Which are the Most Effective Measures for Improving Employees' Security Compliance?

Completed Research Paper

Martin Kretzer
University of Mannheim
Mannheim, Germany
kretzer@es.uni-mannheim.de

Alexander Mädche
University of Mannheim
Karlsruhe Institute of Technology
Germany
maedche@es.uni-mannheim.de

Abstract

Employees' compliance behavior with information security policies has been extensively researched yet. In particular, many studies identified and explained measures that increase employees' security compliance such as trainings and controls. Although the identification and explanation of these measures is valuable for managers, these findings are insufficient. Since managers need to balance limited resources, they need to be able to prioritize and invest in the most effective measures for improving employees' security compliance.

Therefore, to complement extant research, we survey 332 employees in an organization that has established 15 security measures. Our results provide managers with a quantitative assessment of these 15 security measures. Furthermore, we discuss the implications of our findings and give recommendations for managers. In addition, our results may also be valuable for theorists because, e.g., we show and explain which type of information security agent is most effective.

Keywords: Information security/privacy, training, data security, change agent, compliance behavior.

Introduction

The latest SIM IT Key Issues study revealed security as the number one "worrisome technology for IT leaders" (University of Minnesota 2014). It is well understood that security attacks increasingly cause fatal consequences. For instance, in 2014 attackers were able to obtain login credentials from eBay employees and copy 233 million personal user records (DataBreaches.net 2014; Forbes 2014). Further recent and popular examples include, e.g., an attack on the bank JPMorgan Chase in which 80 million customer records were stolen over a period of three months (Bloomberg 2014; Reuters 2014) and an attack on the retailer Target in which 70 million customer records were stolen – including 40 million credit and debit card numbers (Target 2015). These security attacks lead to the question why extant research has not yet been able to provide effective guidance to organizations for improving information systems (IS) security.

For many years, IS security research emphasized technology-based solutions to fight IS security threats (e.g., Spears and Barki 2010; Whitman 2004). Although these types of solutions improve security (Straub 1990), they have been criticized for being insufficient (Bulgurcu et al. 2010; Dhillon and Backhouse 2001; Siponen 2005a), because they neither investigate users as a problem (Stanton and Stam 2006; Whitman 2008), nor users as an asset to fight attacks (Siponen 2005b; Spears and Barki 2010), nor any other socio-organizational predictors of IS security (Boss and Kirsch 2007; Siponen et al. 2007). Therefore, the IS security discipline started to investigate socio-organizational predictors such as employees' compliance behavior with information security policies (ISPs; e.g., Bulgurcu et al. 2010; Dittes et al. 2015; Herath and Rao 2009; Siponen and Vance 2010; Siponen et al. 2010).

However, the emphasis of extent research has been on revealing and explaining antecedents of employees' compliance behavior with ISPs. As a consequence, practical insights for managers have been limited to recommendations based on theoretical findings. That is, many studies focus on specific measures for improving security compliance behavior. For instance, Johnston et al. (2015) recently focused on sanctions and found that sanctions enforced by the organization have a smaller influence on compliance behavior than informal sanctions imposed by peer groups. From this the authors concluded that managers should "encourage the development of an environment that includes informal gatherings that could facilitate the use of informal sanctions" (Johnston et al. 2015, p. 130). However, the authors did not compare the effectiveness of their recommendations to alternative approaches that do not use sanctions. Another example in which the authors focus on a specific class of security measure is the study of Puhakainen and Siponen (2010). In their study, the authors design and develop effective security trainings. As a consequence, their implications for practitioners focus on using specific training methods such as "methods and ideas that enable learner's systematic cognitive processing of information" (Puhakainen and Siponen 2010, p. 775) but are not compared against potential alternative security measures such as controls or sanctions.

Besides studies focusing on specific security measures, several IS security scholars have reviewed and summarized potential security measures. For instance, Tu and Yuan (2014) reviewed and identified dependencies between critical success factors for effective information security management. However, their work does not compare the reviewed security measures according to their effectiveness. Similarly, D'Arcy et al. (2014) reflected on measures that influence employees' security behavior. However, their summary of measures for improving employees' security behavior also does not compare the effectiveness of these measures.

Without any doubt, the identification and explanation of measures for improving employees' security behavior is valuable, interesting, helpful and important for managers. However, we argue that *identification* and *explanation* of security measures are not sufficient. Managers also need to be able to *relate* alternative measures to each other. As implied by the word *management* itself, managers need to make decisions about controlling and allocating limited available resources efficiently and effectively (Merriam-Webster 2015). Organizations cannot simply invest into and implement all recommended security measures because their resources (mostly financial capital and human capital) are limited. Therefore, managers need to focus their investments and prioritize the most promising measures for improving their employees' compliance behavior with ISPs. To aid managers with this, we investigate the following research question: *Which measures are perceived by employees to be most effective for improving employees' compliance behavior with information security policies?*

To address this research question, we review and synthesize extant literature by developing a framework of measures for improving employees' compliance behavior with ISPs. Subsequently, we empirically investigate an organization who implemented 15 distinct security measures three years before the study was conducted. First, we show how the implemented security measures map to our literature-based framework. After that, we ask employees to assess the effectiveness of the 15 security measures based on their personal experiences.

The remainder of this article is structured as follows. Section 2 presents the results of our literature review and develops a framework of measures for improving employees' compliance behavior with ISPs. Subsequently, section 3 introduces our survey and the field partner at which the survey was conducted. We also explain how the different security measures are implemented at the field partner. After that, section 4 shows the results of the survey and section 5 discusses their value, novelty and limitations. Finally, section 6 concludes this article and gives recommendations for managers.

Literature Review

The objective of our work is to quantify and rank the effectiveness of measures for improving employee's compliance behavior with ISPs. Such a quantitative ranking is valuable for organizations because it allows managers to balance and prioritize their investments.

We first review literature and synthesize a framework that describes different classes of security measures to increase employees' compliance with ISPs (Webster and Watson 2001). Since other scholars reviewed information security measures previously (D'Arcy and Herath 2011; Puhakainen and Siponen 2010; Tu and Yuan 2014) we focused on one popular database for our review, i.e., AISeL, and conducted an extensive backward search based on the identified articles. We conducted two rounds of literature search. In the first round, we used the search string "security" in combination with the keyword "security". This yielded 118 hits. We scanned the titles and abstracts and downloaded 18 articles of which 10 turned out to recommend specific security measures. Most of the articles that we omitted focused on technical design principles for increasing information security or contrasting security and privacy. In the second round, we used the search string "compliance behavior" (without any limiting keyword). However, as this search string resulted in 1614 hits, we narrowed the search down to journal articles. Furthermore, since similar literature reviews were conducted in 2010 and 2011 (e.g., D'Arcy and Herath 2011; Puhakainen and Siponen 2010), we narrowed the search to publications within 2011-2015. This yielded 122 hits. We ignored articles that we already scanned in the first round and, based on titles and abstracts, downloaded 8 additional articles of which 5 turned out to recommend specific security measures. Most of the articles that we omitted in the second literature search round focused on process management or already resulted from the first round. Finally, we checked for additional articles referenced in the relevant articles (backward search). This yielded further 26 articles. Thus, our review was based on 41 articles in total. Appendix A provides a list of all reviewed articles.

Building on the identified set of articles, we developed a framework that describes six *classes* of security measures: trainings, informational materials, controls, security agents, sanctions, and incentives. Organizations may instantiate these classes with specific security measures. For instance, organizations may establish specific types of trainings (Puhakainen and Siponen 2010) or introduce specific types of sanctions (D'Arcy and Herath 2011; Johnston et al. 2015). Appendix A provides a concept matrix that indicates which class of security measure has been examined and/or discussed in a certain article.

Trainings. One of the most studied approaches for improving employees' compliance with ISPs are trainings (Puhakainen and Siponen 2010). Trainings typically incorporate a pedagogical orientation as a primary means of improving user compliance with ISPs. A comprehensive literature review specifically focusing on IS security trainings is provided by Puhakainen and Siponen (2010).

Informational Materials. As a second class we identified informational materials. These are mostly tangible assets which illustrate correct compliance behavior and typical mistakes. These include, for instance, posters (Rudolph et al. 2002), leaflets (Hadland 1998; Murray 1991; Peltier 2000, 2002; Spurling 1995), and gadgets (Rudolph et al. 2002). However, also intangible assets such as e-mails may be used as a medium for spreading knowledge about ISPs and security compliance behavior (Murray 1991; Spurling 1995; Thompson and von Solms 1997).

Controls. Monitoring compliance behavior (Lampe et al. 2013) and conducting regular controls are a common measure for improving employees' compliance behavior (Rudolph et al. 2002; Perry 1985; Kwon and Johnson 2011). Organizations have responded to the growing list of security threats through a combination of technical, administrative, and physical controls (D'Arcy and Herath 2011). Depending on their severity, some controls should be conducted by external parties while other controls may be conducted by employees themselves (Johnston et al. 2010).

Security Agents. Security agents are internal employees who specialize in disseminating knowledge about ISPs in their organization (Peltier 2000, 2002; Perry 1985). Besides deep knowledge about security-related topics, they also have strong knowledge about their colleagues' tasks and work routines. Although every organization may define the role of a security agent differently, several characteristics can be highlighted. For instance, security agents typically train and support colleagues as well as persuade them to comply with ISPs (Johnston et al. 2010; Warkentin et al. 2011). They may also maintain and control IS user authorizations and define to what degree specific business data needs to be protected.

Sanctions. As a fifth class of security measure for improving employees' compliance with ISPs, we identified the use of sanctions (Liang et al. 2013; Siponen et al. 2007; Straub 1990). Deterrence-based approaches argue that fear of sanctions determines whether employees comply with the policies (Akers and Sellers 1994; Johnston et al. 2015; Straub 1990; Siponen et al. 2007). According to avoidance motivation theorists, individuals are generally motivated to avoid threats (Liang and Xue 2010). However, extant research provides inconsistent and partly contradictory findings regarding the use of sanctions in the context of compliance with ISPs (e.g., D'Arcy and Herath 2011). A detailed review dealing with sanctions in the information security area is provided by Johnston et al. (2015).

Rewards. Similarly to sanctions, literature found that rewards (e.g., financial incentives or promotions) also increase employees' IS security behavior (Liang et al. 2013). While sanctions are perceived as costs of non-compliance by employees, rewards are perceived as benefits of compliance (Bulgurcu et al. 2010). However, results regarding the effectiveness of rewards have been ambiguous. Multiple studies have not been able to statistically confirm a benefit of rewards on employees' compliance behavior with ISPs (e.g., Boss and Kirsch 2007; Pahnila et al. 2007). For instance, Bulgurcu et al. (2010) studied incentives and found that rewards cause statistically significant improvements in employees' compliance behavior with ISPs if employees are informed about the rewards in advance. The announcement of the possibility to be rewarded increases employees' intrinsic motivation to comply and, thus, improves their security behavior (Bulgurcu et al. 2010).

To conclude our review, we identified six classes of measures for improving employees' compliance behavior with ISPs. In the following, we will present our study setting and explain how our field partner implemented the identified classes of security measures.

Research Method

Study Setting

Our study was conducted within the corporate purchasing department of *ALPHA* (pseudonym). *ALPHA* is a large, multinational engineering company with its headquarters in Germany. Alpha is a leading supplier of numerous technologies and has more than 100,000 employees working in more than 100 countries. *ALPHA* was apt for this study, because security-related topics are taken very seriously at *ALPHA*. Specifically, *ALPHA* already had 15 distinct security measures in place that could be mapped to our framework. Thus, employees at *ALPHA* were able to compare and assess the effectiveness of different measures for improving employees' compliance behavior with ISPs based on their personal experiences.

In 2009, *ALPHA* centralized most of its purchasing activities in the corporate purchasing unit *PURCHASER* (pseudonym). *PURCHASER* was particularly suited for this study, because, as *ALPHA*'s purchasing unit, it initiates the highest cash outflow and, thus, represents one of the most important business units for implementing high information security standards. *PURCHASER* employs 3'000 employees in its German headquarters and further 3'000 employees in Australia, Asia, Europe, North America, and Latin America. Overall, these 6'000 employees manage a cumulated purchasing volume of approximately $20 billion each year. Thus, it is crucial for *ALPHA* that all employees at *PURCHASER* comply with the defined ISPs because non-compliant behavior can have fatal consequences. For instance,

if details about contracts with suppliers would "get out", this would severely weaken *PURCHASER's* position in future negotiations. Similarly, if unauthorized users would not only be able to access information but even be able to execute transactions, huge financial losses could be generated due to the budget that *PURCHASER* manages.

Importantly, at *PURCHASER* many departments already established a security agent who informs fellow colleagues about new information security trends and developments. These security agents consult and train their colleagues and create and maintain detailed security concepts for all departments. At *PURCHASER* each department has a department security concept which, for instance, defines employees' business roles, assigns technical authorizations to specific business roles, and defines sensitivity and criticality of data and applications. However, as not all departments had introduced a security agent yet, our study focused on those departments that had a security agent for at least three months when the study was conducted. Combined these departments employed 2'300 employees. Most of them had a security agent for approx. three years because they introduced their security agent right away when *PURCHASER* itself was established as a business division within *ALPHA*.

In the following, we instantiate the security measure classes of our framework with the specific security measures implemented at *PURCHASER*. After talking to *PURCHASER's* senior security manager and observing two individual trainings and two training workshops, we distinguished 15 specific information security measures for improving employees' compliance behavior with ISPs that were already implemented at *PURCHASER*. Furthermore, since we focused on measures that employees have already experienced, employees at *PURCHASER* were able to compare and assess the effectiveness of those measures in relation to each other.

Trainings. *PURCHASER* differentiates five training measures: individual trainings (with regards to personal training sessions with a trainer), group trainings and workshops (Thompson and von Solms 1997), mandatory trainings (e.g., if employees need to participate in a specific training module once a year; Boss and Kirsch 2007; Mitnick 2002), web-based training programs (Cox et al. 2001), and training presentations provided via global web conferences.

Informational Materials. *PURCHASER* uses four types of informational material in order to increase awareness about ISPs and to give practical examples about good and bad behaviors. Specifically, at *PURCHASER* large posters are pinned to many office walls. Furthermore, leaflets are frequently handed out to employees personally and deposited at frequently visited corridors. In addition, *PURCHASER* uses several gadgets to increase awareness about security-related topics. These include, for instance, coffee cups, mouse pads, pens, key holders. Also, e-mails are sent around by security agents weekly or bi-weekly in which the security agent summarizes his or her most recent observations.

Controls. A specific type of controls are audits (Kayworth and Whitten 2010). Audits are official examinations of employees' compliance behavior with existing ISPs. At *PURCHASER*, audits are conducted by an *external* auditor from another organization or institution. *PURCHASER* distinguishes audits from self-checks that are conducted by an *internal* auditor – typically the information security agent. Furthermore, *PURCHASER* distinguishes audits based on who sponsors and initiates them. This is important because self-checks and audits are sponsored and initiated by executives and managers and, thus, potentially biased. To mitigate this bias, *PURCHASER* also introduced controls sponsored and initiated by the revision department. The specialty of these controls is that the results of these controls are not reported to the executive board but directly the supervisory board.

Security Agents. *PURCHASER* differentiates between full-time security agents and part-time security agents. While a full-time security agent works only in his or her role as a security agent, a part-time security agent only works in the role of a security agent for a specific percentage of his or her working hours – typically 10%-20%. Importantly, full-time security agents represent the security agent for multiple departments. Conversely, part-time security agents are primarily "ordinary" employees within a specific department and "only" work in the role of a security agent for that specific department. As a consequence, part-time security agents typically have less knowledge about security-related topics but a better understanding about their colleagues' work routines than full-time security agents. Furthermore, a part-time security agent only reports to his or her own department's head, while a full-time security agent reports to multiple department heads.

Sanctions. At *PURCHASER*, security agents were able to assign sanctions to employees for repeated non-compliance. These sanctions included increasing the frequency of mandatory trainings for specific employees or assigning additional training sessions to them.

Rewards. We excluded rewards from this study, because employees at *PURCHASER* did not receive specific rewards for complying with ISPs.
Table 1 provides an overview of the implemented security measures at *PURCHASER*.

Table 1. Overview of Security Measures at *PURCHASER*.

Class	Security Measure	Description
Trainings	Individual trainings	One employee receives personal instructions by a security trainer. No further employees are participating in this training session.
	Group trainings and workshops	Multiple employees receive instructions during the same training session. These training session are conducted via in-person conferences/presentations.
	Mandatory trainings	Ongoing trainings at a specified frequency, e.g. once a year
	Trainings via global web conferences	A training session that is conducted by a human trainer via global web conferences. It is typically shared across remote locations using the internet.
	Web-based trainings	A training program in which the employee participates (e.g., multiple choice questions for testing his/her knowledge about the ISPs. The employee does not interact with a human trainer.
Informational materials	Posters	A large printed picture or notice which can be pinned to a wall
	Leaflets	Flyer and newsletters which provide information about ISPs
	Gadgets	Trinkets and giveaways providing information about ISPs (e.g., cups, pens, mouse pads)
	Information via e-mails	Frequent reminders providing information about ISPs
Controls	Self-checks	Examination of compliance with ISPs through an internal auditor
	ISP-audits	Official examination of compliance with ISPs by an external auditor
	Checks by the revision department	Official examination of compliance with ISPs through an employee of the revision department
Security agents	Full-time security agents	An employee who acts as consultant and trainer regarding security topics and performs security-related tasks (e.g. user authorization). A full-time security agent can typically take care of multiple departments.
	Part-time security agents	Similar to a full-time security agent. However, since a part-time security agent has less time resources, he or she typically can only take care of one department.
Sanctions	Sanctions for non-compliance	Punishments for individuals that do not comply with ISPs

Survey

To quantify the perceived effectiveness of different measures for improving security behavior, we administered a survey at *PURCHASER*. The survey asked participants to assess the effectiveness of each of the 15 measures for improving security behavior on a five-point Likert-type scale ranging from "not effective" (1) to "very effective" (5). The link to the survey was distributed to participants via e-mail.

Furthermore, the survey ran on a specific, organization-internal survey server. This server had previously been approved by experts from IT and all of *PURCHASER's* worker's councils. These approvals were important because they assured that (1) participants' were identified by the survey server as internal employees, (2) participants could not participate multiple times, and (3) data about participants was stored encrypted, protected, and separated from the assessments of the security measures. Consequently, we were able to guarantee anonymity to employees, while simultaneously keeping employees from participating more than once.

Data collection took place during November and December 2012. We reached out to all employees at *PURCHASER* who were assigned to a department that already established a security agent for at least three months. Of 2,300 contacted employees, 379 employees participated in the survey. This led to a response rate of 16.5%. However, five employees did not completely fill out the survey and therefore their answers were ignored. In addition, responses of 42 participants were ignored because these participants stated that they would not know the information security agent assigned to them and/or would not have had at least one information security training at *PURCHASER* within the last three years. We removed their responses in order to assure that all participants were able to assess the security measures for improving security behavior based on personal experiences. Assessments based on personal experiences have shown to lead to more reliable results than assessments based on expectations (Brown et al. 2014). Eventually, data analysis was based on 332 usable responses. Table 2 summarizes respondent demographics. Since respondent demographics are very similar to *PURCHASER's* overall employee demographics, we assume that this survey was not affected by non-response bias. The only difference was the high ratio of information security agents who participated in the study. However, as our survey was particularly interesting for information security agents, the high response rate within the group of information security agents was not surprising. Therefore, we decided to analyze the assessments for information security agents and non-information security agents separately.

Table 2. Respondent Demographics.

		Absolute	**Relative**
Usable responses		**332**	**100%**
Selected survey language	English	154	46%
	German	178	54%
Years having worked at *ALPHA*	Less than 1	60	21%
	1-3	71	25%
	3-7	47	17%
	More than 7	105	37%
	Not specified	*49*	*n.a.*
Department	Supporting business function	158	54%
	Manufacturing	34	12%
	IT	44	15%
	R&D	27	9%
	Other	29	10%
	Not specified	*40*	*n.a.*
Job role	Employee	228	86%
	Manager	37	14%
	Not specified	*67*	*n.a.*
"I am an information security agent."	Yes	72	22%
	No	260	78%

Results

Measures for improving employees' compliance behavior with ISPs were assessed on a five-point Likert-type scale ranging from "not effective" (1) to "very effective" (5). Table 3 shows the means and standard deviations of all measures. Besides overall assessments, we differentiate between assessments by employees working as information security agents and employees who are not working as information security agents. This differentiation is reasonable, because (1) information security agents have significantly deeper expertise in information security and privacy topics, (2) information security agents not only participate in security trainings but also provide trainings to their fellow colleagues, and (3) the assessment of the effectiveness of information security agents would likely depend on whether the person who makes the assessment is himself or herself working as an information security agent.

Regarding differences between means of various measures, significance depends on the measures' standard deviations. The higher a measure's standard deviation, the less significant a given difference to another factor will be. Our significance tests revealed that (1) a difference between two means of at least 0.11 is significant at the 5% significance interval, (2) a difference of at least 0.15 is significant at the 1% interval, and (3) a difference of at least 0.19 is significant at the 0.1% interval (all two-tailed and based on the average standard deviation of 1.04).

Results demonstrate that overall information security agents and their fellow colleagues assess the effectiveness of security measures for improving employees' compliance behavior in relation to each other similarly. However, information security agents tend to rate the measures' effectiveness greater (except for the measure *part-time security agents*) than employees who are not information security agents. Figure 1 visualizes the results graphically.

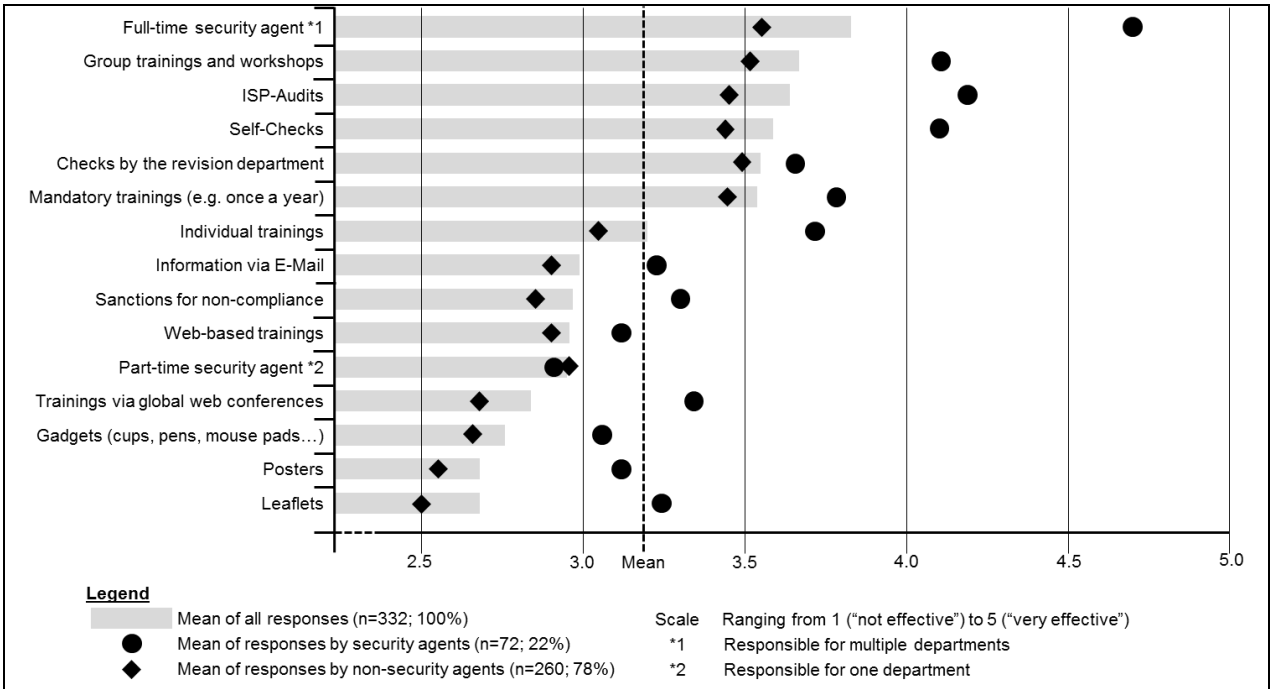

Figure 1. Results.

Table 3. Perceived Effectiveness of Measures for Improving Employee's Compliance Behavior with ISPs.				
Measure	**Class of Measure**	**All Mean (Std. Dev.)**	**Information Security Agents Mean (Std. Dev.)**	**Non-Information Security Agents Mean (Std. Dev.)**
Full-time security agent *1	Security Agents	3.83 (1.11)	4.76 (0.46)	3.57 (1.10)
Group trainings and workshops	Trainings	3.67 (0.97)	4.17 (0.78)	3.53 (0.97)
ISP-Audits *2	Controls	3.64 (1.06)	4.24 (0.84)	3.47 (1.05)
Self-Checks	Controls	3.59 (0.95)	4.15 (0.84)	3.44 (0.92)
Checks by the revision department	Controls	3.55 (1.01)	3.71 (0.95)	3.51 (1.02)
Mandatory trainings (e.g., once a year)	Trainings	3.54 (0.97)	3.85 (0.97)	3.46 (0.96)
Individual trainings	Trainings	3.20 (1.10)	3.76 (0.98)	3.05 (1.09)
Information via E-Mail	Inform. Materials	2.99 (0.98)	3.28 (0.95)	2.91 (0.97)
Sanctions for non-compliance	Sanctions	2.97 (1.11)	3.35 (1.14)	2.86 (1.08)
Online trainings	Trainings	2.96 (0.97)	3.15 (0.92)	2.91 (1.00)
Part-time security agent *3	Security Agents	2.95 (1.14)	2.93 (1.11)	2.96 (1.15)
Trainings via global web conferences	Trainings	2.84 (0.99)	3.39 (0.94)	2.69 (0.96)
Gadgets *4	Inform. Materials	2.76 (1.11)	3.11 (1.15)	2.67 (1.07)
Posters	Inform. Materials	2.68 (1.05)	3.15 (1.14)	2.55 (0.99)
Leaflets	Inform. Materials	2.68 (1.07)	3.28 (1.04)	2.51 (1.01)
Average		**3.19 (1.04)**	**3.62 (0.95)**	**3.07 (1.02)**
N		**332**	**72 (22%)**	**260 (78%)**

*1: Responsible for multiple departments; *2: Information Security and Privacy-Audits; *3: Responsible for one department; *4: E.g., cups, pens, mouse pads.

Furthermore, we computed correlations between measures in order to check whether measures of a specific class according to the framework are evaluated similarly. Table 4a and Table 4b summarize all correlations between the identified measures for improving compliance behavior. Surprisingly, only measures of the class *informational material* and the class *controls* correlate with other measures of the same class. This indicates a need for further research which examines why the effectiveness of measures that belong to the same class (especially trainings) may be perceived differently.

Table 4a. Correlations									
Measure		**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1	Full-time security agent	1.00							
2	Group trainings and workshops	0.26***	1.00						
3	ISP-Audits	0.21***	0.24***	1.00					
4	Self-Checks	0.20***	0.17**	0.22***	1.00				
5	Checks by the revision department	0.17**	0.19***	0.38***	0.30***	1.00			
6	Mandatory trainings (e.g., once a year)	0.07	0.12*	0.18***	0.02	0.13*	1.00		
7	Individual trainings	0.20***	0.10	0.21***	0.10	0.16**	0.09	1.00	
8	Information via E-Mail	0.10	0.09	0.13*	0.10	0.04	0.17**	0.10	1.00
9	Sanctions for non-compliance	0.11*	0.14*	0.28***	0.12*	0.29***	0.14*	0.17**	0.13*
10	Online trainings	0.04	0.02	0.10	0.15**	0.00	0.12*	0.13*	0.07
11	Part-time security agent	-0.02	0.11*	0.07	-0.01	0.09	0.06	0.11*	0.05
12	Trainings via global web conferences	0.20***	0.16**	0.20***	0.14*	0.16**	0.20***	0.18***	0.15**
13	Gadgets	0.06	0.04	0.04	0.17**	0.01	0.20***	0.12*	0.18***
14	Posters	0.06	0.17**	0.20***	0.16**	0.23***	0.27***	0.20***	0.26***
15	Leaflets	0.10	0.22***	0.22***	0.10	0.14*	0.24***	0.20***	0.29***

Significance (two-tailed): *0.05; **0.01; ***0.001.

Table 4b. Correlations								
Measure		**9**	**10**	**11**	**12**	**13**	**14**	**15**
9	Sanctions for non-compliance	1.00						
10	Online trainings	0.08	1.00					
11	Part-time security agent	0.03	0.01	1.00				
12	Trainings via global web conferences	0.15**	0.33***	0.08	1.00			
13	Gadgets	0.14*	0.07	0.09	0.14*	1.00		
14	Posters	0.20***	0.22***	0.14*	0.31***	0.36***	1.00	
15	Leaflets	0.09	0.16**	0.14*	0.25***	0.29***	0.56***	1.00

Significance (two-tailed): *0.05; **0.01; ***0.001.

Discussion

Implications

In our survey, we asked employees to assess effectiveness of measures for improving employees' compliance behavior with ISPs. The results are interesting from an academic as well as a practitioner perspective, because they show for which classes the identified measures actually correlate with one another and what the most and least effective measures for improving compliance with information security policies are. This is important, because if measures do not correlate with other measures of the same class, managers need to be particularly careful when selecting the measures they want to invest in. This is consistent with extant literature which found that, for some classes of security measures, there exist measures that significantly improve employees' compliance with ISPs (Bulgurcu et al. 2010) as well as measures for which effects could not be confirmed (Boss and Kirsch 2007; Pahnila et al. 2007).

Overall, our findings indicate that full-time security agents are perceived by far as the most effective measure for improving security behavior. They are followed by controls, group trainings and mandatory trainings which also are significantly more effective than the average measure. Besides, further measures, i.e., information via e-mail, sanctions, and online trainings, are still perceived as being more effective than part-time security agents. This is surprising, because one could have assumed that part-time security agents would be similarly effective as their full-time colleagues. Finally, trainings via web-conferences, gadgets (such as cups, pens, and mouse pads), posters, and leaflets represent the least effective measures for improving information security behavior.

Furthermore, we found that employees who are working as information security agents tend to assess effectiveness of security measures in general higher than employees who are not working as information security agents. However, when looking at the assessments of single measures in relation to each other, the assessments by information security agents and non-information security agents are quite similar. This indicates a general selection bias. However, there are also a few security measures of which the effectiveness in relation to other security measures is experienced differently by information security agents and non-information security agents. In particular, information security agents experienced that the effectiveness of full-time security agents is much higher than the effectiveness of any other measure (difference of 0.61 to the second highest factor!). In addition, information security agents themselves perceived part-time information security agents as the least effective measure of all. In contrast, their colleagues who are not working as security information agents, assessed their effectiveness "only" a little below the average.

This fact, that security agents rate all measures' effectiveness greater than employees who are not security agents except for the measure part-time security agent, is very interesting. While a selection bias may be a reason why security agents rate all measures' effectiveness greater, there is no obvious explanation why part-time security agents are an exception to this bias. However, based on our observations and experiences from working at *PURCHASER* (the first author worked full-time at *PURCHASER*'s information security department for six months), we believe that the primary reason why information security agents rate part-time security agents relatively low is, that part-time security agents frequently are faced with deadlines from other daily work. As a consequence, part-time security agents tend to work less hours in their role of information security agents than they should, because they need to free up some time in order to be able to meet deadlines in other roles. For instance, if part-time security agents are simultaneously project team members who need to complete certain tasks before a specific date, they tend to reduce their work as a security agent. Thus, a potential explanation for why security agents rated full-time security agents very high and part-time security agents surprisingly low, may be that they wanted to express their dissatisfaction with the little amount of time that part-time security agents actually have left for working in their security agent role.

Besides, the effectiveness of posters and leaflets is experienced differently by employees working as security agents and employees who are not working as security agents, too. Specifically, information security agents seem to overestimate the effectiveness of posters and leaflets. However, we believe that this may be caused by a selection bias because the difference is rather moderate and we did not find any reason at *PURCHASER* that would explain this difference.

Another interesting point is that all measures of the identified classes *informational materials* and *controls* correlate with measures from the same class at the 0.1% significance level. Since our results do not indicate a similar effect for the classes *trainings* and *security agents*, further research should focus on these two classes. Theories and frameworks could be developed that explain why some measures appear to be much more effective than other measures although they may be aggregated to the same class of security measures.

To our knowledge, previous research merely identified security measures. No study yet attempted to quantify and compare their effectiveness in relation to each other. Hence, the results of this study are particularly interesting for managers, because the results enable managers to prioritize, balance and optimize their financial resources and human resources. In particular, we infer five specific recommendations for managers focusing on how to allocate limited resources below.

Limitations and Future Research

Our work is subject to several limitations. First, we asked employees to assess the effectiveness of the identified security measures based on their experiences. As a consequence, the assessments represent personal perceptions. Second, we focused on one organizational unit, i.e., *PURCHASER*. We selected *PURCHASER* as field partner for this study because focusing on *PURCHASER* and its context allowed us to instantiate the identified classes of security measures with concrete security measures that had been adopted and experienced by employees before the study was conducted (Johns 2006). However, future research should fill, and potentially enhance, our framework with concrete security measures in further settings. Finally, our review and framework of security measures is limited with regards to our literature search strategy. For instance, other search terms, literature databases, outlets, books etc. could have yielded different results. Nevertheless, although our framework may be complemented when reviewing or conducting further studies, we believe that the identified classes of security measures already encompass the large majority of security measures that are frequently implemented in organizations.

Conclusions and Recommendations for Managers

Our study focuses on developing a conceptual framework and a quantitative assessment of measures for improving employees' compliance behavior with ISPs. In particular, the study was conducted at *PURCHASER*. *PURCHASER* was apt for our study for several reasons: (1) security-related topics are taken very seriously, (2) 15 specific information security measures for improving employees' compliance behavior with ISPs were already implemented at *PURCHASER*, and (3) employees at *PURCHASER* were able to compare and assess the effectiveness of those measures in relation to each other. Upon our findings, we draw five recommendations for managers.

First, managers need to prioritize security measures in order to optimize resource exploitation. In particular, the greatest share of a security manager's budget should be invested in full-time security agents as they represent the most effective security measure for increasing compliance with ISPs. Since they work full-time on security-related topics, they are able to develop extensive ISP knowledge and thus serve as great advisors for their fellow colleagues. To the best of our knowledge, no prior studies have yet examined and compared the effectiveness of full-time security agents and part-time security agents. Furthermore, this is not a trivial finding, because advocates of part-time security agents typcially argue that part-time security agents have deeper understanding of their colleagues daily work routines and, thus, can better put themselves in their colleagues' position when training them. However, our results show that full-time security agents are perceived far more effective than part-time security agents and, thus, should be the preferred measure for improving employees' security behavior.

Second, consistent with our first recommendation, we infer that organizations should avoid establishing part-time security agents. Even regular e-mails, sanctions and online trainings are evaluated as being more effective in improving employees' compliance behavior than part-time security agents. In contrast to full-time security agents, part-time security agents do not have enough time resources to develop sufficient expertise in security-related topics. Furthermore, it is likely that part-time security agents might be tempted to use the time they should be working as security agents for working on tasks that are not, or only little, related to information security. For instance, if a part-time security agent is simultaneously a member of a project team, he or she might be tempted (and even pressured) to use his or her working

hours for working towards project completion instead of working towards improving employees' compliance with ISPs.

Third, besides full-time security agents, organizations should emphasize controls, group trainings and mandatory trainings as means for improving employees' compliance behavior. Controls, group trainings, and mandatory trainings are significantly more effective than the average security measure.

Fourth, trainings via web-conferences, gadgets (e.g., cups, pens, mouse pads), posters, and leaflets are not sufficient security measures and organizations should not rely on them. However, as they demand relatively small resources, they are suited as complementary measures for improving employees' compliance behavior with ISPs.

Fifth, managers need to be particularly careful when investing in security trainings because the effectiveness of different types of trainings varies significantly. As a consequence, managers should carefully consider concrete instantiations of a particular class of security measures before spending their budget. Based on our results, we particularly recommend group trainings and workshops.

Appendix A: Concept Matrix of Reviewed Literature

As explained in section 2 ("Literature Review"), we conducted a structured literature review in order to develop a framework which describes classes of measures for improving employees' compliance behavior with ISPs. Table 5 lists all identified articles and indicates to which of the classes each article is assigned.

Table 5. Concept Matrix of Reviewed Literature.

Article	Trainings	Informational Materials	Controls	Security Agents	Sanctions	Incentives
Johnston et al. (2015)					X	
D'Arcy et al. (2014)	X		X	X		
Glisson and Welland (2014)			X			
Tu and Yuan (2014)	X		X	X	X	
Lampe et al. (2013)			X			
Liang et al. (2013)			X		X	X
Ramachandran et al. (2013)	X					
Willison and Warkentin (2012)			X		X	
D'Arcy and Herath (2011)			X		X	
Karjalainen and Siponen (2011)	X					
Kwon and Johnson (2011)			X			
Warkentin et al. (2011)	X	X		X		
Xu et al. (2011)			X			
Bulgurcu et al. (2010)					X	X
Johnston et al. (2010)	X		X	X		
Kayworth and Whitten (2010)	X		X			
Liang and Xue (2010)			X		X	
Puhakainen and Siponen (2010)	X					
Siponen and Vance (2010)					X	

Table 5. Concept Matrix of Reviewed Literature.						
Article	**Trainings**	**Informational Materials**	**Controls**	**Security Agents**	**Sanctions**	**Incentives**
Siponen et al. (2010)					X	X
Heikka (2008)	X					
D'Arcy et al. (2009)	X		X			
Knapp et al. (2009)			X			
Boss and Kirsch (2007)					X	X
Siponen et al. (2007)					X	X
Siponen (2005a, 2005b)	X					
Mitnick (2002)	X					
Peltier (2002)	X	X				
Rudolph et al. (2002)	X	X	X			
Peltier (2000)	X	X				
Hadland (1998)	X	X				
Straub and Welke (1998)				X		
Thomson and von Solms (1997)	X	X				
Spurling (1995)	X	X				
Akers and Sellers (1994)					X	
Lafleur (1992)	X					X
Murray (1991)	X	X				
Straub (1990)					X	
Perry (1985)	X		X	X	X	X
Arvey and Ivancevich (1980)					X	

References

Akers, R. L., and Sellers, C. S. 1994. *Criminological Theories: Introduction, Evaluation, and Application*, Los Angeles: Roxbury Publishing.

Arvey, R. D., and Ivancevich, J. M. 1980. "Punishment in Organizations: A Review, Propositions, and Research Suggestions," *The Academy of Management Review* (5:1), pp. 123-132.

Bloomberg 2014. "JPMorgan Hack said to Span Months Via Multiple Flaws." Available online: http://www.bloomberg.com/news/articles/2014-08-29/jpmorgan-hack-said-to-span-months-via-multiple-flaws (Date accessed: 04/24/2015).

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

Brown, S. A., Venkatesh, V., and Goyal, S. 2014. "Expectation Confirmation in Information Systems Research: A Test of Six Competing Models," *MIS Quarterly* (38:3), pp. 729-756.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Quarterly* (34:3), pp. 523-A7.

Cox, A., Connolly, S., and Currall, J. 2001. "Raising Information Security Awareness in the Academic Setting," *VINE* (31:2), pp. 11-16.

DataBreaches.net 2014. "World's Biggest Data Breaches". Available online: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/ (Date accessed: 04/24/2015).

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

D'Arcy, J. D., Gupta, A., Tarafdar, M., Turel, O. 2014. "Reflecting on the 'Dark Side' of Information Technology Use," *Communications of the AIS* (35:5), pp. 109-118.

D'Arcy, J. D., and Herath, T. 2011. "A Review and Analysis of Deterrence Theory in the IS Security Literature: Making Sense of the Disparate Findings," *European Journal of Information Systems* (20), pp. 643-658.

Dhillon, G., and Backhouse, J. 2001. "Current Directions in Information Security Research: Toward Socio-Organizational Perspectives," *Information System Journal* (11:2), pp. 127-153.

Dittes, S., Urbach, N., Ahlemann, F., Smolnik, S., Müller, T. 2015. „Why don't you Stuck to Them? Understanding Factors Influencing and Counter-Measures to Combat Deviant Behavior Towards Organizational IT Standards," in *Wirtschaftsinformatik Proceedings*, paper 42.

Forbes 2014. "The Top 5 Most Brutal Cyber Attacks of 2014 So Far." Available online: http://www.forbes.com/sites/jaymcgregor/2014/07/28/the-top-5-most-brutal-cyber-attacks-of-2014-so-far/ (Date accessed: 04/24/2015).

Glisson, W. B., and Welland, R. 2014. "Web Engineering Security (WES) Methodology," *Communications of the AIS* (34:71), pp. 1359-1396.

Hadland, T. 1998. "IS Security Management: An Awareness Campaign," in *UKOLUG98: New Networks, Old Information - UKOLUG's 20th Birthday Conference*, C. J. Armstrong and R. J. Hartley (eds.), Manchester, UK.

Heikka, J. 2008. "A Constructive Approach to Information Systems Security Training: An Action Research Experience," in *Proceedings of Americas Conference on Information Systems*, paper 319.

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

Johns, G. 2006. "The Essential Impact of Context on Organizational Behavior," *Academy of Management Review* (31:2), pp. 386-408.

Johnston, A. C., Wech, B., Jack, B., and Beavers, M. 2010. "Reigning in the Remote Employee: Applying Social Learning Theory to Explain Information Security Policy Compliance Attitudes," *Proceedings of Americas Conference on Information Systems*, paper 493.

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

Karjalainen, M., and Siponen, M. 2011. "Toward a New Meta-Theory for Designing Information Systems (IS) Security Training Approaches," *Journal of the Association for Information Systems* (12:8), pp. 518-555.

Kayworth, T., and Whitten, D. 2010. "Effective Information Security Requires a Balance of Social and Technology Factors," *MIS Quarterly Executive* (9:3), pp. 163-175.

Knapp, K., Denney, G. D., and Barner, M. E. 2009. "Data Center Security: Analysis of Two Audit Reports," *SAIS Proceedings*, paper 2.

Kwon, J., and Johnson, M. E. 2011. "The Impact of Security Practices on Regulatory Compliance and Security Performance," *32nd International Conference on Information Systems*, Shanghai 2011.

Lafleur, L. M. 1992. "Training as Part of a Security Awareness Program," *Computer Control Quarterly* (10:4), pp. 4-11.

Lampe, U., Wenge, O., Müller, A., and Schaarschmidt, R. 2013. „On the Relevance of Security Risks for Cloud Adoption in the Financial Industry," in *Proceedings of Americas Conference on Information Systems*, Chicago, IL.

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

Liang, H., Xue, Y., and Wu, L. 2013. "Ensuring Employees' IT Compliance: Carrot or Stick?" *Information Systems Research* (24:2), pp. 279-294.

Merriam-Webster 2015. "Management." Available online: *http://www.merriam-webster.com/dictionary/management* (Date accessed: 04/10/2015)

Mitnick, K. D. 2002. *The Art of Deception: Controlling the Human Element of Security*, New York, NY, US: Wiley Publishing.

Murray, B. 1991. "Running Corporate and National Security Awareness Programs," in *Proceedings of the 7th International Conference on IS Security*, Amsterdam, The Netherlands: North-Holland Publishing Co., pp. 203-207.

Pahnila, S., Siponen, M., and Mahmood, A. 2007. "Employees' Behavior Towards IS Security Policy Compliance," *in Proceedings of the 40th Annual Hawaii International Conference on System Sciences*.

Peltier, T. R. 2002. *IS Security Policies, Procedures, and Standards: Guidelines for Effective IS Security Management*, Boca Raton, FL: Auerbach Publications.

Peltier, T. R. 2000. "How to Build a Comprehensive Security Awareness Program," *Computer Security Journal* (16:2), pp. 23-32.

Perry, W. E. 1985. *Management Strategies for Computer Security*, Newton, MA: Butterworth-Heinemann.

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

Ramachandran, S., Rao, V. S., Goles, T., and Dhillon, G. 2013. "Variations in Information Security Cultures across Professions: A Qualitative Study," *Communications of the AIS* (33:11), pp. 163-204.

Reuters 2014. "JPMorgan Hack exposed Data of 83 Million, among Biggest Breaches in History." Available online: http://www.reuters.com/article/2014/10/03/us-jpmorgan-cybersecurity-idUSKCN0HR23T20141003 (Date accessed: 04/24/2015).

Rudolph, K., Warshawsky, G., and Numkin, L. 2002. "Security Awareness," in *Computer Security Handbook* (4th ed.), S. Bossworth, and M. E. Kabay (eds.), New York, NY: John Wiley & Sons, pp. 29.1-29.19.

Siponen, M. T. 2005a. "An Analysis of the Traditional IS Security Approaches: Implications for Research and Practice," *European Journal of Information Systems* (14:3), pp. 303-315.

Siponen, M. T. 2005b. "Analysis of Modern IS Security Development Approaches: Towards the Next Generation of Social and Adaptable ISS Methods," *Information and Organization* (15:1), pp. 339-375.

Siponen, M. T., Pahnila, S., and Mahmood, M. A. 2007. "Employees' Adherence to Information Security Policies: An Empirical Study," in *Proceedings of the 22nd International Information Security Conference*, Boston, MA: Springer, pp. 133-144.

Siponen, M. T., and Vance, A. 2010. "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations," *MIS Quarterly* (34:3), pp. 487-A12.

Siponen, M., Pahnila, S., and Mahmood, M. A. 2010. "Compliance with Information Security Policies: An Empirical Investigation," *IEEE Computer* (February 2010), pp. 64-71.

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

Spurling, P. 1995. "Promoting Security Awareness and Commitment," *Information Management and Computer Security* (3:2), pp. 20-26.

Stanton, J. M., and Stam, K. R. 2006. *The Visible Employee*, Medford, NJ: Information Today, Inc.

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

Straub, D. W., and Welke, R. J. 1998. "Coping with Systems Risk: Security Planning Models for Management Decision Making," *MIS Quarterly* (22:4), pp. 441-469.

Target 2015. "Data Breach FAQ." Available online: https://corporate.target.com/about/shopping-experience/payment-card-issue-faq (Date accessed: 04/24/2015).

Thomson, M. E., and von Solms, R. 1997. "An Effective IS Security Awareness Program for Industry," in *Proceedings of the 13th International Conference on IS Security*, London, UK: Chapman and Hall.

Tu, Z., and Yuan, Y. 2014. "Critical Success Factors Analysis on Effective Information Security Management: A Literature Review," in *Proceedings of Americas Conference on Information Systems, Savannah*.

University of Minnesota. 2014. "The 2014 SIM IT Key Issues and Trend Study," *MIS Quarterly Executive* (13:4), pp. 237-263.

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

Webster, J., and Watson, R. T. 2001. "Analyzing the Past to Prepare for the Future: Writing a Literature Review," *MIS Quarterly* (26:2), pp. xiii-xxiii.

Whitman, M. E. 2008. "Security Policy: From Design to Maintenance," in *Information Security: Policy, Processes, and Practices*, D. W. Straub, S. Goodman and R. L. Baskerville (eds.), Armonk, NY: M. E. Sharpe, Inc., pp. 123-151.

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

Willison, R., and Warkentin, M. 2012. "Beyond Deterrence: An Expanded View of Employee Computer Abuse," *MIS Quarterly* (37:1), pp. 1-20.

Xu, H., Dinev, T., Smith, J., and Hart, P. 2011. "Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances," *Journal of the Association for Information Systems* (12:12), pp. 798-824.