compliance intentions.	Like the cost-benefit analyses in the prior work, we found that employees make personally rational decisions when choosing both organizationally adaptive and maladaptive responses to IS security.	Beyond RCT, we uncover a belief framework that shows how specific beliefs about IS security relate to four distinct profiles, each with its own actions and potential outcomes. Further, we show specific forms of maladaptive behaviors. Finally, we exhibit the potential for a nonvirtuous cycle of IS security.
Neutralization theory	Siponen & Vance (2010)	Found that employees engage in various neutralization techniques (e.g., appeals to higher loyalties, denial of injury) to justify policy violations.	Like the neutralizations in the prior study, we found that employees provided justifications for both adaptive and maladaptive responses to IS security measures.	Beyond neutralizations, we uncover an emergent belief framework of insider security belief profiles. As we show, these profiles each have their own associated actions and outcomes that are distinct from those explained as neutralizations. This profile framework expands on the theoretical linkage between beliefs, actions, and outcomes in IS security beyond what is explained by neutralization theory. Finally, we provide an extended BAO theory of IS security that explains the potential of a nonvirtuous cycle of IS security.
Reactance theory	Lowry & Moody (2015)	Found that threats to freedom from policies negatively relate to compliance intentions through employees' reactance.	Like the threats to freedom and reactance in the prior study, we found that productivity hindrance corresponds to specific responses to IS security measures.	Beyond reactance, we found an IS security belief framework that describes four insider profiles. Additionally, we explain how insiders' lived experiences are both an outcome of actions and an antecedent to beliefs. Thus, our extended BAO theory exhibits the potential for a nonvirtuous cycle of IS security that goes beyond the threats to freedom explored in the prior work.
Organizational justice	Li et al. (2014)	Found that organizational justice positively relates to Internet use policy compliance intention.	Like informational justice, beliefs about whether a security measure is justified can be influenced by organizational communication.	Beyond informational justice, many of our respondents challenged the necessity of security measures. These beliefs are not based on the perception that insiders do not know enough about the reasons for the measures, but that they believe the measures are not reasonable given the objective they serve. Finally, the security belief framework, the role of lived IS security experience, and the potential nonvirtuous cycle of IS security are not evident in this prior work.

Future research should seek to integrate our findings with those on organizational communication to better understand how organizations can better justify necessary security measures to insiders. This could help organizations reduce maladaptive responses to IS security and avoid the potential of its nonvirtuous cycle. Additionally, we found that insiders' responses to IS security varied based on two dimensions (the importance of the security measure to the individual and the risk of security breaches to the organization). Therefore, our IS security belief-response framework provides fertile ground for future researchers to

investigate how these beliefs form and how they can be influenced in an organization. Such research could help organizations discover how to elicit more "IS knows best" responses and reduce maladaptive behaviors.

In addition to these theoretical contributions, our findings also have significant managerial implications for organizations looking to increase their security. First, we challenge a dominant view in organizational security that more security measures are associated with more security. While researchers have made this

case in the past (Lowry & Moody, 2015; Lowry et al., 2015; Posey et al., 2011a), our findings show how a nonvirtuous cycle can emerge in response to IS security. Armed with these insights, organizations can work to change beliefs among insiders that are associated with maladaptive responses to security measures. And when employing a security measure that is likely to foster an unfavorable lived experience, organizations can reevaluate the needs of the employees while also prioritizing their justification efforts. Complementing research that clarifies ways to communicate more effectively to employees (Johnston et al., 2019b) and research on how often to communicate (Anderson et al., 2016), our findings encourage organizations to recognize and justify, rather than downplay, the productivity hindrances incurred from security measures and to be open to creative problem solving that will reduce the burden on employees.

Second, by uncovering important security-related beliefs and showing their linkages, our research can help organizations reduce security vulnerabilities by managing these troubling beliefs. Except for the IS knows best profile, each quadrant in the belief-response framework was associated with maladaptive actions. Thus, our research provides insights into the troubling beliefs that can lead to maladaptive responses to security measures. Organizations may find that there are key organizational constituencies that need greater consideration when implementing security measures. For example, we found that many, but not all, IT workers had “IS knows best” responses, while others, such as those working in other highly productive areas of the university, were more likely to have responses associated with maladaptive actions. As organizations continue to struggle to allocate resources effectively to mitigate security risks, these findings can organizations acquire much-needed efficiencies and greater effectiveness.

## 6 Limitations

There are trade-offs with every research method and analytical choice, and each has its own benefits and limitations. Thus, our qualitative approach has certain benefits and drawbacks. First, we employed a case study in a single organization. Although this is a widely accepted practice (Sarker et al., 2013), a mention of the study’s generalizability is warranted. As noted by Lee and Baskerville (2003), there are (at least) four categories of generalization. The type of generalization most applicable to a case-based study is generalizing from description to theory, which entails generalizing from “observations or other descriptions to theory” (Lee & Baskerville, 2003, p. 236). As with other case study methods, our goal was not to develop

a study with statistical generalizability but rather “to discover patterns for the purpose of theory building and to gain a better understanding of the main issues in this context” (Parks et al., 2017, p. 53). We agree with Orlikowski (1993) that our findings, integrated with the previous IS security research, conducted in a variety of settings and employing a variety of methods, will help generate a more general substantive theory. Thus, the emergent IS security belief framework needs continued future research and theoretical integration to become an established part of the formalized body of IS security theory. However, as discussed in the previous section, we found strong initial evidence of theoretical integration with several existing theories (see Table 5).

Second, another potential boundary or limitation to our study that future research could address is the fact that our results are all drawn from the education sector. That said, we believe that the education sector is an important and relevant sector for our study of information security. As noted previously, 58% of higher education institutions indicated they had experienced at least one public data breach in 2018, and over half indicated these attacks cost the institution over \$500,000 (Cisco, 2018). Additionally, like data in other regulated industries (e.g., financial, retail), federal law protects certain student data. Therefore, we believe PHEI is a relevant and credible institution in which to study information security. To help validate our findings across industries, we collected additional qualitative and quantitative data that affirms our theoretical premises (see Appendices B and C).

## 7 Conclusion

Previous researchers have employed a number of methods and theories to help explain insiders’ security-related behaviors. However, few have employed qualitative methods to understand adaptive and maladaptive responses to organizational security measures, an established issue in the literature. Drawing on Melville’s (2010) BAO model, we conducted a case study at a large private university in the southwestern United States. Based on our analyses, we uncovered two key categories of belief: (1) beliefs about the importance of IS security measures and (2) beliefs about the likelihood and impact (i.e., the risk) of security breaches.

Our analyses also revealed an IS security belief framework. We found that each profile in the framework is associated with adaptive and maladaptive actions. Rather than contradicting most related IS security theories, we found that the beliefs about IS security and the belief framework integrate well with the extant literature while providing

significant contributions to several key theories (see Table 5). Most notably, we found that IS security has the potential to create a nonvirtuous cycle (i.e., an “adversarial dance”) whereby IS security measures lead to adaptive and maladaptive actions that foster favorable and unfavorable lived experiences. Unfavorable lived experiences often elicit new or reinforce existing negative IS security beliefs, which can lead to maladaptive behaviors. Maladaptive behaviors such as circumvention and avoidance often introduce new security risks. Thus, to counter the new risks, organizations may employ additional security measures that lead to more maladaptive responses, and so on. Thus, an “adversarial dance” ensues.

While we are not the first to suggest that security measures can elicit maladaptive behaviors, the key construct of beliefs about IS security and the emergent belief framework constitutes an important contribution to the behavioral IS security literature. Our results do not in any way challenge the need for security measures but suggest that some security measures can have adverse effects that need to be addressed. We

contend that our extended BAO model of IS security provides a novel explanation of these opportunities for maladaptive responses in terms of our emergent belief framework.

## **Acknowledgments**

We thank the acting senior editor, Dr. John D’Arcy, and the anonymous reviewers for their guidance and constructive comments. We are also grateful to the reviewers and the participants of ICIS 2016 and HICSS 2017 for their valuable feedback on earlier papers using this dataset. Lastly, this paper was submitted prior to Dorothy Leidner beginning her term as editor-in-chief of JAIS. Nevertheless, to maintain the integrity of the review process, the acting senior editor performed a double-blinded senior editorial role (e.g., the senior editor did not know of our identities nor did we of his until the paper’s acceptance). We wish to thank Dr. Paul Lowry for serving as the intermediating senior editor in order to maintain the double-blinding between the authors and the acting senior editor.

## References

- Anderson, B., Vance, A., Kirwan, C. B., Jenkins, J. L., & Eargle, D. (2016). From warning to wallpaper: Why the brain habituates to security warnings and what can be done about it. *Journal of Management Information Systems*, 33(3), 713-743.
- Balozian, P. & Leidner, D. (2016). Is security menace: When security creates insecurity. *Proceedings of the International Conference on Information Systems*.
- Balozian, P., Leidner, D., & Warkentin, M. (2019). Managers' and employees' differing responses to security approaches. *Journal of Computer Information Systems*, 59(3), 197-210.
- Barrett, M., Oborn, E., Orlikowski, W. J., & Yates, J. (2012). Reconfiguring boundary relations: Robotic innovations in pharmacy work. *Organization Science*, 23(5), 1448-1466.
- Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*, 39(4), 837-864.
- Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. *European Journal of Information Systems*, 18(2), 151-164.
- Brooks, C. (2022). Cybersecurity in 2022: A fresh look at some very alarming stats. *Forbes*. <https://www.forbes.com/sites/chuckbrooks/2022/01/21/cybersecurity-in-2022-a-fresh-look-at-some-very-alarming-stats>
- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(4), 523-548.
- Burns, A. J., Roberts, T. L., Posey, C., Bennett, R. J., & Courtney, J. F. (2018). Intentions to comply versus intentions to protect: A vie theory approach to understanding the influence of insiders' awareness of organizational seta efforts. *Decision Sciences*, 49(6), 1187-1228.
- Burns, A. J., Roberts, T. L., Posey, C., & Lowry, P. B. (2019). The adaptive roles of positive and negative emotions in organizational insiders' security-based precaution taking. *Information Systems Research*, 30(4), 1228-1247.
- Canadian Press, T. (2018). Edmonton's Macewan university recovers more than \$10 million lost to phishing attack. *Toronto Star*. <https://www.thestar.com/news/canada/2018/04/04/edmontons-macewan-university-recovers-more-than-10-million-lost-to-phishing-attack.html>
- Chen, Y., Ramamurthy, K., & Wen, K.-W. (2012). Organizations' information security policy compliance: Stick or carrot approach? *Journal of Management Information Systems*, 29(3), 157-188.
- Chen, Y. & Zahedi, F. M. (2016). Individual's internet security perceptions and behaviors: Polycontextual contrasts between the United States and China. *MIS Quarterly*, 40(1), 205-222.
- Choi, T. Y., Dooley, K. J., & Rungtusanatham, M. (2001). Supply networks and complex adaptive systems: Control versus emergence. *Journal of Operations Management*, 19(3), 351-366.
- Cisco. (2011). *Cisco connected world technology report*. <https://www.cisco.com/c/dam/en/us/solutions/enterprise/connected-world-technology-report/2011-CCWTR-Chapter-3-All-Finding.pdf>
- Cisco. (2018). *Annual cybersecurity report: Impacts on the public sector*. <https://www.cisco.com/education/new-cybersecurity-report-how-to-stay-ahead-of-the-latest-cyber-threats-in-higher-ed>
- Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, 32, 90-101.
- D'Arcy, J., Herath, T., & Shoss, M. (2014). Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of Management Information Systems*, 31(2), 285-318.
- D'Arcy, J., Hovav, A., & 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.
- D'Arcy, J. & Lowry, P. B. (2019). Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal*, 29(1), 43-69.
- Deci, E. L. & Ryan, R. M. (2000). The "what" and "why" of goal pursuits: Human needs and the

- self-determination of behavior. *Psychological Inquiry*, 11(4), 227-268.
- Dell. (2017). *Dell end-user security survey*. Available at <https://datasecurity.dell.com/wp-content/uploads/2017/09/Dell-End-User-Security-Survey-2017.pdf>.
- Dinev, T. & 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(1), 386-408.
- Fayard, A.-L., Gkeredakis, E., & Levina, N. (2016). Framing innovation opportunities while staying committed to an organizational epistemic stance. *Information Systems Research*, 27(2), 302-323.
- Galluch, P. S. & Thatcher, J. B. (2011). Maladaptive vs. Faithful use of internet applications in the classroom: An empirical examination. *Journal of Information Technology Theory and Application*, 12(1), 5-21.
- Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2013). Seeking qualitative rigor in inductive research: Notes on the gioia methodology. *Organizational research methods*, 16(1), 15-31.
- Gregory, R. W., Kaganer, E., Henfridsson, O., & Ruch, T. J. (2018). IT consumerization and the transformation of IT governance. *MIS Quarterly*, 42(4), 1225-1254.
- Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems*, 28(2), 203-236.
- Gwebu, K. L., Wang, J., & Hu, M. Y. (2020). Information security policy noncompliance: An integrative social influence model. *Information Systems Journal*, 30(2), 220-269.
- Herath, T. & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, 18(2), 106-125.
- Herley, C. (2009). So long, and no thanks for the externalities: The rational rejection of security advice by users. *Proceedings of the 2009 workshop on New security paradigms workshop* (pp. 133-144).
- Hsu, J. S.-C., Shih, S.-P., Hung, Y. W., & Lowry, P. B. (2015). The role of extra-role behaviors and social controls in information security policy effectiveness. *Information Systems Research*, 26(2), 282-300.
- IBM. (2018). 2018 cost of a data breach study: Global overview. <https://www.ibm.com/security/data-breach>
- IBM. (2021). *Cost of a data breach report 2021*. <https://www.ibm.com/security/data-breach>
- Johnston, A. C., Di Gangi, P. M., Howard, J., & Worrell, J. (2019a). It takes a village: Understanding the collective security efficacy of employee groups. *Journal of the Association for Information Systems*, 20(3), 186-212.
- Johnston, A. C. & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, 34(3), 549-566.
- Johnston, A. C., Warkentin, M., Dennis, A. R., & Siponen, M. (2019b). Speak their language: Designing effective messages to improve employees' information security decision making. *Decision Sciences*, 50(2), 245-284.
- Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly*, 39(1), 113-134.
- Karjalainen, M., Sarker, S., & Siponen, M. (2019). Toward a theory of information systems security behaviors of organizational employees: A dialectical process perspective. *Information Systems Research*, 30(2), 687-704.
- Koutsikouri, D., Lindgren, R., Henfridsson, O., & Rudmark, D. (2018). Extending digital infrastructures: A typology of growth tactics. *Journal of the Association for Information Systems*, 19(10), 2.
- Lee, A. S. & Baskerville, R. L. (2003). Generalizing generalizability in information systems research. *Information Systems Research*, 14(3), 221-243.
- Li, H., Sarathy, R., Zhang, J., & 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.
- Liang, H. & 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.
- Lowry, P. B. & Moody, G. D. (2015). Proposing the control-reactance compliance model (CRCM)

- to explain opposing motivations to comply with organisational information security policies. *Information Systems Journal*, 25(5), 433-463.
- Lowry, P. B., Posey, C., Bennett, R. J., & Roberts, T. L. (2015). Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: An empirical study of the influence of counterfactual reasoning and organisational trust. *Information Systems Journal*, 25(3), 193-273.
- Marett, K., Vedadi, A., & Durcikova, A. (2019). A quantitative textual analysis of three types of threat communication and subsequent maladaptive responses. *Computers & Security*, 80, 25-35.
- McKenzie, L. (2021). FBI warns of increased ransomware attacks targeting colleges. *Inside Higher Ed*. <https://www.insidehighered.com/quicktakes/2021/03/18/fbi-warns-increased-ransomware-attacks-targeting-colleges>
- Melville, N. P. (2010). Information systems innovation for environmental sustainability. *MIS Quarterly*, 34(1), 1-21.
- Miller, S. (2018). *2017 U.S. State of cybercrime highlights*. Carnegie Mellon University Software Engineering Institute. <https://insights.sei.cmu.edu/insider-threat/2018/01/2017-us-state-of-cybercrime-highlights.html>
- Montealegre, R., Iyengar, K., & Sweeney, J. (2019). Understanding ambidexterity: Managing contradictory tensions between exploration and exploitation in the evolution of digital infrastructure. *Journal of the Association for Information Systems*, 20(5), 647-680.
- Orlikowski, W. J. (1993). Case tools as organizational change: Investigating incremental and radical changes in systems development. *MIS Quarterly*, 17(3), 309-340.
- Oshri, I., Henfridsson, O., & Kotlarsky, J. (2018). Re-representation as work design in outsourcing: A semiotic view. *MIS Quarterly*, 42(1), 1-23.
- Padayachee, K. (2012). Taxonomy of compliant information security behavior. *Computers & Security*, 31(5), 673-680.
- Parks, R., Xu, H., Chu, C.-H., & Lowry, P. B. (2017). Examining the intended and unintended consequences of organisational privacy safeguards. *European Journal of Information Systems*, 26(1), 37-65.
- Posey, C., Bennett, B., Roberts, T., & Lowry, P. (2011a). When computer monitoring backfires: Invasion of privacy and organizational injustice as precursors to computer abuse. *Journal of Information System Security*, 7(1), 24-47.
- Posey, C., Bennett, R. J., & Roberts, T. L. (2011b). Understanding the mindset of the abusive insider: An examination of insiders' causal reasoning following internal security changes. *Computers & Security*, 30(6), 486-497.
- Post, G. V. & Kagan, A. (2007). Evaluating information security tradeoffs: Restricting access can interfere with user tasks. *Computers & Security*, 26(3), 229-237.
- PWC. (2015). *Managing cyber risks in an interconnected world: Key findings from the global state of information security*. [www.pwc.com/gsis2015](http://www.pwc.com/gsis2015)
- Rippetoe, P. A. & Rogers, R. W. (1987). Effects of components of protection-motivation theory on adaptive and maladaptive coping with a health threat. *Journal of Personality and Social Psychology*, 52(3), 596-604.
- Salovaara, A., Lyytinen, K., & Penttinen, E. (2019). High reliability in digital organizing: Mindlessness, the frame problem, and digital operations. *MIS Quarterly*, 43(2), 555-578.
- Sarker, S., Xiao, X., & Beaulieu, T. (2013). Guest editorial: Qualitative studies in information systems: A critical review and some guiding principles. *MIS Quarterly*, 37(4), iii-xviii.
- Simon, H. A. (1955). A behavioral model of rational choice. *The Quarterly Journal of Economics*, 69(1), 99-118.
- Simon, H. A. (1996). *The sciences of the artificial*. Cambridge, MA: MIT Press.
- Siponen, M. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, 8(1), 31-41.
- Siponen, M. & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly*, 34(3), 487-502.
- Siponen, M. & 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.
- Stanton, J. M. & Stam, K. R. (2006). *The visible employee: Using workplace monitoring and surveillance to protect information assets—without compromising employee privacy or trust*. Information Today.

- Stanton, J. M., Stam, K. R., Mastrangelo, P. M., & Jolton, J. A. (2006). Behavioral information security: An overview, results, and research agenda, In P. Zhang & D. Galletta (Eds.), *Human-computer interaction and management information systems: Foundations* (pp. 262-280). M. E. Sharpe.
- Vance, A., Lowry, P. B., & Eggett, D. (2013). Using accountability to reduce access policy violations in information systems. *Journal of Management Information Systems*, 29(4), 263-289.
- Waldrop, M. M. (1992). *Complexity: The emerging science and the edge of order and chaos*. Simon & Schuster.
- Willison, R. & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly*, 37(1), 1-20.
- Woods, N. & Siponen, M. (2018). Too many passwords? How understanding our memory can increase password memorability. *International Journal of Human-Computer Studies*, 111, 36-48.
- Woods, N. & Siponen, M. (2019). Improving password memorability, while not inconveniencing the user. *International Journal of Human-Computer Studies*, 128, 61-71.
- Yin, R. K. (1989). *Case study research and applications: Design and methods* (2nd ed.). SAGE.

## **Appendix A: Semi-Structured Interview Guide**

Interview Duration:

Job Title (Faculty, non-IT staff, IT staff, student); College (-----); Department (-----)

Introduction to Informant: Hello. Thank you for agreeing to sit with me today and answer a few questions about the security policies here at \_\_\_\_\_. I want to remind you that everything we talk about will remain strictly confidential, and your own personal answers and identity will never be revealed to anyone. Only summarized answers from the entire group will appear in our research articles. Please be honest and complete in your answers, and please let me know if you need any clarification. Finally, remember that you can decline to answer any question, and you can quit at any time. Let's begin ...

### *For IT Team Members*

1. Reflecting upon the last 10 years of computer security policies, what are the things that changed? What are the things that remained the same? How have new security measures affected your own work?
2. How is the IT department able to chase a moving target (ever-changing security threats, therefore ever-changing security policies)? How often are the policies updated?
3. How does IS policy compliance increase IS security effectiveness? What, in your opinion, is IS security effectiveness?
4. How do you know your policy is effective?
5. Can you give me an example of a security policy your users may think is over-the-top but that you feel ITS has to do for reasons other than security—such as maintaining an image of being on top of things, or because everyone else is doing it, etc...;
6. Have you ever faced a situation in which security policies have hindered your own ability to work effectively in your role as (insert job title)? How did you deal with them?
7. Describe what you see as the biggest threat to IT security of the university? How about to individual faculty, staff and students?
8. How do you set policies? How do you communicate these policies?

### *For Employees/Users*

1. How important is computer security in your professional work? How do you handle or manage data that is sensitive or important and might be threatened by loss or theft? Is this more important now than it was five or ten years ago? Why?
2. Describe what you know about your university's IS security policies.
3. How do security policies enable and constrain your work practice? In what ways do IT security policies make you more effective in your role as (faculty, staff, administrator...)? Are there ways that you feel the security policies constrain your work? If so, can you give me an example?...
4. For you personally (not for your unit or department), what are the most important security concerns you have regarding IT (including your desktop, laptop, personal data on the University systems, mobile devices etc.)? In the last 10 years, have you been facing some difficulties in order to comply with security policies? What did you do about them?
5. Why do you think ITS does what it does regarding security policies?
6. Are there specific IT security policies that you feel are intrusive or overly demanding?
7. Are there areas where you feel there should be more security than there currently is?
8. What is your perception of ITS?

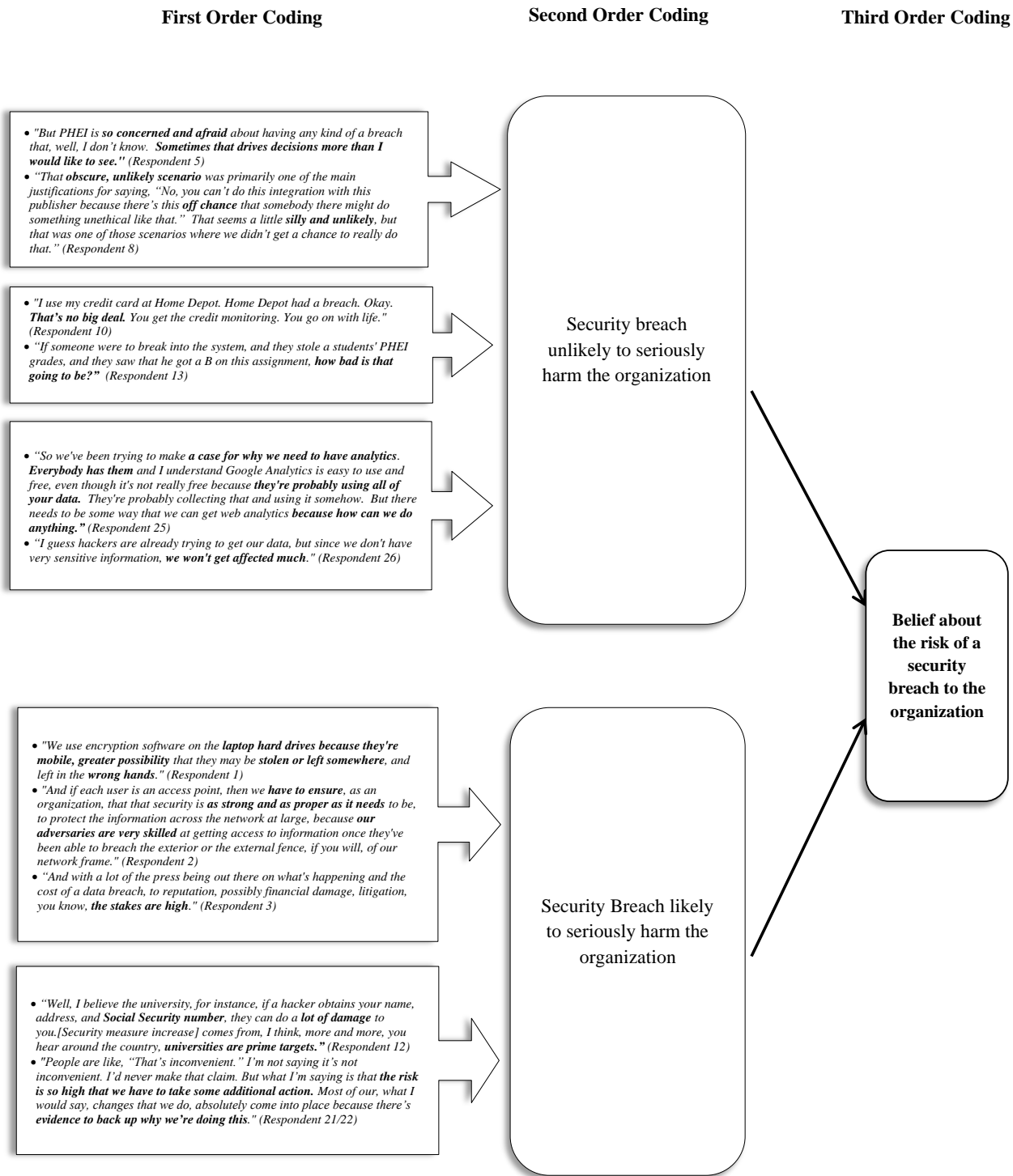


Figure A1. Data Structure for Belief about the Risk of a Security Breach to the Organization

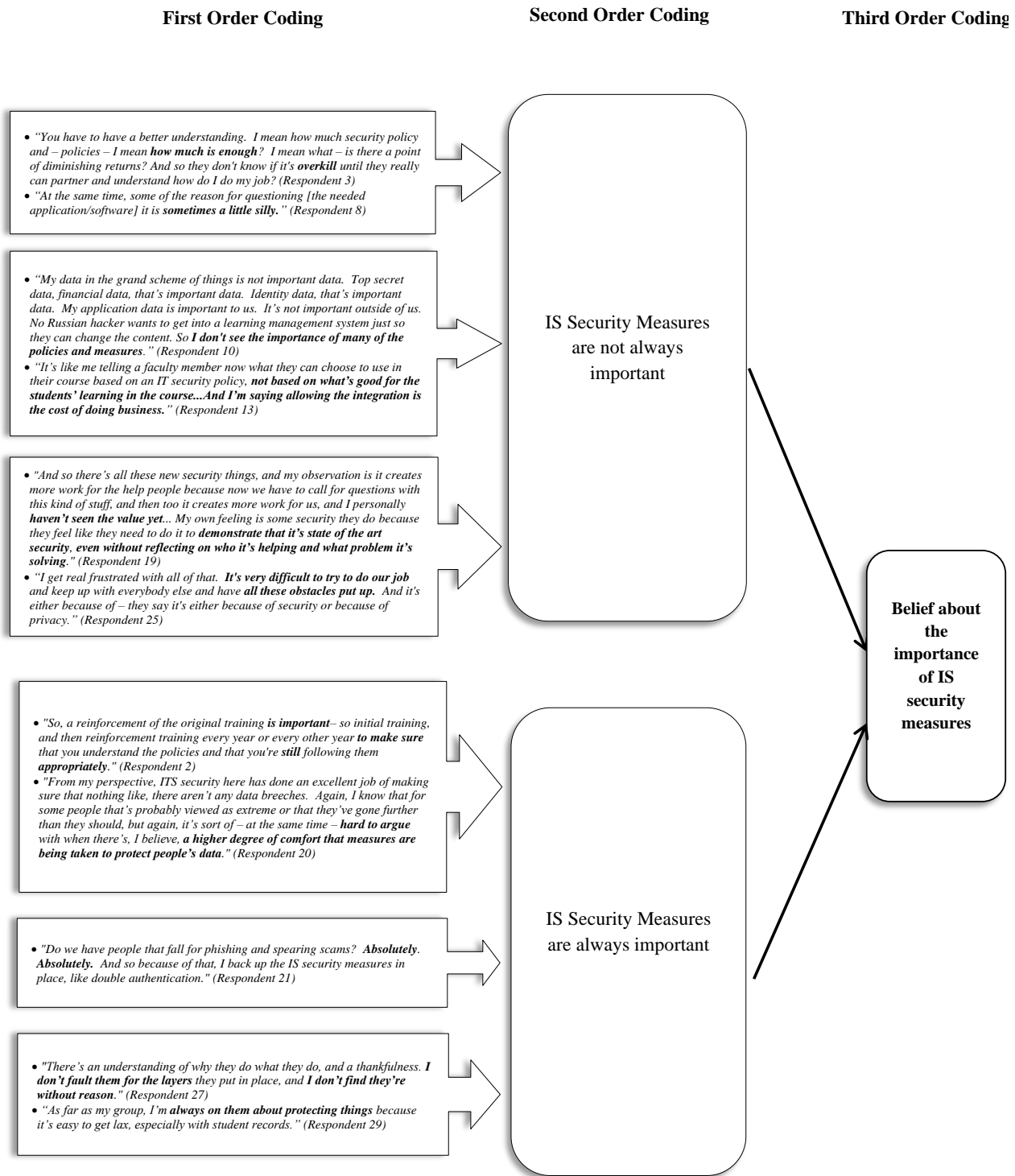


Figure A2. Data Structure for Belief about the Importance of IS Security Measures

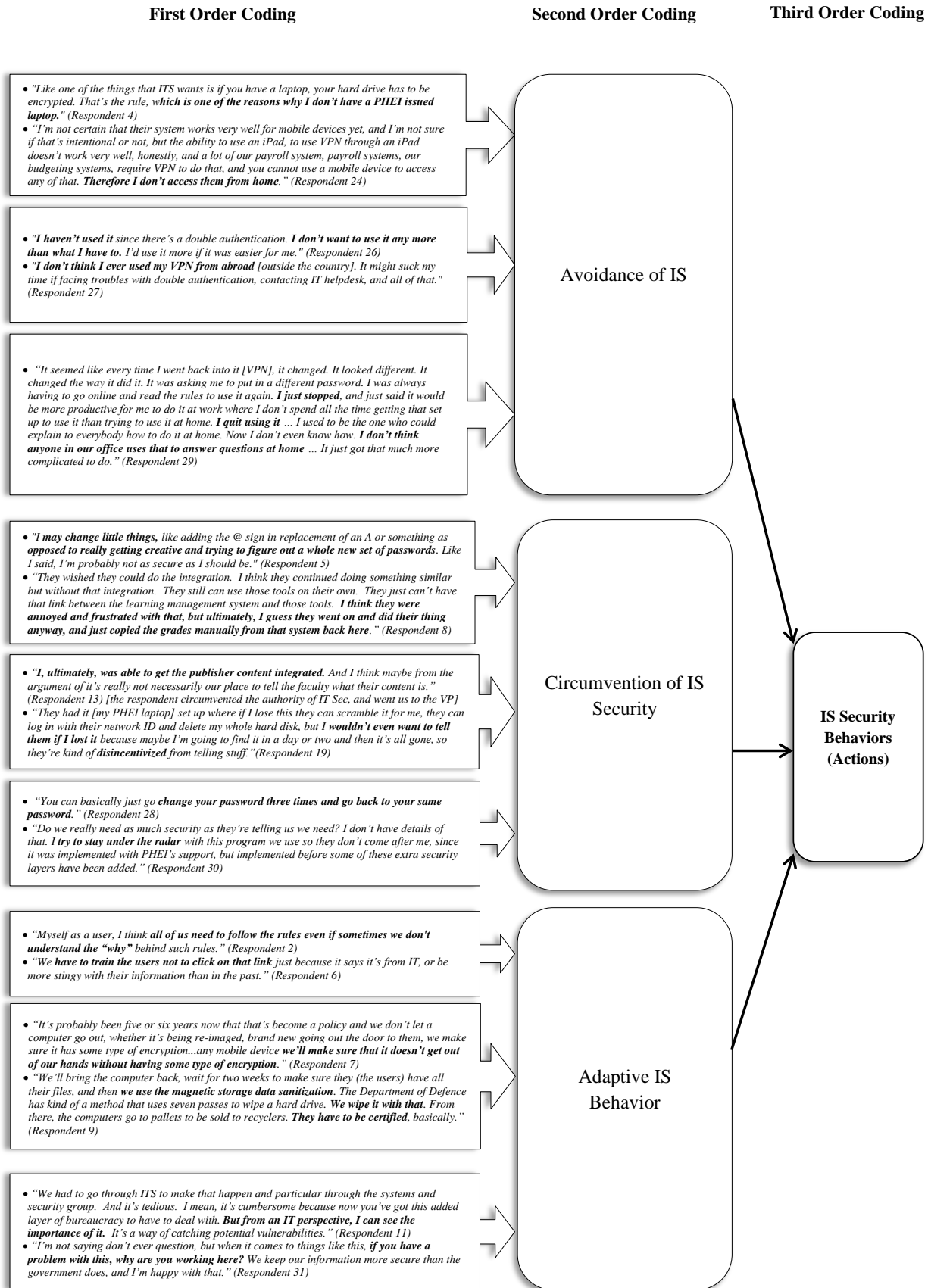


Figure A3: Data Structure for IS Security Behaviors

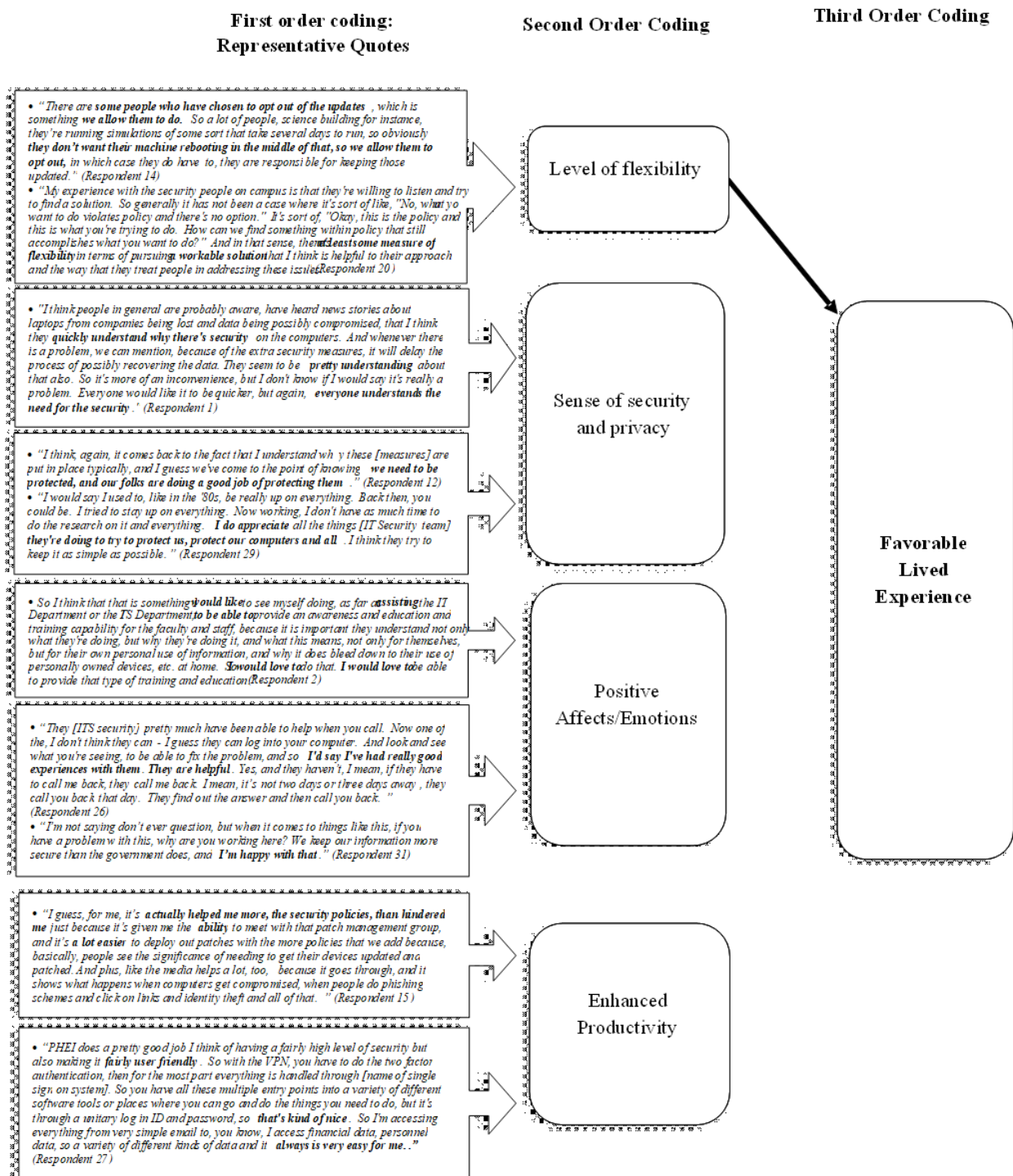


Figure A4. Favorable Lived Experiences

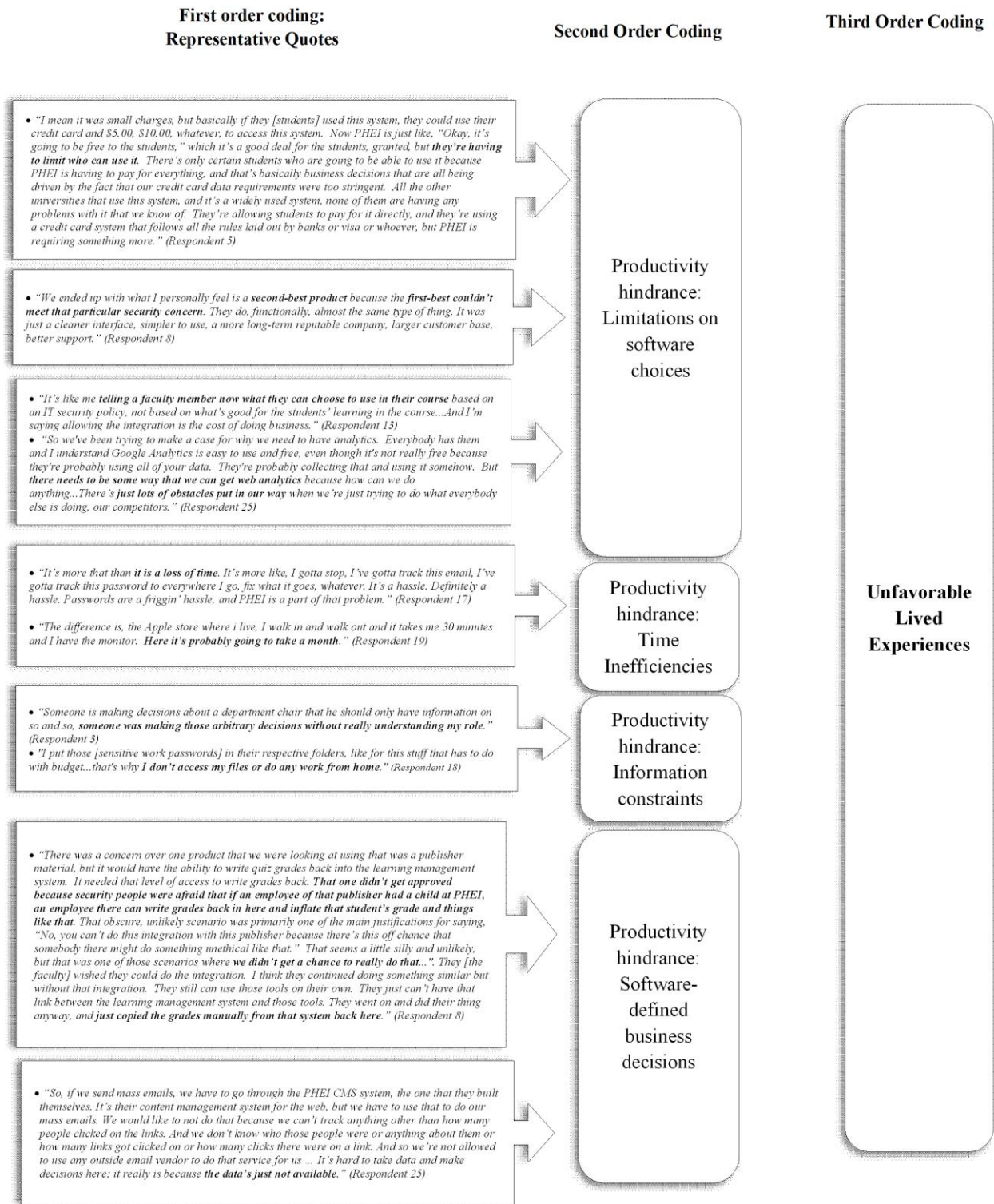


Figure A5. Unfavorable Lived Experiences

## Appendix B: Seven Additional Interviews

To verify that the profiles we extracted are not specific to the educational context only, we conducted an additional set of interviews with managers from different industries including four from the finance/banking sector (a financial exchange stock market agent, a financial manager from a wholesaler, a senior business development manager from Western Union, and a deputy head of the collection unit of a big bank), one from the medical industry (an ENT doctor working in a large medical center), one from the technology sector (a project manager in an IT company) and one from consumer goods (a senior digital merchandiser for a multinational company). These were recruited using random sampling out of a pool of 32 potential respondents (the sample pool consisted of students in an executive MBA course).

Because these interviews served to ascertain whether the belief profiles and responses we had induced from our analysis would hold outside of an educational context, the analysis of the interview transcripts entailed specifically looking for evidence, or lack thereof, of our belief profiles and responses. The tables below provide evidence that even in this small sample of seven, the four profiles and three responses are evident. While we cannot eliminate the possibility that other security profiles and responses exist, we can suggest that the specific profiles and responses emerging from our study have relevance outside the industry context from which the profiles were first observed.

**Table B1. Supplementary Evidence of IS Security Overindulgence**

IS security overindulgence (Quadrant 1)	Beliefs about the risk of security breaches	Security breach unlikely to seriously harm the organization	<i>"So again, in my case, a breach into my account, it's going to give them access to, let's say, one of the brands out of like the 50 that they own ... Specifically [a breach] into my account, I would say it wouldn't be that big of an effect on the organization. ... The reasons behind their focus on certain less important things would be standard measures that are followed generally by companies, wherever they are. So in the sense of maybe giving the IT department a standard purpose, so they just end up following and imposing certain rules that are more generic than oriented for the threats that might be harmful."</i> (Additional Respondent 3)
	Beliefs about the importance of IS	IS Security measures are NOT always important	<i>[When asked about double authentication] "They're actually working on it now. So they're trying to implement it now. I don't see any specific reasons as to why they might go for that ... [Also] I don't understand the point of the VPN if I would be able to access the files from anywhere. So as long as I'm connected to it, I can access it. Then that kind of makes the whole point of setting up a VPN system pointless, so to say ... So there's too much focus on the wrong thing and not enough on what it actually needs to be."</i> (Additional Respondent 3)
	Action	Circumvention	<i>"I think we tend to get lazy with most of them (security measures). They've been sending us emails since the beginning of January concerning the double authentication, which is supposed to happen in March. So I think the company is aware of us being lazy as well. And as I mentioned previously, we often end up just reusing our old passwords. So I would say, often we try to go around the policies that they try to enforce."</i> (Additional Respondent 3)

**Table B2. Supplementary Evidence of IS Security Indulgence**

IS security indulgence (Quadrant 2)	Beliefs about the risk of security breaches	Security breach unlikely to seriously harm the organization	<i>"If my personal account, my personal account was breached, I don't think it would affect my organization because I don't have that [much of important/sensitive] data in my circle of work ... I guess there are other more important data that are found in the organization that if someone gets them, it would be very dangerous. So it depends on the hierarchy, I mean, it depends on the level you are at the organization and the things given to you ... So from my point, I don't have that."</i> (Additional Respondent 1)
	Beliefs about the importance of IS security measures	IS Security measures are always important	<i>"So yeah, I guess that the main purpose is for this thing, it's not, they are there to limit our privacy, but I guess they have there for protecting data from any other outside breach ... So when those measures are there it's not to limit your privacy or to totally limit your privacy. I guess they are there to prevent the company from anything that tries to destroy it or to steal its data."</i> (Additional Respondent 1)
	Action	Avoidance of IS	<i>[Respondent under the pressure of departmental culture avoiding the strict compliance with the policy to the letter] "...when you live together or work together for a long time, some boundaries fall down, as you become more like family or like brother, sister, and you say, "Oh, it's okay, no problem. I give you my password, okay, no problem". So things become more loose if you want, so taking each other's password and accessing each other's work or information. It's not something good, but unfortunately it's something being done because of this so much friendly environment."</i> (Additional Respondent 1)

**Table B3. Supplementary Evidence of IS Knows Best**

<b>IS knows best (Quadrant 3)</b>	<b>Beliefs about the risk of security breaches</b>	Security breach likely to seriously harm the organization	<i>"In fact, whatever the position a certain employee is in an organization, a security breach could affect the organization assets. For sure, this will have a more effect for those who have a direct access to the important data of the company, okay. But let's say for example, a hacker could be establishing a certain breach in a PC, even for a small employee, let's say, let's use this word, who don't have any access to data ... Even through this PC, he could have access to other PCs, since once he have access to the network ... So here we have as a problem of network exposure, risk that could affect other people working on the same network or the same LAN. So the security measures, it should be applied to all the organization employees, whatever the position or even the profile they are working on, they have access to sensitive data or not. And final thought, any breach will cause for sure an impact on the most important assets of the organization." (Additional Respondent 2)</i>
			<i>"A breach into my account would affect the company immensely, because as a CFO, I oversee part of the IT section as well and I house some of the passwords. I don't keep any copies of my passwords on my desktop or on my mobiles, I keep them on a separate hardware documentation separately. But technically, I also have authorities and rights over some of the software of the company, that if any breach happens into my account or into my computer, it might affect the organization immensely." (Additional Respondent 6)</i>
			<i>"[A breach on my work account is] pretty serious, actually, because on my password protected personal computer, I have, first of all, data on the many patients that I see and follow up. Those would be compromised eventually. What would they actually want to do with those is up to them, but that's something very serious of course. At the institution, we also perform a lot of research. Once again, this research, most of it is, we're bound to privacy by the IRB at our institution. Once again, this would be a serious breach and of course would affect the institution is what I'm saying. That's mostly it on my personal computer that would affect my organization. Anything that has to do with my work, which is patients and research. That data is available there, so they would be able to get it." (Additional Respondent 7)</i>
	<b>Beliefs about the importance of IS security measures</b>	IS Security measures are always important	<i>"In fact, everything has a purpose. For applying IT security measures in a software industry is very important. And as an employee, I totally understand is the company's policies and procedures to be applied." (Additional Respondent 2)</i>
			<i>"The IS security measures are done for the safety of the information, and the safety of our computer, and overall information of the company and the company's well-being. So in my perception all the measures are justified." (Additional Respondent 6)</i>
			<i>"Information security measures are always important. Yes, they're always necessary. You can't do without them. I think the more technologically advanced we become, the more necessary those measures and the more sophisticated those measures would have to be." (Additional Respondent 7)</i>
	<b>Action</b>	Adaptive Behavior	<i>"When asked about how does he perceive the breaking of the rule of opting out of the VPN use for a higher goal, he put it as an exception, and opted for taking permission from the IT to go for that exception] But sometimes, as we say, have some exceptions to deal with, especially when we have a critical case affecting the customer and affecting the business. So maybe we could have an approval from our security team or our management to apply this way of having a direct access instead of using VPN access." (Additional Respondent 2)</i>
			<i>"Technically we have the single sign-on, and the majority of our software is databases or information that we use, like we sign into the computer and then we have the access, we sign into our emails with a separate password. And then we have technically three or four passwords, main passwords, and then there is half of the passwords of the IT's that I share with. I don't believe that it takes a lot off my time. It's manageable." (Additional Respondent 6)</i>
			<i>"I think we abide by them at least from my own perspective. We abide by them almost with no doubt, really. We just go with it. The small team I work with, we understand that those measures are here to stay and they're part of the small price that you have to pay to have an electronic system, an electronic patient care system to be able to use the email, systems, or technology. It's the price to pay in order to use those appliances safely. In a way, it comes with it. It's the whole package. You want to use technology, you have to also be safe using it." (Additional Respondent 7)</i>

**Table B4. Supplementary Evidence of IS Security Disconnect**

IS security disconnect (Quadrant 4)	Beliefs about the risk of security breaches	Security breach likely to seriously harm the organization	<p>[This respondent #4 has based his answers on his previous job of 10 years because he only recently began a new position.]</p> <p>“In my case, I can say that it’s quite serious given that for the past 10 to 12 years, I’ve been dealing in a business development field. More or less, I price tenders and I negotiate lots of sensitive deals. If I know that in case somebody succeeded to put his hand on these confidential data, then this might be an issue. Just imagine the fact that you’re pricing a tender for tens of millions of dollars, and a competitor has got the chance to see your pricing strategy. Definitely, you’ll end up losing this tender, which you’ve been working for the past couple of months.” (Additional Respondent 4)</p>
			<p>“A security breach on my account would be very serious, especially because I work with the team that had access to every single account. So if they were to breach, let’s say my computer or any of my coworkers’ computers in my team, then they would have access to every single account ID and password. And we have a lot of clients, and some of these clients have large funds in their accounts. So it would be very detrimental to the firm, to put in short.” (Additional Respondent 5)</p>
	Beliefs about the importance of IS security measures	IS Security measures are NOT always important	<p>“In my job for a PPP company [public-private partnership] there were lots of bureaucracy. The structure was extremely vertical. At the same time, this led to some sort of nonproductivity because we used to report on a solid line to somebody and on a dotted line to somebody else. And of course, we had to take lots of approvals and change lots of passwords. Everything was encrypted and in a secure format. To some extent, this led to some frustration to us and particularly to myself, given that we felt that it is an overkill.” (Additional Respondent 4)</p>
			<p>“I need to open a client account. I can watch the account, but I can’t touch anything in it. The client calls me and tells me there’s a problem with his laptop, he’s not able to do anything through his account. He needs to enter and buy let’s say, some contracts of Euro to dollar, for example. I would need to open his account and personally do it on his behalf after he had sent me the email or a phone call or recorded phone call. But to open his account, I need double authentication. To get this I would need to either contact IT or the manager. And each second, when it comes to such a thing, counts. ... But if something were to happen, let’s say after midnight, the manager would be asleep. Till the manager wakes up, till they get the new code, till they send it to our team, a lot could happen. So sometimes [this security measure or policy] wouldn’t be beneficial. It would have been the same as if they had left it with IT with this understanding, we came to the conclusion that how about in our specific team where we need this information [double authentication pin], every member on their shift will have access to this [system generating the pin].” (Additional Respondent 5)</p>
	Action	Circumvention	<p>“We were not allowed to send, let’s say, attachments to external computers. All the attachments that we have, all the files that we have, they should remain as a property of the company. We were not allowed to put them on USB in order to save them on a personal file. In that case, I know that I breached this when I was going from one company to another. The fact that I was working on this file, and I contributed directly to all of these, let’s say, financial models, presentations, et cetera. I thought back then that, you know what, it’s not fair to keep all of these files to them and not keep a copy for myself on my external hard disk given that I’m leaving the company. I remember that I transferred these files to my external hard disk and IT knew that I did that. We had a fact conversation and I need to do some sanitization with the data to make sure that I’m protecting all the clients of my previous employers, especially that there were nondisclosure agreements and clauses that we were not supposed to breach.” (Additional Respondent 4)</p>
			<p>[This stock exchange agent along with his colleagues found themselves in a position of fighting a policy in place and pushing for a change] “I remember when the double authentication came out, first we pushed for our manager to have access [to the pin that allows us to buy and sell stocks for a specific customer] and give it to us instead of just the IT [generating the pin]. The IT has to take care of the company as a whole. It has its work to do so. Even though they need to take care of us as well, they also have other priorities. We moved it to our manager. Then we noticed the manager also isn’t there 24/7, and our firm is opened basically 24 hours a day, five days a week. With this understanding, we came to the conclusion that how about in our specific team where we need this information, every member on their shift will have access to this [system generating the pin]. In case anything happens [in the stock market], they [the agents] can quickly react and stop it from growing, stop any problem from escalating, so to speak.” (Additional Respondent 5)</p>

## Appendix C: Additional Survey Data

To further validate our findings, we contracted with an online marketing firm to collect data from 120 additional working individuals across various industries. Table C1 provides the demographic summary of the respondents and C2 exhibits the representative industries across our sample.

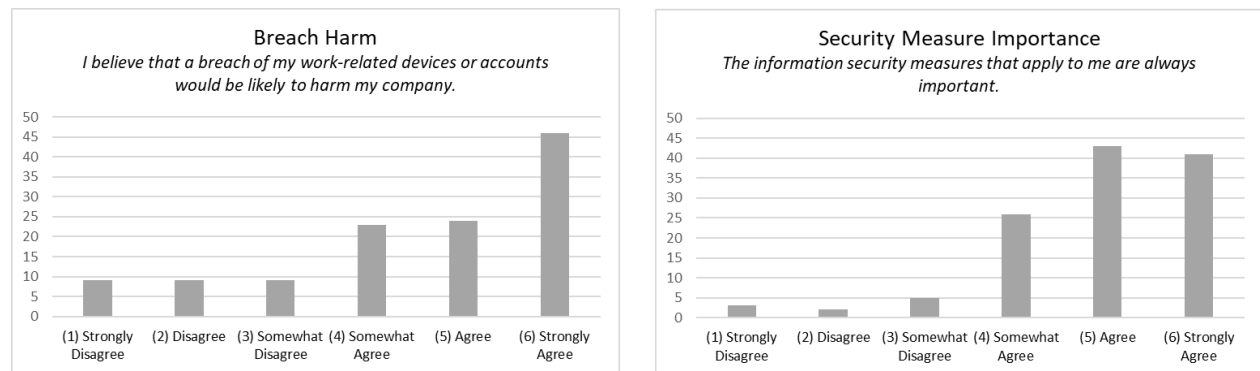
To ascertain the prevalence of the beliefs we identified in our qualitative study and to establish their existence across insiders working in a variety of industries, we constructed scales to capture the two key beliefs: (1) breach harm, and (2) security measure importance. Figure C1 exhibits the prevalence of IS security beliefs that delineate the security profiles: breach harm and security measure importance. As shown, these beliefs vary across our diverse panel of insiders.

**Table C1. Sample Demographic Summary**

Category	Percent	Category	Percent	Category	Percent		
Female	49.2%	Management	65.0%	IT position	48.3%		
Employees	Percent	Tenure	Percent	% day using IS	Percent	SETA frequency	Percent
1-100	19.20%	0-9 years	30.8%	0-40% of day	20.0%	Never	6.7%
100-499	15.80%	10-14 years	40.0%	50% of day	11.7%	Once or twice a year	39.1%
500-999	24.20%	15-19 years	14.2%	60-90% of day	49.2%	Several times a year	33.3%
1000 or more	40.80%	20 or more years	15.0%	100% of day	19.2%	At least monthly	20.9%

**Table C2. Industries Represented**

Education	12
Finance or insurance	7
Government	4
Healthcare or social assistance	13
Information	14
Manufacturing	6
Other	41
Professional, scientific or technical services	14
Retail trade	7
Transportation or warehousing	1
Wholesale trade	1
<b>Total</b>	<b>120</b>

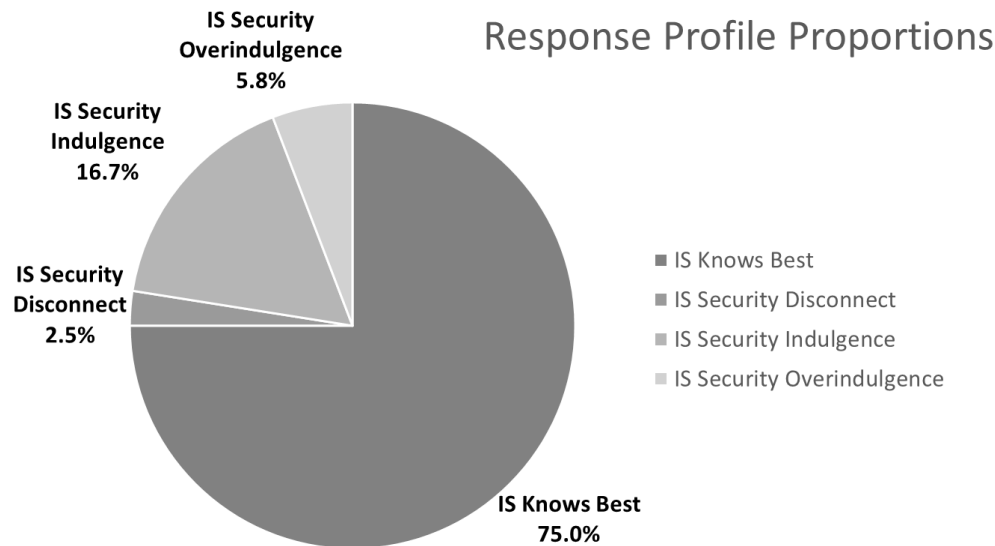


**Figure C1. IS Security Measure Beliefs: Breach Harm and Security Measure Importance**

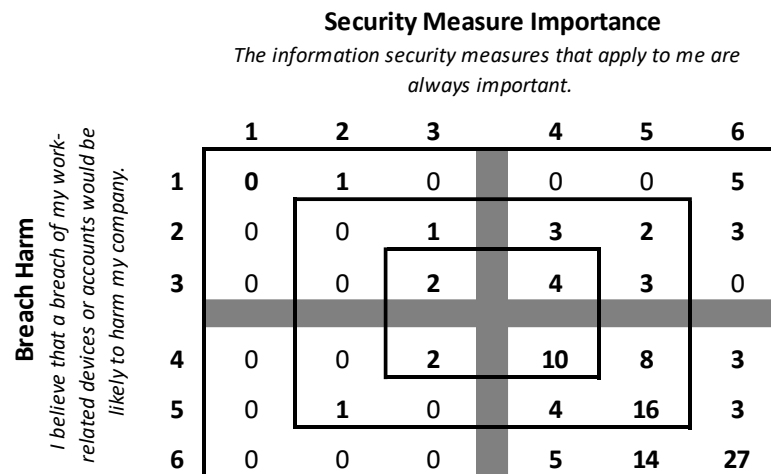
Importantly, our prior research found that we can ascribe an individual to an IS security profile based on this set of beliefs: breach harm and security measure importance. Figure C2 shows the breakdown of our sample by profile.

Seventy-five percent of our sample falls into the IS knows best profile based on their beliefs about IS security. Indeed, this should be the profile that captures most employees in an organization. Because each individual's actions can affect organizational IS security, the more employees that fall outside the IS knows best profile, the greater the security risk.

Furthermore, because we used Likert-style scales to capture individuals' beliefs, we are also able to measure the intensity of these beliefs. As shown in Figure C4, only 27 respondents (22.5%) strongly agreed with both belief statements. Thus, these post hoc analyses show that varying intensities of belief are within each profile. Indeed 15% of respondents appear ambivalent, responding "somewhat disagree" and/or "somewhat agree" for both beliefs.



**Figure C2. Security Profile Proportions**



Axes: (1) Strongly Disagree, (2) Disagree, (3) Somewhat Disagree, (4) Somewhat Agree, (5) Agree, (6) Strongly Agree

**Figure C3. Security Belief Intensity**

Next, we wanted to examine the industry make-up of the profiles. Table C3 exhibits the industries represented in each profile (i.e., Figure C3 quadrant). As shown, each profile is representative of respondents across multiple industries. This is important because our original theory was established using qualitative data in a single industry. Thus, our supplemental analyses lend support to the cross-industry relevance of our findings, confirming that the four profiles derived from our qualitative analysis in a single industry are applicable to employees across a range of industries.

According to our model, insider actions will vary according to their profile. To support these findings, we asked our respondents about their IS security actions. Specifically, we “piped” our respondents to specific questions based on their beliefs and the associated profiles. Table C4 shows the prompts and insider responses.

**Table C3. Respondent Industries by Profile**

<b>IS knows best</b>	<b>90</b>	<b>IS security indulgence</b>	<b>20</b>
Education	12	Healthcare or social assistance	3
Finance or insurance	6	Information	3
Government	4	Manufacturing	2
Healthcare or social assistance	9	Other	9
Information	10	Professional, scientific or technical services	2
Manufacturing	2	Retail trade	1
Other	29	<b>IS security overindulgence</b>	<b>7</b>
Professional, scientific or technical services	11	Finance or insurance	1
Retail trade	6	Information	1
Wholesale trade	1	Manufacturing	1
<b>IS security disconnect</b>	<b>3</b>	Other	2
Healthcare or social assistance	1	Professional, scientific or technical services	1
Manufacturing	1	Transportation or warehousing	1
Other	1	<b>Grand total</b>	<b>120</b>

**Table C4. IS Security Actions by Profile**

<b>IS security disconnect &amp; overindulgence—Example of circumvention motive</b>
<i><b>Prompt:</b> Please provide an example of a security measure you have ignored or evaded at work. Can you help us understand why you made this decision?</i>
<b>Transportation or warehousing</b>
To get the job done
<b>Security Indulgence—Examples of avoidance of IS</b>
<i><b>Prompt:</b> Please provide an example of a system or technology you have avoided at work. Can you help us understand why you made this decision?</i>
<b>Healthcare or social assistance</b>
personal cell phone because my employer doesn't want to install extra security
Registering with my Facebook account
<b>Information</b>
People, I hate people
Well, I don't really avoid any of my system or technology at work, but one time I skipped a checking system because I already checked that.
<b>Manufacturing</b>
Didn't use the company's Wi-Fi on my personal phone
<b>Other</b>
harmful device I have avoided
I avoid old systems in usual because they don't have enough security
I don't use my cellphone for work because I don't want customers contacting me personally
<b>IS knows best—Examples of reasons for compliance</b>
<i><b>Prompt:</b> Can you help us understand why you do or do not comply with all security measures at work?</i>
<b>Education</b>
Because I'm a responsible person and I need to protect and secure my job data
I comply because I do not want to compromise my company.
I don't do anything intentionally however I am sure I break a rule here or there
I don't want to lose my job
I feel it is important for an employee to follow the rules of their employer. Also, we work with children and their personal information needs to remain secure to protect them.

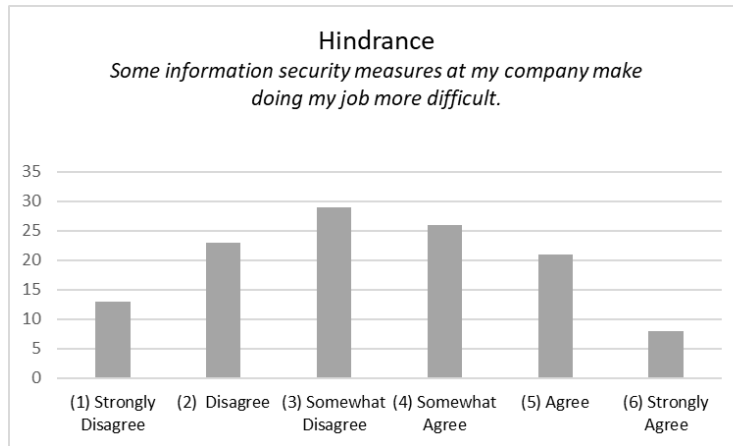
I feel like they are there for a reason, and my company is entrusting next with sensitive material, so I should make every effort to fully comply.
It's in my best interest
Need to keep myself secure online
<b>Finance or insurance</b>
Compliance with security measures is important at my job.
I do comply with all security measure at work because they prevent information from getting in to wrongful hands. They are put in place for a reason and disciplinary action can also result in not following them.
I work for a large company with a huge IT Department. The security measures they take are always carefully explained and come along with what could happen if we get breached, or information is stolen.
<b>Government</b>
Complying with security measures helps protect everyone
I comply with the security procedures because it protects against harmful breaches
I don't want or need to break the rules. I only want to do my work
If not, I will be fired
<b>Healthcare or social assistance</b>
Because the fines to pay for violations are extensive
I comply because I want to protect my client's confidential information
I comply to keep my information safe and my client's information safe
I comply with security measures due to HIPAA
I don't want to cause any breaches or viruses
It's important for my patient safety for me to complete all security measures. I take that very seriously.
<b>Information</b>
Compliance with orders is important for business development
I comply with all security measures, because it's safer for my information, and safer for others' information, and safer for organization work
Important for my job
It is essential to raise the quality of the tasks and maintain customer services.
<b>Manufacturing</b>
The security measures my company uses are unavoidable but require little work: 2-factor login and a badge to get into the office. During COVID, they are requiring masks and 50% office capacity, all fair and reasonable.
<b>Other</b>
Because it makes the business more successful
Because security protocols not only protect my company, but I feel better knowing I am doing my part
I agree with all security measures
I always follow the rules at my places of employment
I completely comply with security measures cat my work to protect my company and my job
I comply with all security measures at work because that protect my company's work.
I comply with all security measures at work to be safe.
I feel that these measures are put into place with our well-being, as well as, others in mind. It is done with the intent to uphold proper standards and overall safety protocol. From my understanding of the measures taken by my company specifically, none cross any lines or issues that I feel are of concern. If this were to change and an element of intrusion or malice was to surface, I would feel otherwise.
Security measures are very important in the company.
The security measures make me feel comfortable in my work
To keep my company safe
<b>Professional, scientific or technical services</b>
Because I must maintain the security and safety of the company
Because it protects me and protects my work from being lost.
Because it's important for the safety of the company
I comply with all security of my company because it's my company rules and I work under this company
I want to keep my job and not have any negative repercussions
To protect firm information and client information and preserve privacy.
We use confidential information that must be protected
<b>Retail trade</b>
Data breach in my company can result in customer and company information that is private to be stolen.
I value my job and the security of info, so I comply.
If the company loses, then I lose. It's in my best interest to do whatever I can to help my employer succeed.
Its customers-based company. If I don't comply with security measures, then it's a breach of trust.

Interestingly, some respondents originally classified as the IS knows best profile provided reasons for their noncompliance that reflected beliefs that we uncovered in our original qualitative analyses. Because our prompt asked for reasons why the respondents “do or do not comply with all security measures at work,” we could further assess these beliefs. Table C5 includes some beliefs disclosed by insiders classified in the IS knows best profile based on their Likert-style responses. While the overwhelming majority of those who were classified in the IS knows best profile provided very clear, strong reasoning for their compliance, these exceptions show that the survey-based approach may overestimate compliance. This should not be taken as a critique of any research method but rather as support for employing multiple methods to understand such vital phenomena.

Thus, as shown in Figures C3 and C4 above, our secondary data analyses support the qualitative finding that insiders often perceive that IS security creates a hindrance to productivity (e.g., an unfavorable lived security experience). To help shed light on the prevalence of this phenomenon, we also directly asked our respondents whether information security measures make doing their job more difficult. Figure C4 summarizes their responses and exhibits the pervasiveness and intensity of this lived experience.

**Table C5. IS Knows Best: Examples of Reasons for Noncompliance (Potential Misclassification)**

<b>Prompt:</b> <i>Can you help us understand why you do or do not comply with all security measures at work?</i>	
<b>Information</b>	
	It is a lot to keep in mind
<b>Other</b>	
	it makes my job harder
	Need to get work done
<b>Professional, scientific or technical services</b>	
	When out in field, may not use VPN
<b>Healthcare or social assistance</b>	
	I work at home and am alone most of the time
<b>Wholesale trade</b>	
	Not all apply to my job



**Figure C4. IS Security Measure Hindrance**

Finally, our model predicts that IS security actions by insiders have the potential to lead to new IS security measures in an organization. To validate that assertion, we asked our sample about how their organizations would respond to noncompliant, circumvention, or avoidance behaviors in the workplace. As shown in Table C6, respondents indicated that their company is likely to add new security policies, procedures, or technologies to address such behaviors in the workplace. This finding supports our original model. Interestingly, the IS knows best profile also showed the strongest belief that their organization would add new security measures based on noncompliance.

We believe this finding uncovers a critical contextualization for our research: the potentially positive impact on security that new IS security measures can have. For example, IS knows best profile may also be influenced by their knowledge that their organization will punish noncompliance, and new IS security measures may be added if noncompliance is discovered. On the other hand, the IS disconnect/overindulgence profiles exhibited the lowest level of belief that their

organization would add new IS security measures if circumvention is discovered. Thus, our work shows that both adaptive and maladaptive responses are possible for both extremes. For example, in certain circumstances adding new IS security measures may be favorable for security and lead to more adaptive behaviors. However, when IS security measures create a productivity hindrance or perpetuate beliefs about a lack of breach harm and/or a lack of security measure importance, maladaptive responses may emerge. Thus, we contend that our analyses show that organizations should strive to enforce their IS security measures while reinforcing adaptive beliefs and minimizing maladaptive beliefs.

**Table C6. IS Security Measures as Response to Circumvention, Avoidance, or Noncompliance**

<b>IS Security Indulgence</b>
<i><b>Prompt:</b> Think about how your company is likely to react if it is discovered you avoided a system or technology at work to avoid extra security measures and then respond to the following question.</i>
Based on your experience, how likely is your company to add new security policies, procedures, or technologies to address these types of security behaviors? <sup>1</sup>
Mean Response = <b>3.80/6.00</b>
<b>IS Security Disconnect/Overindulgence</b>
<i><b>Prompt:</b> Think about how your company is likely to react if it is discovered you ignored or evaded a security measure at work and then respond to the question below.</i>
Based on your experience, how likely is your company to add new security policies, procedures, or technologies to address these types of security behaviors? <sup>1</sup>
Mean Response = <b>2.80/6.00</b>
<b>IS Knows Best</b>
<i><b>Prompt:</b> Think about how your company is likely to react if it is discovered employees do not comply with security measures at work and then respond to the following question.</i>
Based on your experience, how likely is your company to add new security policies, procedures, or technologies to address these types of security behaviors? <sup>1</sup>
Mean Response = <b>4.89/6.00</b>
<sup>1</sup> Scale: (1) <i>Extremely Unlikely</i> to (6) <i>Extremely Likely</i> .

## Appendix D. Data Structure Respondent by Respondent

Table D1a. Illustrative Quotes Respondent by Respondent for Profiles

Response profile	IS Security measures are not always important	IS security measures are always important	Security breach unlikely to seriously harm the organization	Security Breach likely to seriously harm the organization
Resp. 1 “IS Knows Best”		<i>“It’s an inconvenience, but I think most people probably <b>understand the need for the security</b>. There is a little bit of delay [in the repair of the institutionally provided laptops], as I mentioned, if we’re trying to recover data or trying to run some utilities on the drive, the drive needs to be unencrypted. But again, I think <b>most people understand why the security is there</b>. Once we explain what we have to do, <b>they’re pretty understanding about that.</b>”</i>		<i>“We use encryption software on the laptop hard drives because <b>they’re mobile, greater possibility that they may be stolen or left somewhere, and left in the wrong hands.</b>”</i>
Resp. 2 “IS Knows Best”		<i>“So, a <b>reinforcement of the original training is important</b>—so initial training, and then reinforcement training every year or every other year to <b>make sure</b> that you understand the policies and that you’re still following them appropriately.”</i>		<i>“And if <b>each user is an access point</b>, then we have to ensure, as an organization, that that <b>security is as strong and as proper as it needs to be</b>, to protect the information across the network at large. Because our <b>adversaries are very skilled at getting access to information</b> once they’ve been able to breach the exterior or the external fence, if you will, of our network frame.”</i>
Resp. 3 “Disconnect”	<i>“You have to have a better understanding. I mean how much security policy and—policies—I mean <b>how much is enough?</b> I mean what—is <b>there a point of diminishing returns?</b> And so they don’t know if it’s <b>overkill</b> until they really can partner and understand how do I do my job? It’s a lot like, I guess, laws. Laws are passed. I mean how many laws do you see being unpassed? You don’t see that very often.”</i>			<i>“And with a lot of the press being out there on what’s happening and the <b>cost of a data breach, to reputation, possibly financial damage, litigation, you know, the stakes are high.</b>”</i>

<p>Resp. 4</p> <p>“Indulge”</p>		<p><i>[Responding to a question about if they feel caught between policies and productivity demands] the respondent answered “Not really. <b>The policies are not that bad.</b>”</i></p> <p><i>[Comment/Context: The programmer does not see any conflict between any security policies and his productivity or work context.]</i></p>	<p><b>“I don’t think a security breach will affect the reputation of the institution.</b> As far as I know, a security breach is a <b>very common thing. It’s the norm in this century.</b> People are becoming used to it.”</p>	
<p>Resp. 5</p> <p>“Overindulge”</p>	<p><b>“I mean, it would just be like me using my credit card anywhere else. I mean, yeah, PHEI might have pointed me there, but we’re not even really involved in that transaction, so I <b>don’t really understand why we’re driving it that hard.</b>”</b></p> <p><i>[Context: quote “there’s a product that we were looking at, and it had credit card integration, and PHEI was requiring security measures over and above what banks and retailers currently require for credit card data, and this company was like, ‘Well we can’t support that yet.’... Now PHEI is just like, ‘Okay, it’s going to be free to the students,’ which it’s a good deal for the students, granted, but they’re having to limit who can use it. There’s only certain students who are going to be able to use it because PHEI is having to pay for everything, and that’s basically business decisions that are all being driven by the fact that our credit card data requirements were too stringent.”]</i></p>		<p><b>“But PHEI is so concerned and afraid about having any kind of a breach that, well, I don’t know. Sometimes that drives <b>decisions more than I would like to see.</b>”</b></p> <p><i>[Context: see the context in the beginning of this row]</i></p>	
<p>Resp. 6</p> <p>“IS Knows Best”</p>		<p><b>“With the security training, the <i>only</i> way to make it happen would be to enforce it <b>mandatory.</b> You have to attend this training once a year, or something.”</b></p>		<p><b>“As far as security goes, it’s had to become tighter and tighter <i>because of the world we live in.</i> Everything is <b>accessible</b> if you’re devious enough or smart enough, or whatever.”</b></p>

		<p><i>[Context/Comment: The IT helpdesk person is happy with the idea of enforcing trainings on all the employees (didn't specify the mechanism) because they are facing the challenge that some or many employees are not attending the awareness and training programs.</i></p> <p><i>A relationship between the idea of enforcing a training and considering this security measure (the training) as always important might be inferred]</i></p>		
<p>Resp. 7</p> <p>"IS Knows Best"</p>		<p>"Since we've been doing it so long, people are kind of used to it and just go with it. They <b>understand</b> that we're just trying to <b>secure their data</b>."</p> <p><i>[Context/Comment: This is about the encryption of the employee laptops. The repairman needs to decrypt (that takes several days) thus delaying the repair. But he is saying we've been doing this encryption for years now, thus the employees are kind of used to it, and they understand that the encryption is for their data security.]</i></p>		<p>"You've got grades, you've got <b>social security numbers</b>, you have all kinds of stuff that can get out that's a <b>disaster</b> if we didn't apply this type of policy."</p>
<p>Resp. 8</p> <p>"Overindulge"</p>	<p>"At the same time, some of the reason for questioning it is sometimes <b>a little silly</b>."</p> <p><i>[Context of the Quote: "For example, there was a concern over one product that we were looking at using that was a publisher material, but it would have the ability to write quiz grades back into the learning management system. It needed that level of access to write grades back. That one didn't get approved because security people were afraid that if an employee of that publisher had a child at PHEI, an employee there can write grades back in here and inflate that student's grade</i></p>		<p>"The integration, like with that publisher that could write grades back, what's the worst-case scenario that could happen, that one employee there overwrites some grades in one particular class? Yeah, that's a big deal academically, but <b>we're not talking that's top secret government information</b>. That <b>obscure, unlikely scenario was primarily one of the main justifications for saying</b>, 'No, you can't do this integration with this publisher because there's this <b>off chance</b> that somebody there might do something unethical like that.' That seems a <b>little silly and unlikely</b>, but that was one of those scenarios where</p>	

	<i>and things like that. A really obscure, unlikely type scenario that if they ever did that, that would be out in the press. They would be out of business. Nobody would use that publisher. That publisher would have serious ramifications if that ever happened.]”</i>		<i>we didn’t get a chance to really do that.”</i>	
Resp. 9 “IS Knows Best”		NA		<p><i>“Because of the <b>growth of cloud services</b>, the <b>necessity</b> of a login, and the security for that login has increased. The other part of everything would have to be with anything mobile, with the <b>new trend in mobility and technology with mobility</b>, there is a <b>corresponding trend in the security</b> dealing with that.”</i></p> <p><i>[Context/Comment: When responding to what the biggest changes that had been witnessed in terms of policy change, this respondent seemed to see the usage of the cloud, and the proliferation of mobile devices (Ipads etc) an underlying reason why a double authentication was enforced and by inference the lack thereof would have led to security breaches seriously harming the organization.]</i></p>
Resp. 10 “Overindulge”	<i>“<b>My data</b> in the grand scheme of things <b>is not important data</b>. Top secret data, financial data, that’s important data. Identity data, that’s important data. My application data is important to us. <b>It’s not important outside of us</b>. No Russian hacker wants to get into a learning management system just so they can change the content. So <b>I don’t see the importance of many of the policies and measures</b>.”</i>		<i>“I use my credit card at Home Depot. Home Depot had a breach. Okay. That’s <b>no big deal</b>. You get the credit monitoring. <b>You go on with life</b>.”</i>	
Resp. 11		<i>“Before it was always you had a workstation that was on the network or</i>		<i>“So firewalling, network security was one of the reasons why we put it on the</i>

“IS Knows Best”		coming through VPN so they could tie in a name to an address. But the way this stuff works, you couldn't do that. So the security folks were very concerned about that, <b>and I think rightly so... I think it's been very effective</b> from an ITS standpoint in making sure that our systems reduce the number of vulnerabilities.”		DMZ. They just want to get their work done. They know that in <b>this day and age security is an issue</b> and they tolerate it pretty well.”
Resp. 12 “IS Knows Best”		“I think definitely they've been increased [policies] over the last ten years. One is to protect sensitive data and personal data for individuals. From what I understand though, I think most people understand the importance of data security and security of the systems...I think, again, it comes back to the fact that I <b>understand why these are put in place</b> typically, and I guess we've come to the point of knowing <b>we need to be protected</b> , and our folks are doing a good job of protecting them.”		“Well, I believe the university, for instance, if a hacker obtains your name, address, and Social Security number, <b>they can do a lot of damage to you.</b> [Security measure increase] comes from, I think, more and more, you hear around the country, <b>universities are prime targets.</b> ”
Resp. 13 “Overindulge”	“It's like me telling a faculty member now what they can choose to use in their course based on an IT security policy, not based on what's good for the students' learning in the course...And I'm saying allowing the integration is the cost of doing business.”		“If someone were to break into the system, and they stole a students' PHEI grades, and they saw that he got a B on this assignment, <b>how bad is that going to be?</b> ”	
Resp. 14 “IS Knows Best”		“We try to educate the users and <b>make sure</b> they know to check for updates, <b>make sure</b> their machine is updated and that sort of thing.”  [Context/Comment: This quote is a proof that the respondent believes IS security measures (in this case the updates and the patches) are always important, since the context shows that the users delay the updates, and the respondent is “pretty proactive” in		“We try to educate the users and make sure they know to check for updates. But that's easier said than done, <b>getting them to actually do that</b> , which is why we try to be pretty <b>proactive</b> about <b>pushing</b> out updates.”  [Context/Comment: The context of the respondent's statements shows that the respondent feels the software patches and updates are important to avert a serious harm to the organization.

		<i>pushing out the updates. If they respondent doesn't consider the updates/patches as always important, they won't be proactive about them.]</i>		<i>That's why the respondent is pretty proactive about the patches.]</i>
Resp. 15 "IS Knows Best"		<p><i>"10 years ago, it was really difficult to get people to understand the <b>necessity of patching</b>. And now, they realize, especially with how much it is in the media, how <b>important it is for them to keep their devices updated</b>. And so the updates have gotten to the point to where they're happening a lot more frequently. And so that's what we've had to work on, managing more</i></p> <p><i>Well, I mean, we've gotten a very receptive response where people are very happy that we're patching</i></p> <p><i>And what they'll do is they sign an agreement between the user and ITS that says, hey, I'm taking personal responsibility for this device</i></p> <p><i>It's a good thing. It's more overhead, more support on our part, but I think it's a good thing. <b>Because it protects the individual</b>. So, you know."</i></p>		<i>"And so where it used to be that we had to patch a few devices with a few patches, we're now having to patch a lot more devices that have a lot more vulnerabilities. The <b>amount of threats that we're getting are increasing significantly</b> just because our campus has been growing. We've also seen, basically, a lot of <b>vulnerabilities</b> trying to be accessed because a lot of software that's used like Java, Adobe, Microsoft and all those various things are starting to get <b>attacked on a great scale</b>."</i>
Resp. 16 & 23 "IS Knows Best"		<p><i>"I think just the nature of the requirements of the university to protect data has increased, we used to have students' social security number on everything, and now we have an ID number. So, <b>I would say it has increased. But, I think it's a good thing</b>.</i></p> <p><i>But, it's done to protect the individual, and I think <b>the only time they appreciate it is when it's lost or stolen</b>.</i></p> <p><i>I think—I know, from our side, we don't try to. We're trying to <b>protect the data</b>, but from their side, I understand. Because they have—for example, whenever we push updates, security updates, as an example."</i></p>		<i>"we're ensuring that they're not going to be bringing an <b>infected computer</b> here that's going to, basically, potentially, <b>cause security issues</b> for us on the network."</i>

<p>Resp. 17</p> <p>“Disconnect”</p>	<p><i>[it's ok to do personal things and institutional work on the same smartphone; that's the reason he uses his personal phone rather than the institutionally provided phone]. “I don't want the institution to be able to say that this is their phone. In other words, if I'm watching a sports game on this [on my phone], it's my business.”</i></p> <p><i>[Context/Comment: The context shows that the respondent is ok with mixing both work life and private life together on the same device (ie. Using the phone for work-related purposes as well as for private interests). It seems, the respondent is not necessarily seeing a problem that due to their financial position, the sensitive work accounts might become infected with malware while visiting sports websites. In other words, the respondent doesn't see this separation of devices as always important. The separation of devices is a basic security measure (ie. a device for work, and another for personal life).]</i></p>			<p><i>“So I write these passwords down <b>out of fear</b>. So, what I do is, when I change my [PHEI] ID, which I do quite often, for various reasons, but mainly for <b>security reasons</b>, to make sure somebody wasn't looking over my shoulder when I was typing, and they're walking right there, and I go, <b>crap, They were looking over my shoulder when I typed my password</b>. I'm changing my password more often lately.”</i></p> <p><i>[Context/Comment: The respondent changes their system ID (meaning the password) often, out of fear of a breach from shoulder surfing. So they believe a security breach will seriously harm PHEI.]</i></p>
<p>Resp. 18</p> <p>“Disconnect”</p>	<p><i>“It <b>would be nice</b> if within PHEI on all the different things they required us to do <b>you could use the same password</b>.”</i></p>			<p><i>“I <b>totally understand</b> why they would not want us to use our same you know, password and everything on other outside systems and I can fully understand why they wouldn't want to integrate their systems with ours because PHEI has a pretty heavy firewall. And I don't know that these others maintain the integrity of their security systems and they may not match up...our passwords on the outside <b>vendors could get hacked</b>.”</i></p>
<p>Resp. 19</p> <p>“Disconnect”</p>	<p><i>“And so there's all these new security things, and my observation is <b>it creates more work for the help people</b></i></p>			<p><i>“I know that <b>a security breach of social security numbers will affect our reputation...</b>”</i></p>

	<i>because now we have to call for questions with this kind of stuff, and then too it creates more work for us, and I <b>personally haven't seen the value yet...</b> My own feeling is <b>some security they do because they feel like they need to do it to demonstrate that it's state of the art security, even without reflecting on who it's helping and what problem it's solving.</b></i>			
Resp. 20 "IS Knows Best"		<i>"From my perspective, ITS security here has done an excellent job of making sure that nothing like, there aren't any data breaches. Again, I know that for some people that's probably viewed as extreme or that they've gone further than they should, but again, <b>it's sort of—at the same time—hard to argue with when there's, I believe, a higher degree of comfort that measures are being taken to protect people's data.</b>"</i>		<i>"Obviously I think fundamentally they're concerned about people's data, other than the ramifications of that information being exposed, I think there's a genuine concern for taking care of people and the information that we have about people. And then beyond that, it is the specific ramifications, the <b>monetary damages as well as the reputational damage</b> for having some sort of information breach on campus."</i>
Resp. 21 & 22 "IS Knows Best"		<i>"Do we have people that fall for phishing and spearing scams? Absolutely. Absolutely. <b>And so because of that, I back up the IS security measures in place, like double authentication.</b>"</i>		<i>"People are like, 'That's inconvenient.' I'm not saying it's not inconvenient. I'd never make that claim. But what I'm saying is that the <b>risk is so high that we have to take some additional action.</b> Most of our, what I would say, changes that we do, absolutely come into place because there's evidence to back up why we're doing this."</i>
Resp. 24 "Indulge"		<i>"It's all about keeping people, restricting access to our data to the people who really should have access to our data. I am fully aware that there are <b>a lot of people out there</b> who want to try to get <b>access to our data</b>, and whether it's, honestly it's <b>no different than working with a financial institution.</b> We all have dozens of different sites that we go to and they all almost all require us to change our</i>	<i>"I think they're actually quite proactive about it [sending security emails, change of passwords). I don't think that for the layperson a lot of the policies and things that they have, <b>most people don't give them that much thought honestly.</b> I think we just assume that they have the appropriate amount of security to protect the systems that we have, and if they ask us to change passwords every</i>	

		<p>password. So what ITS is asking us to do</p> <p>is not an unusual thing, and the challenge is to try to think of enough new passwords that you can still keep track of to make all this system continue to work. And so <b>no, I don't object to ITS asking me every six months to change my password and to not use one that's the same as the one that I used previously.</b>"</p>	<p>three months or every six months or something, people just do it."</p> <p>[Context/Comment: The whole quote in context shows that the respondent only goes through the motion of the security emails (ie. changing passwords). This could be interpreted as the respondent not believing that a security breach would seriously harm the organization. Otherwise, the respondent would be more proactive about the security emails.]</p>	
<p>Resp. 25</p> <p>"Overindulge"</p>	<p>"I get <b>real frustrated</b> with all of that. It's <b>very difficult</b> to try to do our job and keep up with everybody else and have all these <b>obstacles put up</b>. And it's either because of—they say it's either because of security or because of privacy."</p>		<p>"So we've been trying to make a case for why we need to have analytics. Everybody has them and I understand Google Analytics is easy to use and <b>free, even though it's not really free because they're probably using all of your data. They're probably collecting that and using it somehow.</b> But there needs to be some way that we can get web analytics because how can we do anything."</p> <p>[Context/Comment: The case is about using Google administered surveys to research the interests of prospective students. The IT security doesn't want to use a free Google service for the surveys.</p> <p>The quote shows that the respondent is aware that Google breaches the confidentiality of the data of the students who are taking the surveys and using it for ads by profiling the IP etc., but still doesn't believe that this confidentiality breach would seriously harm PHEI.]</p>	
<p>Resp. 26</p> <p>"Indulge"</p>		<p>"I mean they've done a really good job of keeping it secure, but there's still stuff filtering</p>	<p>"I guess hackers are already trying to get our data, but since we <b>don't have very sensitive information, we won't get affected much.</b>"</p>	

		<i>through, and I'd like to see that taken care of."</i>		
Resp. 27  "Indulge"		<i>"I know that you do have to agree to certain policies as you begin to use things like a VPN, but for the most part, that's fairly standard, so I don't have any problems with agreeing to any of the policies."</i>	<i>"But I know our, I guess it's [Web Name] is the one system which is, I guess, where we approve GA timecards and things of that nature, and our staff timecards are submitted through that, so that's a completely separate login, and generally speaking, I have a certain set of kind of password go to's that I think of."</i>  <i>[Context/Comment: The respondent is reusing the same password across different systems/accounts whether personal or work related. Thus, the respondent doesn't believe that a security breach of their password will seriously harm PHEI.]</i>	
Resp. 28  "Overindulge"	<i>"Does everything need to be, sometimes I do feel like we're a little bit ridiculous. Do we need two factor authentication when I can get into the same resources by a web authentication with single factor authentication? Maybe we do, because there's other things you can get to on the VPN that you can't get to through the web. But yeah, sometimes I feel like it's like, 'Are we a bank? No.'"</i>		<i>"So the real question is, could they somehow communicate to everybody the fact that yes it's a little over the top for what you do, but we do this over here which requires us to do this?"</i>	
Resp. 29  "Indulge"		<i>"As far as my group, I'm always on them about protecting things because it's easy to get lax, especially with student records."</i>	<i>"One thing that's really hard for us is IT does not want us to put any grade, calculation, or any grade information in email, and that is impossible for us not to do...It's almost impossible not to include grades, but they really don't want us to do that because it's so easy to break in to our stuff." [by inference, then he does not consider the potential breach of that info, a serious harm to the organization]</i>	
Resp. 30	<i>"I think they go overboard on security. That's another thing. We didn't have</i>			<i>"I think, that PHEI supports us well by getting new computers. Once you use</i>

“Disconnect”	<i>any problems using our software, but that was before. I’ve been using it since 2008. I know another department is trying to add the same software we’re using, and PHEI is giving them fits. I got lucky.”</i>			<i>it, and you’re out there, and <b>things get infected</b>—one time I pressed on something, and I don’t know what it was. <b>There was a link, and every single webpage I would go to had these pop-ups that would come up.</b> I had to call the helpline to get rid of them, and they helped me through it. It came back, and I had to call them back, but eventually—it hasn’t come back in a long time.”</i>
Resp. 31 “IS Knows Best”		<i>“There’s an <b>understanding</b> of why they do what they do, and a <b>thankfulness</b>. I don’t fault them for the layers they put in place, and <b>I don’t find they’re without reason.</b>”</i>		<i>I think that the way they operate it is <b>quite reasonable</b>, especially for the amount of knowledge, and security, and information they store and maintain. When you think about having to pull transcripts from 15 or 20 years ago, and with the incoming class of freshman of over 3,000, and multiply that. That in and of itself is <b>just massive</b>. Then you have the <b>financials</b> that have to be maintained, <b>tuition records</b>, and everything else. It’s an immense amount of information that’s required. <b>I will never fault them in protecting that knowledge.</b></i>
Resp. 32 “IS Knows Best”		<i>“And honestly if I never had to change my [PHEI ID Name] and password ever again until I retire, I would not be unhappy, but I <b>understand why they’re doing it</b> and everything. It doesn’t mean you’re not happy about it, that type of thing. I think you have to be a little <b>more accepting about it, knowing that it is for your best interest in the end.</b> To the students, the faculty, tell them to be a little more patient with ITS. That they’re doing it for <b>their benefit, to keep them safe.</b>”</i>		<i>“The ITS, you know they’re doing something to try to keep us secure on campus, and they’re having to deal with <b>all these things that are trying to come to get into the system.</b> You need to keep the faculty <b>research secure</b>, and you need to keep the students where their <b>accounts aren’t compromised</b>. So you can <b>understand</b> what they’re trying to doing.”</i>

Table D1b. Illustrative Quotes Respondent by Respondent for Actions and Lived Experiences

Resp #	Action theme	Actions	Lived experience (LE)	LE theme
1	<b>IS adaptive behavior</b>	<p>“Security policies do come into play and affect our operations. For example, the PGP software that we use for extra security, the <b>encryption software that we use</b>, mainly with the laptop hard drive.”</p> <p>[Context/Comment: The director is happy that they decided, implemented and enforced encryption on the institutionally provided laptops. The PGP is the encryption program they are using.]</p>	<p>“I think people <b>in general are probably aware</b>, have heard news stories about laptops from companies being lost and data being possibly compromised, that I think <b>they quickly understand</b> why there’s security on the computers. And whenever there is a problem, we can mention, because of the extra security measures, it will delay the process of possibly recovering the data. <b>They seem to be pretty understanding</b> about that also. So it’s more of an inconvenience, but I don’t know if I would say it’s really a problem. Everyone would like it to be quicker, but again, <b>everyone understands the need for the security.</b>”</p>	<b>Sense of security and privacy</b>
2	<b>IS adaptive behavior</b>	<p>“Myself as a user, I think <b>all of us need to follow the rules</b> even if sometimes we don’t understand the ‘why’ behind such rules.”</p>	<p>“So I am very curious about why we are not given much more specific awareness of the security policies and the security needs within the PHEI environment...So I think that that is something <b>I would like to see myself doing</b>, as far as assisting the IT Department or the ITS Department, to be able to provide an awareness and education and training capability for the faculty and staff, because it is important they understand not only what they’re doing, but why they’re doing it, and what this means, not only for themselves, but for their own personal use of information, and why it does bleed down to their use of personally owned devices, etc. at home. <b>So I would love to do that. I would love to be able</b> to provide that type of training and education.”</p>	<b>Positive affect/emotion</b>
3	<b>Circumvention of IS security</b>	<p>“At what point do you keep loading people up [with policies], where they get fed up and say, ‘You know what? <b>I’m going to bypass this.</b>’”</p> <p>[Context/Comment: The department chair is weary about so many new policies and did not specify what specific policies they had in mind. The respondent mentioned a similar thing that is happening in congress: they pass so many laws, they seldom or never undo any laws. The end result is ever increasing piles of laws. The action of circumvention is inferred by the respondent’s statement: “at some point employees will say I’m going to bypass this, because of so many policies”(a paraphrase)]</p>	<p>“Someone is making decisions about a department chair that he should only have <b>information on so and so</b>, someone was making <b>those arbitrary decisions without really understanding my role.</b>”</p> <p>[Context/Comment: This might be considered a productivity hindrance, because the chair is not able to see the students’ grades (those who are changing majors coming from other schools/departments onto another major). These students usually take advice from the chair of A (a major) if they should change their major to A. The chair should be able to see the students’ grades in the other schools specially their grades in the courses relevant to A, in order to better assess their capabilities thus advise them to change major to A or not. Currently the chair cannot do that because of access controls (each chair can see the records of the students exclusively enrolled in their department), for whatever reason. The chair/respondent feels it’s counterproductive and wants to be able to see the grades of all and any student.]</p>	<b>Productivity hindrance: Information constraints</b>

4	<b>Avoidance of IS</b>	<p><i>“Like one of the things that ITS wants is if you have a laptop, your hard drive <b>has to be encrypted</b>. That’s the rule, which is <b>one of the reasons why I don’t have a PHEI-issued laptop.</b>”</i></p>	<p><i>[Question asked to the respondent]: Since you are in the middle of in between users and ITS, if you see some gaps, some things that you can change that need to be changed, are you able to voice your concern both toward ITS and toward the faculty, and how do you do that?</i></p> <p><i>[Answer]: Sure. Pick up the phone or send an email off to ITS folks. <b>They’re going to listen.</b> Now if you have a complaint, it’s like, ‘Well I don’t like the way this works,’ <b>they’ll listen</b> but it doesn’t necessarily mean that they’ll fix it. Because to them, you’re not fixing it, you’re breaking it. But if there’s something wrong <b>they’re open</b>, which is nice.</i></p>	<b>Level of flexibility</b>
5	<b>Circumvention of IS security</b>	<p><i>“I may change <b>little things</b>, like adding the @ sign in replacement of an A or something <b>as opposed to really getting creative</b> and trying to figure out a whole new set of passwords. Like I said, I’m probably not as secure as I should be.”</i></p>	<p><i>“For example, there was a product that we were, I don’t want to get—there’s a product that we were looking at, and it had credit card integration, and PHEI was requiring security measures over and above what banks and retailers currently require for credit card data, and this company was like, ‘Well we can’t support that yet.’ PHEI is basically looking at what the security group thinks the next level of security requirements are going to be, whatever the industry is going to require in a year, two years, three years, and they’re starting to require some of that now. <b>So that kind of puts limits on what companies we can do business with.</b>”</i></p>	<b>Productivity hindrance: Limitations on software choices</b>
6	<b>IS adaptive behavior</b>	<p><i>“We have to <b>train the users</b> not to click on that link just because it says it’s from IT, or be more stingy with their information than in the past.”</i></p>	<p><i>[Regarding troubleshooting phone calls]: What I’ll tell my staff is, “<b>They’re [users] not mad at you.</b> They’re just mad and frustrated. If you don’t have one now, you’re going to have a pretty thick skin by the time you take 100 calls because not everybody—and once again people are 95 percent of the time nice—the other 5 percent, they are just frustrated because they have their work that they have to do, and when their computer’s not working, and they can’t do their work, <b>I totally understand that. If you’re empathetic, and you understand where they’re coming from, you can’t fault them for being mad</b> because I’ve made a mad phone call before in my life, once or twice, too. <b>I understand. We’re all human. You just have to understand where they’re coming from.</b>”</i></p>	<b>Positive affect / emotion</b>
7	<b>IS adaptive behavior</b>	<p><i>“It’s probably been five or six years now that that’s become a policy and we <b>don’t let a computer go out</b>, whether it’s being re-imaged, brand new going out the door to them, <b>we make sure it has some type of encryption</b>...any mobile device <b>we’ll make sure that it doesn’t get out of our hands without having</b> some type of encryption.”</i></p>	<p><i>[Question asked to the respondent]: One of the IT staff said “For some users, for some clients, we are the knights in shining armor. For others we are the devil incarnate.” What is your feedback on that?</i></p> <p><i>[Answer]: No, we are—yeah, I mean, as far as the knights in shining armor yeah, <b>they think we’re great.</b> You know, the installer’s group, they have the Santa Clause effect. They’re bringing new stuff in, they get shoes, shirts, hats, you know ... They install all the new stuff, so they get all the stuff. Go to athletics, they get shoes, they get jerseys, footballs, they look at us as far as, okay, we just repaired it and they’re very <b>thankful</b>, but yeah, <b>we always get pretty good compliments.</b></i></p>	<b>Positive affect / emotion</b>

8	<b>Circumvention of IS security</b>	<p><i>“They wished they could do the integration. I think they <b>continued doing something similar</b> but without that integration. They still can use those tools on their own. They just can’t have that link between the learning management system and those tools. I think they were annoyed and frustrated with that, but ultimately, I guess they <b>went on and did their thing anyway</b>, and just copied the grades <b>manually</b> from that system back here.”</i></p> <p><i>[Context/Comment: Since the faculty were not able to get the integration of the grades written back via the learning management system, they still did it manually, wrote back the grades (or imported them from excel manually). Their action was to circumvent the hindrance, accepting all the things that can go wrong with manual data entry of grades (human error). Thus, the above mentioned quote might be classified as circumvention of the security measure.]</i></p>	<p><i>“One of the concerns that security person brought up was what if someone taking an exam had a child get out of the bathtub in the other room and suddenly walk in past the camera. Now does that mean we are recording child pornography online? Again, <b>really obscure, kind of stretching a little bit here, but that was one of their big concerns about this sort of tool. We can’t do that. We can’t have this.</b> We have to have methods to delete those files immediately...It is one of those situations where the better product didn’t have the ability to take those videos offline right away. <b>We ended up with what I personally feel is a second-best product because the first-best couldn’t meet that particular security concern in a way that we felt was adequately addressed ...</b> They do, functionally, almost the same type of thing. <b>It was just a cleaner interface, simpler to use, a more long-term reputable company, larger customer base, better support.</b> It was kind of like comparing large corporation A to large corporation B, <b>kind of a Coca-Cola to Pepsi kind of thing. Pepsi is good. It can do most of the same stuff, but it’s not Coca-Cola kind of a deal. We would have liked the Coca-Cola of this particular product. It seemed like it was a better fit for our institution, but Coca-Cola didn’t have the ability to do this one thing</b> we want it to do as far as going in and deleting videos immediately without a 90-day waiting period.”</i></p> <p><i>[Context/Comment: This is a security concern related to a software that monitors the exams taken online at home. It uses the camera of the laptop to take the video of the student while taking the test. There is a productivity hindrance because exam proctoring software A (that has “a cleaner interface, is simpler to use, better customer support”..., thus more productive) was denied because of a fringe security concern.]</i></p>	<b>Limitations on software choices &amp; productivity hindrance: Software-defined business decisions</b>
9	<b>IS adaptive behavior</b>	<p><i>“We’ll bring the computer back, wait for two weeks to make sure they (the users) have all their files, and then <b>we use the magnetic storage data sanitization.</b> The Department of Defense has kind of a method that uses seven passes to wipe a hard drive. <b>We wipe it with that.</b> From there, the computers go to pallets to be sold to recyclers. They have to <b>be certified</b>, basically.”</i></p>	<p><i>“Like I installed new MacBook for a lady, I want to say it was two days ago. I mean, she’s not a new employee. I would assume, I’d think, from what I remember, since our computer policy is every four years, she’s at least been here for four years, because I think she’s the only one who had the computer beforehand, so she’s been here for a while. And she said she had tried to use VPN multiple times and that it didn’t work. <b>So I, again, I walked her through, and I’ll even email them on campus, I’ll go ahead and go through, walk them through, how to connect, this is what you do to connect show them how it’s connected, and everything,</b> and I would have thought that especially for the people who need VPN on a daily basis, they would already know how to do that. And so it’s a little bit surprising that I still have to go out and teach that. I get it when it’s a person who’s new to the university, but it’s interesting that I’m still running into that. Now obviously you get a lot of, because a lot of people don’t use it basically because they’re on a desktop and they switched to a laptop. So a little bit of that is just the fact that people are becoming more mobile in dealing with more mobile</i></p>	<b>Level of flexibility</b>

			systems. So, but like I said, it does surprise me that I'm still having to teach that to people on a regular basis."	
10	<b>Circumvention of IS security</b>	<i>"I actually just recently made a more concerted effort to decouple my personal life from my work life. And on my personal machine, it's been really mixed. I have personal photos on this [work] machine. Drop Box seems to have some things that are more interesting [than PHEI's Box]...IT's preference that, if it's a PHEI related document, it needs to be on your work machine or in Box. And if it's personal, it really doesn't belong in either."</i>	NA (Lived Experience not found in the transcribed file)	<b>NA</b>
11	<b>IS adaptive behavior</b>	<i>"We had to go through ITS to make that happen and particular through the systems and security group. And it's tedious. I mean, it's cumbersome because now you've got this added layer of bureaucracy to have to deal with. But from an IT perspective, I can see the importance of it. It's a way of catching potential vulnerabilities."</i>	<i>"Before it was always you had a workstation that was on the network or coming through VPN so they could tie in a name to an address. But the way this stuff [the new measure] works, you couldn't do that. So the security folks were very concerned about that, and I think rightly so."</i>	<b>Sense of security and privacy</b>
12	<b>IS adaptive behavior</b>	<i>"I think most people understand the importance of data security and security of the systems; For the most part, I think people have become more understanding."</i>  <i>[Context/Comment: This is a testimony from an IT security director that the people mostly are showing adaptive compliant behavior. Quote "From what I understand though, I think most people understand the importance of data security and security of the systems. And so I think it comes to a matter of trusting, are the people that are then interpreting the environment, the risks, and the things that are in your environment, and then developing and implementing those policies, if you feel that they are doing a good job, then you would tend to trust them and try to support them. That's how we feel. I don't get a lot of pushback when faculty can't use things. There will always be some. But then, also, I'm not as much on the frontline. So the people in my group tend to have more direct contact. So I may not hear about people might be a little dissatisfied.]"</i>	<i>"I think, again, it comes back to the fact that I understand why these [measures] are put in place typically, and I guess we've come to the point of knowing we need to be protected, and our folks are doing a good job of protecting them".</i>	<b>Sense of security and privacy</b>
13	<b>Circumvention of IS security</b>	<i>"I, ultimately, was able to get the publisher content integrated. And I think maybe from the argument of it's really not necessarily our place to tell the faculty what their content is."</i>	<i>"It's like me telling a faculty member now what they can choose to use in their course based on an IT security policy, not based on what's good for the students' learning in the course...And I'm saying allowing the integration is the cost of doing business."</i>	<b>Productivity hindrance: Limitations on software choices</b>

		<p>[Context: “At some point, I ended up having to have the VP assume the risk for allowing us to link to the publisher’s content. They call it a deep integration. So it’s an integration between the publisher’s content and their course within the Learning Management System. And so IT security policy was no, we don’t think it’s a good idea. It opens up this system to too much risk. Our recommendation is we can’t go forward. And I’m saying this is the cost of doing business when I don’t know what every book that is on campus that faculties are going to choose to use. And so I had to make the argument to the dean that publisher content, it’s like me telling a faculty member now what they can choose to use in their course based on an IT security policy, not based on what’s good for the students’ learning in the course.”</p> <p>Comment: From the context it seems the “action” is pushing back the ITS security decision/concern, and circumventing the IT security power and position, going all the way up to the Vice President (to whom the IT security reports) to get the approval of the software integration.]</p>	<p>[Comment: From the context many of the solutions were being denied, thus in the eyes of the respondent, there were undue limitations on software choices.]</p>	
14	<b>IS adaptive behavior</b>	<p>“I work with the security group as far as making sure the machines, desktop machines on campus, <b>are secure and updated and patched.</b>”</p>	<p>“There are some people who have chosen to opt out of the updates, <b>which is something we allow them to do.</b> So a lot of people, science building for instance, they’re running simulations of some sort that take several days to run, so obviously they don’t want their machine rebooting in the middle of that, <b>so we allow them to opt out,</b> in which case they do have to, they are responsible for keeping those updated. <b>In those cases, we have a form they fill out that basically says that they’ll take responsibility for that.</b> It doesn’t necessarily mean they do keep things updated, but they’ve at least claimed responsibility.”</p>	<b>Level of flexibility</b>
15	<b>IS adaptive behavior</b>	<p>“And so where it used to be that we had to <b>patch</b> a few devices with a few patches, <b>we’re now having to patch a lot more devices</b> that have a lot more vulnerabilities. The amount of threats that we’re getting are increasing significantly just because our campus has been growing.”</p>	<p>[Question]: Have you ever faced a situation in which security policies have hindered your own ability to work effectively in your role?</p> <p>[Answer]: I guess, for me, <b>it’s actually helped me more,</b> the security policies, than hindered me just because <b>it’s given me the ability to meet with that patch management group, and it’s a lot easier to deploy out patches with the more policies that we add</b> because, basically, people see the significance of needing to get their devices updated and patched. And plus, like the media helps a lot, too, because it goes through, and it shows what happens when computers get compromised, when people do phishing schemes and click on links and identity theft and all of that.</p>	<b>Enhanced productivity</b>
16 & 23	<b>IS adaptive behavior</b>	<p>“We started <b>requiring all laptops to have encryption...</b>But, it’s done to protect the individual, and I think the only time</p>	<p>NA (Lived Experience not found in the transcribed file)</p>	<b>NA</b>

		<i>they appreciate it is when it's lost or stolen. And then, they see, oh, well, I don't have to worry about that, because it's got encryption on it."</i>		
17	<b>Circumvention of IS security</b>	<i>"I have been in the <b>habit of setting that as the same ID as my PHEI ID</b>, whether that's good or bad ... I got to go back to <b>my snazzy little page, here, and add the account, and the user ID and the password, right there</b>. And, the sad thing is, if you go through a lot of these, the <b>passwords are very similar</b>, you know? So, they are similar consecutively, but also similar throughout the systems ... Yeah, I'm very embarrassed. User ID and name. I mean, it's embarrassing."</i>	<i>"It's more that than it is a <b>loss of time</b>. It's more like, I gotta stop, I've gotta track this email, I've gotta track this password to everywhere I go, fix what it goes, whatever. <b>It's a hassle. Definitely a hassle. Passwords are a friggin' hassle</b>, and PHEI is a part of that <b>problem</b>."</i>	<b>Productivity hindrance: Time inefficiency</b>
18	<b>Circumvention of IS security</b>	<i>"I put the <b>written down passwords in their respective folders</b>, like for this stuff that has to do with budget. I have a little post-it note that I stick in that file or I print off when I do my initial creation of it I print off that page and write it on it and that goes in the file with that, in case I forget it."</i>	<i>"I put those [sensitive work passwords] in their respective folders, like for this stuff that has to do with budget...that's <b>why I don't access my files or do any work from home</b>."</i>	<b>Productivity hindrance: Information constraints</b>
19	<b>Circumvention of IS security</b>	<i>"They had it [my PHEI laptop] set up where if I lose this they can scramble it for me, they can log in with their network ID and delete my whole hard disk, but <b>I wouldn't even want to tell them if I lost it</b> because maybe I'm going to find it in a day or two and then it's all gone, so they're kind of <b>disincentivized from telling stuff</b>."</i>	<i>"The difference is, the <b>Apple store</b> where i live, I walk in and walk out and it takes me <b>30 minutes</b> and I have the monitor. <b>Here [in PHEI] it's probably going to take a month</b> because of the security check ups."</i>	<b>Productivity hindrance: Time inefficiency</b>
20	<b>IS adaptive behavior</b>	<i>"The fact that ITS chose to implement two factor authentication to be able to VPN into campus <b>was a good move to strengthen the security without</b>, in my mind, adding a whole lot of burden to people to be able to use that."</i>	<i>"My experience with the security people on campus is that <b>they're willing to listen and try to find a solution</b>. So generally it has not been a case where it's sort of like, 'No, what you want to do violates policy and there's no option.' It's sort of, 'Okay, this is the policy and this is what you're trying to do. <b>How can we find something within policy that still accomplishes what you want to do?</b>'" And in that sense, there's at least some <b>measure of flexibility</b> in terms of pursuing <b>a workable solution</b> that I think is helpful to their approach and the way that they treat people in addressing these issues.'"</i>	<b>Level of flexibility</b>
21 & 22	<b>IS adaptive behavior</b>	<i>"Last Friday I spoke to executive council, all the vice presidents and president, and gave them an update, including the chair of the board, on information security. What are we doing on campus? What's our new initiatives? What are the things we're concerned about? All those sort of things. <b>They hear it. They absolutely hear it. They understand the risk.</b>"</i>	<i>"I do presentations to all new users of PHEI. Every time there's a new staff member that comes on, we have orientations that happen and I'm one of the presenters. And I get to sit in that room and say—I joke, you know—"You walk in the room and, Yeah, you don't have your credit card number on your shirt. You don't have your social security number on your shirt but you don't treat your passwords that carefully. Why? What is—well, because you don't see a risk in sharing a password. Let me explain the risk. Let me quantify it for you.'... And then you talk about things like their personal information. You talk about things like [PHEI information] and things like that. And <b>of a sudden the light bulb goes on. They're like, wow.</b>"</i>	<b>Sense of security and privacy</b>

24	<b>Avoidance of IS</b>	<i>"I'm not certain that their system works very well for mobile devices yet, and I'm not sure if that's intentional or not, but the ability to use an iPad, to use VPN through an iPad doesn't work very well, honestly, and a lot of our payroll system, payroll systems, our budgeting systems, require VPN to do that, and you cannot use a mobile device to access any of that. <b>Therefore I don't access them from home.</b>"</i>	<i>"I mean, I have <b>no complaints</b> with IT security honestly. <b>I really don't.</b> I find them to be very responsive, I mean, we live in a world now where we expect information to be at our fingertips instantly at all times, and so there is a minor irritation when that is not the case, <b>but once you get past that minor irritation</b>, the fact of the matter is that 98 percent of the time we want our systems to work they're actually working, and if there are problems and you call the help line or we have, in the case of the computers, we have the folks in the computer center over here, and those individuals are just <b>extremely responsive. They're really good.</b> And that doesn't mean they can always solve every problem, but I have had <b>great luck</b> in getting people to try to help me solve problems, and when the problem cannot be solved, whether it's a hardware problem or a software problem, there is somebody who will work and continue to work to try to get that fixed. So I think it's actually, <b>honestly, I just have no complaints</b> about them."</i>	<b>Positive affect / emotion</b>
25	<b>Circumvention of IS security</b>	<i>"I have like <b>five or six passwords</b> that I use pretty <b>consistently</b>. And this is probably not the best security practice but that's what I do. <b>And then I kind of rotate them.</b>"</i>	<i>"So, if we send mass emails, we have to go through the PHEI CMS system, <b>the one that they built themselves. It's their content management system for the web</b>, but we have to use that to do our mass emails. We would like to not do that because we <b>can't track anything other than how many people clicked on the links</b>. And we <b>don't know who</b> those people were or <b>anything about them</b> or how many links got clicked on or <b>how many clicks there were on a link</b>. And so <b>we're not allowed to use any outside email vendor</b> to do that service for us ... It's <b>hard to take data and make decisions here; it really is because the data's just not available.</b>"</i>	<b>Software-defined business decisions &amp; limitations on choices</b>
26	<b>Avoidance of IS</b>	<i>"<b>I haven't used it since there's a double authentication.</b> I don't want to use it any more than what I have to. <b>I'd use it more if it was easier for me.</b>"</i>	<i>"They pretty much have been able to help when you call. Now one of the, I don't think they can—I guess they can log into your computer. And look and see what you're seeing, to be able to fix the problem, and so I'd say <b>I've had really good experiences with them.</b> They are helpful. Yes, and they haven't, I mean, if they have to call me back, they call me back. I mean, it's <b>not two days or three days away, they call you back that day.</b> They find out the answer and then call you back."</i>	<b>Positive Affect/ Emotion</b>
27	<b>Avoidance of IS</b>	<i>"<b>I don't think I ever used my VPN from abroad</b> [outside the country]. It might suck my time if facing troubles with double authentication, contacting IT helpdesk, and all of that."</i>	<i>"PHEI does a pretty good job I think of having a fairly high level of security but <b>also making it fairly user friendly</b>. So with the VPN, you have to do the two factor authentication, then for the most part everything is handled through [name of single sign on system], and I guess that's the way you would pronounce that, but <b>that's really quite nice. So you have all these multiple entry points into a variety of different software tools</b> or places where you can go and do the things you need to do, <b>but it's through a unitary log-in ID and password, so that's kind of nice.</b> So I'm accessing everything from very simple email to, you know, I access financial data, personnel data, so a variety of different kinds of data and it <b>always is very easy for me.</b>"</i>	<b>Enhanced Productivity</b>

28	<b>Circumvention of IS security</b>	<i>"You can basically <b>just go change your password three times and go back to your same password.</b>"</i>	<i>"The password policy at PHEI says that you can write the passwords on a piece of paper but you need to keep it safe physically...<b>What, I'm going to always be near where I've locked up my password?</b>"</i>	<b>Time inefficiency</b>
29	<b>Avoidance of IS</b>	<i>"It seemed like every time I went back into it [VPN], it changed. It looked different. It changed the way it did it. It was asking me to put in a different password. I was always having to go online and read the rules to use it again. <b>I just stopped</b>, and just said it would be more productive for me to do it at work where I don't spend all the time getting that set up to use it than trying to use it at home. <b>I quit using it ...</b> I used to be the one who could explain to everybody how to do it at home. Now I don't even know how. <b>I don't think anyone in our office uses that to answer questions at home ...</b> It just got that much more complicated to do."</i>	<i>"I would say I used to, like in the '80s, be really up on everything. Back then, you could be. I tried to stay up on everything. Now working, I don't have as much time to do the research on it and everything. <b>I do appreciate all the things [IT Security team] they're doing to try to protect us, protect our computers and all.</b> I think they try to keep it as simple as possible."</i>	<b>Sense of security and privacy</b>
30	<b>Circumvention of IS security</b>	<i>"Do we really need as much security as they're telling us we need? I don't have details of that. <b>I try to stay under the radar with this program we use so they don't come after me</b>, since it was implemented with PHEI's support, but implemented before some of these extra security layers have been added."</i>	<i>"What <b>we don't have is the sophistication of automated marketing campaigns</b> and things because those are extra security features that I can't get through PHEI."</i>	<b>Software-defined business decisions</b>
31	<b>IS Adaptive behavior</b>	<i>"I'm not saying don't ever question, but when it comes to things like this, <b>if you have a problem with this, why are you working here?</b> We keep our information more secure than the government does, and I'm happy with that."</i>	<i>"I'm not saying don't ever question, but when it comes to things like this, if you have a problem with this, why are you working here? We keep our information more secure than the government does, <b>and I'm happy with that.</b>"</i>	<b>Positive affect / emotion</b>
32	<b>IS Adaptive behavior</b>	<i>"With the majority of our databases that we subscribe to they do go through <b>review process</b> before we subscribe to them so I think that they are looked at and made sure there's not anything that will cause a problem with the university."</i>	<i>"A lot of people look at the line there what the email's about, they probably think 'oh yeah, there's another one of those emails about something' and they'll go ahead and delete it. And I imagine there is a pretty good amount of that going on even if it's something going out from ITS that might be <b>something you need to know about. If there's a new computer virus going around and they're trying to make people aware of it</b> so you don't click on something coming to you in your email and you delete that email and don't look at it to see that, <b>then there you are without that information.</b> If that comes into your email and you do what you should be doing then you are in trouble. I know that has happened in the last year or two because somebody that I happened to know did that. He didn't read the email and when a virus came and he clicked on it and there your computer is infected ... I just know he felt foolish about what he had done because he said 'I should have known better' and he had to take his computer and get it cleaned and get the virus off of it, <b>but I think it was pretty well contained.</b>"</i>	<b>Sense of security and privacy</b>

## About the Authors

**Puzant Baloizian** is an assistant professor of computer information systems at James Madison University. His research focus is primarily on the impacts of organizational factors on individual user behaviors in the context of information security and privacy and addressing security policy compliance and violation. He has published in *Journal of Intellectual Capital*, *Journal of Enterprise Information Management*, *The Data Base for Advances in Information Systems*, *Journal of Computer Information Systems*, *Vaccines*, *Proceedings of the International Conference on Information Systems*, and other outlets. ORCID: 0000-0002-8410-1188

**A. J. Burns** is an assistant professor in the Stephenson Department of Entrepreneurship & Information Systems at the E. J. Ourso College of Business at Louisiana State University. He received his DBA from Louisiana Tech University and completed a postdoc at Vanderbilt University. His research focuses on organizational and behavioral information security. His research has been published in *Information Systems Research*, *Journal of the Association for Information Systems*, *European Journal of Information Systems*, *Decision Sciences*, and other outlets. ORCID: 0000-0001-8222-4144

**Dorothy E. Leidner** is the Leslie H. Goldberg Jefferson Scholars Foundation Distinguished Professor of AI Ethics at the University of Virginia. She is a LEO and a Fellow of the Association of Information Systems. Dorothy received her PhD in information systems from the University of Texas at Austin and holds an honorary doctorate from Lund University. She is a professional research fellow with Deakin University in Australia and a visiting professor with the University of Gothenburg, Sweden. Her current research focuses on the ethics of personal data digitalization. ORCID: 0000-0002-7159-6273

Copyright © 2023 by the Association for Information Systems. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and full citation on the first page. Copyright for components of this work owned by others than the Association for Information Systems must be honored. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers, or to redistribute to lists requires prior specific permission and/or fee. Request permission to publish from: AIS Administrative Office, P.O. Box 2712 Atlanta, GA, 30301-2712 Attn: Reprints, or via email from [publications@aisnet.org](mailto:publications@aisnet.org).