Why Employees (Still) Click on Phishing Links: an Investigation in Hospitals

Mohammad S. Jalali, Maike Bruckes, Daniel Westmattelmann, Gerhard Schewe

Working Paper CISL# 2020-10

January 2020

Cybersecurity Interdisciplinary Systems Laboratory (CISL)
Sloan School of Management, Room E62-422
Massachusetts Institute of Technology
Cambridge, MA 02142

Working paper - January 2019
Please send your comments to: jalali@mit.edu

Why Employees (Still) Click on Phishing Links: an Investigation in Hospitals

Mohammad S. Jalali[1,2], **Maike Bruckes**[3], **Daniel Westmattelmann**[3], **Gerhard Schewe**[3]

[1] MIT Sloan School of Management, Cambridge, MA, USA
[2] Harvard Medical School, Boston, MA, USA
[3] University of Muenster, Center for Management, Muenster, Germany

Abstract

Employees are considered the weakest link in information security; their compliance with security policies has been a major area of research. However, employees click on phishing links even after receiving training. In this study, we explore the factors that influence information security policy compliance, using the theory of planned behavior (TPB) and integrating trust theories. We conduct a survey in hospitals to investigate the components of compliance intention and match employees' survey results with their actual clicking data from organizational phishing campaigns. Our analysis (N = 430) revealed that TPB factors (attitude, subjective norms, and perceived behavioral control), as well as collective felt trust and trust in information security technology, have positive effects on compliance intention. However, surprisingly, compliance intention does not predict compliance behavior. Of the variables we tested, only the level of employees' workload shows a significant relationship to their actual behavior. This study contributes to the information systems literature by understanding factors influencing compliance behavior. Also, unlike studies that assess behavior through a questionnaire, our method was able to measure observable compliance behavior using clicking data. Our findings can help organizations augment employees' compliance with their cybersecurity policies and reduce the likelihood of clicking on phishing links.

Keywords: Information security management, phishing emails, compliance, trust, theory of planned behavior

INTRODUCTION

The human ability to rapidly learn and problem solve is driving the growth of a globally connected network; however, the result is an overly complex system riddled with cybersecurity holes, leaving organizations susceptible to information security threats. Incentives are high to hack information systems (IS) and steal valuable data. These attacks are becoming increasingly more sophisticated as advanced hacker tools develop. Advanced defense tools have developed as well, but are still not enough to overcome the security risk posed by employee error.

In information security management, people are the weakest link in organizations (Boss, Kirsch, Angermeier, Shingler, & Boss, 2009; Hu, Dinev, Hart, & Cooke, 2012). Any employee who violates information security policies (ISP) makes their organization vulnerable. Discovering 'why' employees fail to comply with ISP is of critical importance for protecting an organization's information. Even in regards to seemingly small issues, noncompliance may lead to a snowballing effect and trigger a larger problem.

Phishing emails demonstrate this dynamic. Phishing is the practice of sending emails claiming a false identity to induce individuals to reveal information. These fraudulent emails are tailored to access IS by targeting those with access to the system. Phishing poses a major cybersecurity risk for two reasons: 1) employees usually have detailed knowledge about IS within the organization, and they access the data frequently during their work; 2) even one innocent click could expose the organization to a network of hackers nearly impossible to trace (Bulgurcu, Cavusoglu, & Benbasat, 2010; Herath & Rao, 2009a; Johnston & Warkentin, 2010; Siponen & Vance, 2010). Organizations have taken steps at addressing this insider problem by providing training programs to educate and increase cybersecurity awareness, but these efforts remain insufficient. Even educated employees violate ISP by clicking on phishing links or not reporting phishing emails. In this study, we examine whether employees intend to follow ISP and what factors influence their compliance.

To investigate employee's compliance to ISP, previous research has often focused on behavioral theories based on cognitive beliefs. These include general deterrence theory (D'Arcy, Hovav, & Galletta, 2009; Straub, 1990), rational choice theory (Bulgurcu et al., 2010; D'Arcy & Lowry, 2017), protection motivation theory (Crossler & Bélanger, 2014; Herath & Rao, 2009b), and theory of planned behavior (TPB) (Bulgurcu et al., 2010; Hu et al., 2012). As we will examine in depth, TPB has been the most widely validated and extended to measure different antecedents to ISP compliance (Lebek, Uffen, Neumann, Hohler, & H. Breitner, 2014; Moody, Siponen, & Pahnila, 2018; Sommestad, Hallberg, Lundholm, & Bengtsson, 2014). Thus, TPB provides a well-established theoretical framework that we draw on for this study.

Although previous studies have examined the cognitive beliefs that drive ISP compliance, they have not adequately investigated the components of these cognitive beliefs. One such component is trust. Trust influences how individuals assess cost-benefit considerations, how they make decisions, and ultimately how they behave (Fulmer & Gelfand, 2012; Talaulicar, Grundei, & Werder, 2005). Trust has been researched from a broad range of research directions and has evolved to a widely accepted and established concept (Jarvenpaa, Shaw, & Staples, 2004; Lankton, McKnight, & Tripp, 2015; McEvily & Tortoriello, 2011; Rousseau, Sitkin, Burt, & Camerer, 1998). However, despite its importance in various domains, including organizational behavior, compliance and commitment, ISP compliance literature has not adequately considered the role of trust.

Particularly in regards to phishing attacks, two major questions remain unanswered: 1) What is the role of trust in predicting employees' compliance intention? 2) To what extent does compliance intention correspond to compliance behavior? In order to address these questions, we draw on the TPB and investigate individual and organizational factors that motivate compliance with information security guidelines. We conduct a survey and use data from phishing campaigns to highlight relationships among employees' attitudes and beliefs and their actual compliance behavior.

The study consists of two steps: First, as a part of phishing tests, employees of hospitals received a faux phishing email. Second, about six weeks after the phishing tests, all individuals (clickers and non-clickers) answered a survey that examined their attitudes towards cybersecurity policy. Furthermore, we assessed employees' perceived risk, workload, collective felt trust, and trust in information security technologies. We respond to the call made by Lowry et al. (2017) to move beyond merely measuring intentions by including data on compliance actions. Since we are comparing individual's qualitative answers in the survey against their own clicking data, we are able to observe and compare their compliance intention with their actual behavior.

This is the first study to investigate 'why' employees click on phishing emails by focusing on individual and organizational factors, and by using actual clicking data. Our study contributes to the literature of information security compliance by providing an extension of TPB and individual-level compliance factors. We gauge the factors that influence clicking behavior such that organizations can identify individuals who may be at risk for phishing attacks. Given the heterogeneity across industries in employees' ISP compliance and the type of cyber threats, we chose to focus on the healthcare industry for this study. Hospitals have been one of the major targets for cybercriminals, and despite efforts to improve compliance, they still significantly suffer from cyber attacks (Jalali & Kaiser, 2018; Jalali, Razak, Gordon, Perakslis, & Madnick, 2018; Jalali, Russell, Razak, & Gordon, 2019).

This paper is organized as follows: We first review the relevant literature and theoretical background. Next, we present our research methods, including the structure of the phishing ploy and the survey. Finally, we present our data analysis, results, and discussions.

LITERATURE REVIEW

Recent research in IS security focuses on employee compliance to information security rules and policies. Over the last several years, the literature emphasized behavioral research in information security to explain employee behavior. We review this literature and argue that focusing on the theory of planned behavior (TPB) and including additional individual and organizational level factors can enhance the understanding of employee compliance.

Two main theories have emerged regarding organizational employee behavior: the TPB and Protection Motivation Theory (PMT). Research shows that PMT is better suited to explain personal security behaviors, where the consequences of misbehavior directly impact the individual (D'Arcy & Lowry, 2017; Johnston, Warkentin, & Siponen, 2015; Sommestad et al., 2014). TPB on the other hand has received substantial theoretical and empirical support for predicting ISP compliance (e.g. Bulgurcu et al., 2010; Hu et al., 2012; Ifinedo, 2012; Siponen, Mahmood, & Pahnila, 2014). Moody et al. (2018) conducted a large-scale study and compared 11 different theories regarding their applicability in an information security setting. They found that the TPB ranked among those with

the best explanatory power. Thus, TPB provides a well-established theoretical framework and is well suited for our research on the link between intention and behavior.

However, research on TPB in ISP compliance has mainly focused on its core components (attitudes, subjective norm, and perceived behavioral control) and does not cover how decisions are made about these components and what influencing factors are involved. Most studies on ISP focus on cognitive factors for compliance, such as Bulgurcu et al. (2010) which focused on rationality-based beliefs about outcomes and consequences of compliance. However, decisions are rarely solely based on cognitive beliefs. As D'Arcy and Lowry (2017) point out, the affective side of employee compliance deserves further attention. In addition to logical beliefs about the rules themselves, feeling and influence also make a significant impact, but most TPB studies have yet to account for these factors. Some studies which do not focus on TPB have pushed beyond cognitive components and found strong evidence for the relevance of affective or indirect influences on security compliance. These studies have demonstrated that organizational commitment (Herath & Rao, 2009b; Safa, Solms, & Furnell, 2016) and organizational culture (Hu et al., 2012) positively influence employees' compliance intentions. Also, management has been shown to influence employees' perception of compliance policies. Management engagement (Puhakainen & Siponen, 2010) and top management participation (Hu et al., 2012) influence employees' perceptions and considerably increase employees' compliance with ISP.

Besides these organizational level factors, other studies argue that security policy compliance intention is influenced by individual factors, such as perceived organizational support (Warkentin, Johnston, & Shropshire, 2011) and affect (D'Arcy & Lowry, 2017). These factors affect compliance indirectly by influencing cost-benefit perceptions on ISP compliance. Hence, evidence shows that more indirect aspects also provide explanatory power over cognitive measures.

Nor has previous research been limited to the employees' attitudes towards their organization. Studies have also examined attitudes towards security technologies. Zhang et al. (2009) propose a model that includes perceived effectiveness of technical security protection and show that this affects the perceived behavioral control and the intention to comply.

Recently, a number of studies based on other theoretical approaches have focused on the effects of perceived organizational trust on employees' compliance. Workman (2009) showed that higher levels of trust resulted in more positive attitudes towards surveillance. Focusing on organizational trust, Lowry et al. (2015) investigated its effect on computer abuse after a change of security policies and found that organizational trust significantly decreased reactive abusive behavior.

These studies point toward the importance of employees' perceptions of information security policies and systems. However, what shapes these perceptions is still insufficiently understood. Additionally, only a few of these theories have been integrated in TPB. At the same time, an extensive body of interdisciplinary literature exists that shows trust influences employees' behavior and shapes their perceptions (Dirks & Ferrin, 2002; Holtz, 2013). A number of factors related to trust have been examined in the ISP literature. These studies show that the effectiveness of ISP does not only depend on the rules and regulations, but also on how they are implemented and communicated. Thus, trust can serve as an overarching framework that is needed to develop a better theoretical understanding and to better manage ISP compliance.

In summary, the literature shows that TPB is a strong foundation for investigating information security compliance. Yet, within the reviewed studies a strong focus on cognitive drivers of compliance can be seen, while the factors that impact these drivers have not been sufficiently

investigated through the lens of TPB. We address this gap in our study, by focusing on individual and organizational factors, particularly how collective felt trust, and trust in the security system influences the perception of ISP and employees' compliance intentions.

THEORETICAL FRAMEWORK AND HYPOTHESES

In this section, we introduce our hypotheses about the impact of intention on ISP compliance actions. These hypotheses are based on three theoretical frameworks outlined below: the Theory of Planned Behavior, Collective Felt Trust, and Trust in Technology.

Theory of Planned Behavior

Theory of Planned Behavior (TPB) has emerged as one of the most influential frameworks for the explanation of human behavior (Ajzen & Fishbein, 1980; Fishbein & Ajzen, 1975). Drawing on the Theory of Reasoned Action, the TPB explains that attitudes, subjective norms, and perception of behavioral controls form an individual's intention to perform a certain behavior—intention is a direct antecedent of the actual behavior.

Studies have shown some link between attitudes, subjective norms, perceived behavioral controls, and intention in the context of ISP, but have not fully covered them in the context of information security. The relationship between attitudes and intention is the most investigated for TPB in ISP compliance. A positive attitude towards ISP is assumed to predict compliance intention. Bulgurcu et al. (2010) focus on the link between employees' attitudes towards compliance and their intention to comply and found a positive relationship. Similarly, Ifinedo (2012) investigated ISP compliance of managers and IS professionals. He concluded that attitude towards compliance, subjective norms, and response efficacy positively influence employees' general ISP compliance intentions. While these findings all show that TPB is generally suitable for predicting intention in information security research, the specific context (i.e., phishing) is a major influence on the behavioral intention—as the context might substantially influence the outcome. Thus, we build on previous research by proposing that TPB variables are associated with employees' intention to comply specifically with ISP:

H1a: Attitudes towards ISP will positively influence the intention to comply.

H1b: Subjective norms will positively influence the intention to comply.

H1c: Perceived behavioral controls will positively influence the intention to comply.

H2: The intention to comply will have a positive effect on compliance behavior.

Collective Felt Trust

A second factor we believe influences compliance is collective felt trust. In their review, Mayer et al. (1995) suggest that trust influences employees' behavior in the sense that it affects risk-taking in relationships, and impacts processes and outcomes in an organization. Although various trust definitions exist, most agree that trust comprises of: 1) positive expectations (Lewicki & Bunker, 1996), and 2) willingness to be vulnerable to the actions of the other party (Mayer et al., 1995).

Accordingly, Rousseau et al. define trust as "a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another" (1998, p. 395).

Trust has previously been shown to influence attitudes in the TPB. In the context of electronic commerce adoption, Pavlou and Fygenson (2006) investigated whether trust is relevant for the attitude towards a certain product. They found that trust in a vendor had a significant effect on buyer's attitude toward the product. While management in an organization is not selling a product to its employees, they are responsible for providing a work environment within the company that enables employees to focus on their tasks. Meta-analytic evidence has shown that by trusting the management, employees feel more committed to their company and will be more willing to follow organizational policies (Dirks & Ferrin, 2002).

Moreover, trust has been shown to impact organizational support and commitment (Chen, Aryee, & Lee, 2005; Whitener, 2001) and organizational citizenship behavior (Krosgaard, Brodt, & Whitener, 2002; Mayer & Gavin, 2005). Several studies in organizational sciences report a positive relationship between trust and compliance (Colquitt, Scott, & LePine, 2007; Davies, Lassar, Manolis, Prince, & Winsor, 2011; Kim & Mauborgne, 1993; Rafaeli, Sagy, & Derfler-Rozin, 2008). In addition to this relationship, Deutsch Salomon and Robinson (2008) found that felt trust increased employees' responsibility norms and subsequently their performance. We assume that this effect holds in our context too: Employees that feel trusted by their management consider their behavior more closely to not violate the trust they are being given.

Based on these considerations, we argue that collective felt trust influences employees' attitudes towards ISP and their perceived subjective norms. Thus, we propose:

H3a: Collective felt trust will positively influence the attitudes towards ISP.

H3b: Collective felt trust will positively influence subjective norms.

Trust in Technology

Although trust has often been researched on the interpersonal level, recent development in the IS domain shows that trust in technology is as equally important (e.g. McKnight, Carter, Thatcher, & Clay, 2011; Srivastava & Chandra, 2018). Trust in technology has been shown to increase the intention to use a specific technology (McKnight et al., 2011), the acceptance of technologies (Hernández-Ortega, 2011), cloud technology adoption (Ho, Ocasio-Velázquez, & Booth, 2017), and intention to use mobile banking (Kim, Shin, & Lee, 2009).

When individuals find themselves in risky situations in which they have to depend on technologies, trust becomes essential (Han, Ada, Sharman, & Rao, 2015). Individuals are vulnerable to the functioning of that specific technology–similar to trust in people, trust in technology is formed based on the perception of the attributes of a technology. Lankton et al. (2015) suggest differentiating among perceptions of functionality, helpfulness, and reliability as factors affecting trust in technology. In the context of information security, the helpfulness (e.g., of an anti-virus) is rather limited, while functionality and reliability are highly relevant.

When using IS, employees are in a risky situation where they are facing cyber attacks and they have to rely on cybersecurity technologies. High trust in technology will enhance the level of

confidence of facing these threats. We therefore assume that trust in technology is critical for how effective employees perceive their behavioral control to use the technology:

H4: Trust in technology will have a positive effect on perceived behavioral control.

In situations where individuals perceive a higher threat of a cyber attack, the attention towards potential harms might rise. Johnston and Warkentin (2010) discuss the influence of fear appeals in IS security, and argue that the more severe or susceptible a threat is perceived to be, the fewer individuals rely on the ability of the cybersecurity software. Thus, the higher the perceived risk, the more individuals are expected to pay attention to situations where the software did not adequately eliminate the threat, e.g., phishing emails. We therefore propose that:

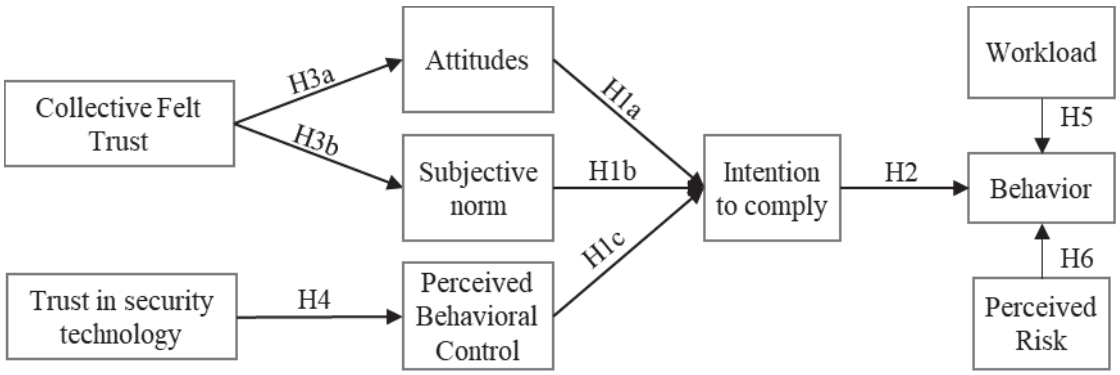
H5: Perceived risk will reduce the behavior of clicking on phishing links.

On the other side, employees that face a high workload might not be able to execute cognitive considerations to decide to follow ISP. As Siponen and Vance (2010) discuss, employees might even use their high workload as an excuse for violating ISP. In situations were high workload stops employees from paying attention to details of an email, whether intentionally or accidentally, the likelihood of opening a potentially dangerous email might increase. Thus, we propose that:

H6: High workload will increase the behavior of clicking on phishing links.

Figure 1 presents our proposed research model.

FIGURE 1: PROPOSED RESEARCH MODEL



METHODS

Data and Procedure

Data was collected in two steps. In the first step, a professional cybersecurity company sent out phishing emails to employees in three networks of hospitals in the eastern United States. The phishing campaigns were designed to resemble real phishing emails so that participants could not know that they are being tested and would behave as if they received a real phishing email. All phishing emails contained a hyperlink. Collected data included the identity of individuals receiving the email and whether they clicked on the link or not. This information was then provided only to the respective hospital.

For the second step, we developed a web-based survey instrument. In order to compare the results of clickers and non-clickers, we created two different survey links based on the same questionnaire. Hospitals' IT departments also created two different pools of employees (clickers and non-clickers)—as they knew the identity of clickers—and distributed one survey to each group. This separation helped facilitate anonymity of the survey analysis as we did not ask hospitals for any clicking data. Participants were informed that their participation in our survey was voluntary and anonymous.

By combining these two steps, we aimed to independently and systematically assess the extent to which attitudes and attributes are related to the actual clicking behavior. Collecting clicking data in the first step has the advantage that the results are not distorted by the survey. To nullify the concern of whether having clicked or not clicked on the phishing email would influence behavior in the survey, the survey was distributed about six weeks after the phishing e-mails were sent out.

The survey contained questions about personal attitudes towards the organization and its ISP. Additionally, we asked about the perception of responsibility, self-efficacy, and trust in both management and technology (e.g., anti-virus and firewall). We also included attributes in the questionnaire to find out whether their general behavior is an influencer of their clicking behavior.

Measures

All survey items were based on previously validated items to maximize reliability—we provide references for each survey construct in Table 1. A pilot test was run with ten researchers to ensure that all questions were clear.

The eight constructs of the survey include attitudes, subjective norm, perceived behavioral control, and intention (Ajzen & Fishbein, 1980; Bulgurcu et al., 2010; Hu et al., 2012), collective felt trust (Deutsch Salamon & Robinson, 2008; Mayer et al., 1995), trust in technology (Lankton et al., 2015; McKnight et al., 2011), perceived security risk (Li, Zhang, & Sarathy, 2010), and workload (Rutner, Hardgrave, & McKnight, 2008). See Table 1 for items, factor loadings, and Cronbach's alpha of each construct.

TABLE 1: Constructs and Items

Construct	Reference	Items*	Loadings	Cronbach's alpha
Attitudes (towards ISP)	Ajzen (1991); Bulgurcu et al. (2010); Hu et al. (2012)	I believe it is beneficial for our organization to establish clear information security policies, practices, and technologies.	.891	.86
		I believe it is useful to for our organization to enforce its information security policies, practices, and technologies.	.756	
		I believe it is a good idea for our organization to establish clear information security policies, practices, and technologies.	.884	
Subjective norm	Ajzen (1991); Bulgurcu et al. (2010);	People who influenced my behavior would think that I should follow the policies and procedures and use the cybersecurity technologies.	.844	.93
		People whose opinions are important to me would think that I should follow the policies and procedures and use the cybersecurity technologies.	.955	

Construct	Reference	Items*	Loadings	Cronbach's alpha
	Hu et al. (2012)	People whom I respect would think that I should follow the policies and procedures and use the cybersecurity technologies.	.952	
Perceived behavioral control	Ajzen (1991); Bulgurcu et al. (2010); Hu et al. (2012)	I am able to follow the cybersecurity policies and procedures and technologies (e.g., antivirus, or other products).	.665	.79
		I have the resources and knowledge to follow the policies and procedures and use the cybersecurity technologies.	.917	
		I have adequate training to follow the policies and procedures and use the cybersecurity technologies.	.850	
Intention to comply	Based on Ajzen (1991)	I intend to follow the information security policies and practices at work.	1	1
Collective felt trust	Based on Deutsch Salamon and Robinson (2008); Mayer et al. (1995)	Management lets me have an impact on issues they find important.	dropped	.77
		Management doesn't feel the need to "keep an eye" on me.	.773	
		Management would be comfortable assigning me a critical task, even if they cannot monitor my actions.	.735	
		Management believes that employees can be trusted.	.688	
Trust in security technology; reliability	Lankton et al. (2015); Kim et al. (2009)	The cybersecurity software at my workplace (e.g., antivirus and firewall) is very reliable.	.897	.95
		The cybersecurity software at my workplace does not fail me.	.939	
		The cybersecurity software at my workplace provides accurate services.	.893	
Trust in security technology; functionality	Lankton et al. (2015)	The cybersecurity software at my workplace has the functionality I need	.946	.95
		The cybersecurity software at my workplace has the features required for my tasks.	.929	
		The cybersecurity software at my workplace has the ability to do what I want it to do.	.909	
Perceived risk	Li et al. (2010)	At my workplace, the risk to my computer and data from Internet security breaches is:	.704	.93
		At my workplace, the likelihood that my computer will be disrupted due to Internet security breaches within the next 12 months is:	.918	
		At my workplace, the chance that my computer will fall a victim to an Internet security breach is:	.967	
		At my workplace, the vulnerability of my computer and data to Internet security risks is:	.910	
Workload	Rutner et al. (2008)	I feel that the number of requests, problems, or complaints I deal with at work is more than expected.	dropped	.82
		I feel that the amount of work I do interferes with how well it is done.	.588	
		I feel busy or rushed at work.	.916	
		I feel pressured at work.	.818	

* A 5-point Likert scale (1=never/strongly disagree/extremely low; and 5=always/strongly agree/extremely high) was used for all items except for intention, where a 7-point-likert scale (1=strongly disagree, and 7=strongly agree) was used.

As control variables in addition to the core concepts, we also asked for the average number of emails received daily, age, sex (male, female, or non-binary), position (clinical or non-clinical), and education level.

Data Analysis

The survey was sent to 3,169 employees in three hospital networks. 488 individuals participated in the study (15% response rate). Due to incomplete data, 58 were dropped from the analysis, resulting in a final sample of 430. Table 2 presents respondent characteristics of all participants. Table 3 reports means, standard deviations, and correlations of all latent variables.

TABLE 2: Respondent Characteristics

Category	Subcategory	Count	Percentage
Sample size		430	100.00%
Sex	Male	95	22.09%
	Female	328	76.28%
	Non-binary	2	0.47%
	Unanswered	5	1.16%
Age	Under 18	0	0%
	18 - 24	28	6.51%
	25 - 34	115	26.74%
	35 - 44	82	19.07%
	45 - 54	83	19.30%
	55 - 64	93	21.63%
	65 - 74	20	4.65%
	75 - 84	2	0.47%
	85 or older	0	0%
	Unanswered	7	1.63%
Position	Clinical	202	46.98%
	Non-Clinical	228	53.02%
	Unanswered	0	0%
Education	Less than high school	29	6.74%
	High school graduate	50	11.63%
	Some college	122	28.37%
	2-year degree	47	10.93%
	4-year degree	130	30.23%
	Professional degree	44	10.23%
	Doctorate	0	0%
	Unanswered	8	1.98%
Response to phishing e-mail	Clicker	248	57.67%
	Non-clicker	182	42.33%
	Unanswered	0	0%

TABLE 3: Zero-order Correlations and Descriptive Statistics

	Construct	Mean	Std. dev	1	2	3	4	5	6	7	8
1	Attitudes	4.79	0.420								
2	Subjective norm	4.42	0.718	.103*							
3	Perceived behavioral control	4.46	0.383	.059**	.101***						
4	Intention to comply	4.79	0.404	.069**	.089***	.094***					
5	Collective felt trust	4.81	0.877	.101***	.136***	.095***	.106***				
6	Trust in technology	4.09	0.747	.080***	.127***	.166***	.123***	.219***			
7	Perceived risk	2.46	0.840	-.034*	-.095***	-.086***	-.080**	-.217***	-.173***		
8	Workload	2.76	0.718	-.027	.005	-.048	-.028*	-.122	-.076	.086**	

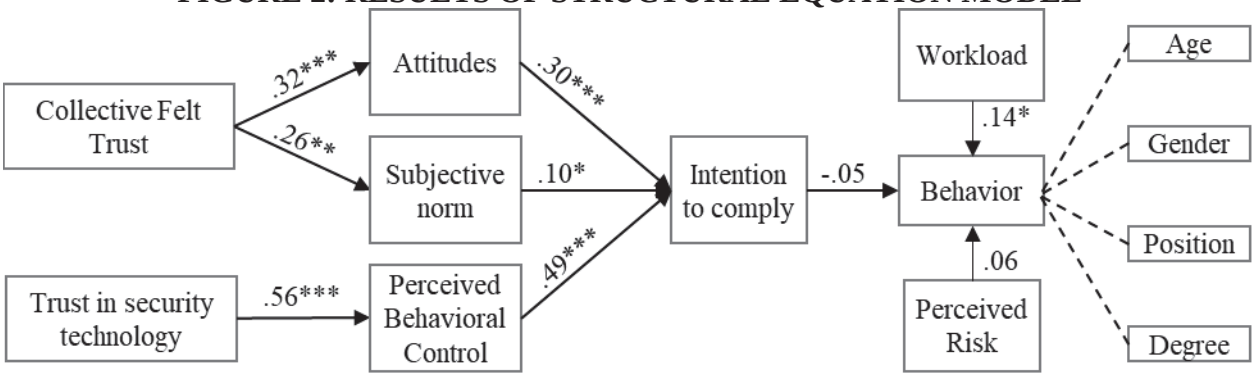
*** p< .001; ** p< .01; * p< .05, two-tailed

We first conducted a confirmatory factor analysis (CFA) to assess the measurement model. After two items were dropped from the analysis (identified in Table 1), all loadings were above .50, as the common threshold value for standardized factor loadings (Hair, 2010). Additionally, Cronbach's alpha exceeded .70 for all constructs (Hair, 2010). The average variance extracted (AVE) was above .68 for all factors, indicating adequate convergent validity. Also, composite reliability (CR) was above .70 for all factors as recommended by Hair (2010). Discriminant validity was also given as all AVEs exceed the corresponding squared inter-construct correlation estimates. Based on the CFA results, the model demonstrated acceptable fit with χ^2 = 675.05, df = 389, comparative fit index (CFI) = .969, Tucker-Lewis Index (TLI) = .963, and root mean square error of approximation (RMSEA) = .041.

RESULTS

We employ a structural equation model (SEM) to test the strength of the relationship among the different constructs, and its effect on the actual clicking behavior. The use of an SEM is particularly appropriate because the complex relationships in the proposed model can be tested simultaneously (Hair, 2010). Our SEM analysis resulted in a good fit to the data (χ^2 = 887.61, df = 443; CFI = .949; TLI = .944; RMSEA = .049). The standardized paths coefficients can be found in figure 2. We included several control variables of which none had a significant effect on the behavior of clicking the link in the phishing email.

FIGURE 2: RESULTS OF STRUCTURAL EQUATION MODEL



*** p< .001; ** p< .01; * p< .05, two-tailed; dashed line indicates non-significant control variables

Hypothesis 1 predicted that a) attitudes towards ISP, b) subjective norms, and c) perceived behavioral control positively influence the intention to comply. This prediction is supported: attitudes towards ISP ($\beta = .30$, $p < .001$), subjective norm ($\beta = .10$, $p = .011$), and perceived behavioral control ($\beta = .49$, $p < .001$) showed significant effects on intention to comply.

Hypothesis 2 predicted that the intention to comply has a positive effect on compliance behavior. Contrary to a rich theoretical body, our results show that intention does not influence the clicking behavior in our analysis ($\beta = -.05$, $p = .300$). Thus, hypothesis 2 is not supported.

Hypothesis 3 predicted that collective felt trust positively influences the attitudes towards ISP and subjective norms. Our results support this hypothesis: Trust is significantly related to attitudes towards ISP ($\beta = .32$, $p < .001$) and subjective norm ($\beta = .26$, $p < .001$). Hypothesis 4 predicted that trust in security technology has a positive effect on perceived behavioral control. Our results support this hypothesis ($\beta = .56$, $p < .001$). Taken together, our analysis shows that collective felt trust and trust in technology do have significant effects on the intention to comply, thereby supporting the TPB.

Hypothesis 5 predicted that high workload increased the likelihood to click on phishing links. Our results show that high workload has a positive effect on the clicking behavior, supporting this hypothesis ($\beta = .14$, $p = .011$).

Lastly, hypothesis 6 predicted that a higher perceived risk of cyber attacks reduced the likelihood to click on phishing links. This hypothesis cannot be supported as our results indicate no significant relationship between perceived risk and the behavior to click on phishing links ($\beta = .06$, $p < .236$).

DISCUSSION

This study investigates the relationship between employees' compliance intention and their actual compliance with information security policies (i.e., not clicking on the phishing link). Drawing on the TPB, we use attitudes, subjective norms, and perceived behavioral control to predict compliance intention. Also, based on organizational behavior literature, we considered both collective felt trust and trust in security technology as antecedents of these variables.

Overall, we found support for the proposed influences on intention to comply. As hypothesized, we found that attitudes, subjective norm, and perceived behavioral control had significant effects on the intention to comply with organizational information security policies. Our results indicate that the effect is stronger for attitudes and perceived behavioral control than for subjective norms. This finding implies that an employee's attitude and the perceived control of behavior considerably increase the intention to comply, while perceived beliefs of influential colleagues or managers have a minor yet significant effect (supporting H1).

However, surprisingly, we did not find a significant effect between the intention to comply and the actual compliance (supporting H2). Previous studies found different results. Pahnila et al. (2007) provided evidence for an effect between intention and compliance. Myyry et al. (2009) also found that intention and behavior are related to each other. However, their results show that the influencing factors are stronger for the intention to comply than for the actual compliance. One potential explanation might be found in Fife-Schaw et al. (2007), that TPB variables influence intention change more substantially than behavioral change. Our results indicate that in the context of phishing emails, intention and compliance are not associated. The role of context in compliance investigations should be carefully considered as it might prove highly relevant. In our context, we agree with Lebek et al. (2014) who critically reflect on this relationship and challenge the assumption that intention predicts behavior.

We also found that collective felt trust had a significant positive influence on an employee's attitudes and subjective norms (supporting H3). Higher collective felt trust is associated with more positive attitudes and subjective norms, which in turn positively influence the compliance intention. The results indicate that management has an effect on employee's perception of security policies. Moreover, a rich literature of trust and control points towards another benefit: trust in the management reduces the risk that employees perceive security policies as a sign of management distrust in them and their abilities (Weibel et al., 2016)—employees might understand that ISP are not designed to reduce their freedom but to enhance their protection. Also, by trusting the management, employees are likely to internalize the organization's goals and thus are more willing to protect the company by accepting the policies (Deery, Iverson, & Walsh, 2006; Maguire & Phillips, 2008).

Furthermore, trust in technology exerts significant influence on an employee's perceived behavioral control (supporting H4). Thus, with high trust in information security technologies in use, employees may perceive that they are more capable of controlling their own behavior.

We found a significant effect of workload on compliance behavior. Employees who experienced high workloads were more likely to click on phishing links (supporting H5). As none of our cognitive variables showed a significant relationship with the behavior, the workload is the only variable that predicted the compliance behavior. This finding is interesting because it offers an insight into the situations in which phishing emails are opened. Siponen and Vance (2010) argued that any form of neutralization of non-compliant behavior (in this case, the necessity to cope with a high workload) might lead to less eagerness to follow security policies. High workload could trigger clicking on phishing links because overworked employees' were unable to notice the threats.

Moreover, we found no significant effect for the perceived risk on the compliance behavior (rejecting H6). A reason for this might be that the risk is too abstract for employees or that the perceived benefits in a certain situation outweigh the perceived risk (Li et al., 2010).

As discussed earlier, we did not find any significant effects for control variables. Age, gender, level of education, and whether employees were in clinical or a non-clinical profession did not influence their compliance behavior. These findings suggest that compliance behavior is a complex phenomenon that cannot be simply attributed to a certain group or predicted based on these variables.

Theoretical Contribution

This study offers several theoretical contributions to the understanding of behavioral issues in information security. First, this study is one of the few to offer insights into intention-behavior relationships. Although this is a central component of TPB, this aspect is often neglected. Studies assume that compliance intention is equal to compliance behavior (Lebek et al., 2014). However, we show that compliance intention does not predict behavior in the context of information security compliance.

A potential explanation for this intention-behavior gap might be found in common research methods. While this study used different sources for the dependent (clicking behavior) and the independent (personal and organizational) variables to assess their relationship, previous studies have used self-reported data to assess the intention and the actual compliance (Myyry et al., 2009; Pahnila et al., 2007). This procedure is prone to common method biases, as individuals could give socially desirable answers, or previous answers could influence later answers (Jalali, 2014; Podsakoff, MacKenzie, Lee, & Podsakoff, 2003). To minimize this bias, we carefully controlled our experiment by using different measurement techniques for dependent and independent variables.

Furthermore, we demonstrate that attitudes, subjective norms, and perceived behavioral control are influenced by employees' beliefs about their organizations. We show that collective felt trust was a significant predictor of attitudes and subjective norms, while trust in technology predicted perceived behavioral control. Trust in technology has been shown to increase the adoption of new technologies and has frequently been used in IS (e.g. Lankton, McKnight, Wright, & Thatcher, 2016; Lowry, Zhang, Zhou, & Fu, 2010), but research on information system security has not adopted this concept so far. Thus, these findings not only contribute to security compliance, but also enhance the understanding of application areas for trust in technology.

Practical Implications

Our findings offer a number of practical implications. Practitioners need to consider organizational factors when designing security policies and training programs. Our results show that attitudes, subjective norms, and perceived behavioral controls have a strong effect on compliance intention and can be influenced by enhancing trust. Collective felt trust can influence attitudes and subjective norms. Thus, engaging in trust building activities enhances employee's compliance. In line with Hu et al. (2012), Puhakainen and Siponen (2010) and Kankanhalli et al. (2003), our findings also highlight the relevance of top management participation. Many top managers neglect information

security problems and address supposedly more important issues (e.g., operational issues directly affecting productivity). If managers fail to clearly demonstrate that information security is an essential matter, employees will not see it as such either. Managers need to show that they acknowledge the problems associated with IS security and are able to provide a foundation of security policy and behavior upon which employees can build.

As discussed earlier, trust in technology was shown to have a strong effect on perceived behavioral control. This finding indicates that the feeling of reliance on technology is associated with a higher intention to comply. Besides ensuring good quality of security technologies, managers need to communicate and inform employees about security technologies. If employees cannot learn about the technology in place, they cannot know how much to rely on it. Trust in technology can be developed through training and by enhancing understanding of the technology—see Puhakainen and Siponen (2010) and Safa et al. (2016) for more discussion.

As our results show that the compliance intention was not related to the actual compliance behavior, organizations must remain vigilant with vulnerabilities that cannot be easily managed. Finally, our results present a relationship between workload and non-compliance behaviors. This finding suggests that organizations should better manage workload in order to increase information security. For instance, extensive emailing may unnecessarily add to workload. Our observations working with organizations show that in addition to communication with colleagues through emails, individuals receive multiple emails on a daily basis including announcements and other general notes, which add to individuals' email loads, putting them in more risks of clicking on phishing emails.

Limitation and Future Research

This study is subject to several limitations. First, we cannot draw causal relationships from our analysis. Second, we used a specific case of phishing emails to investigate employees' compliance. As previous studies have shown, the effects between TPB constructs and influencing variables might depend on the underlying scenario. Moody et al. (2018) found support for TPB in scenarios concerning USB use, workstation logout, and password sharing. The intention-behavior gap might be more relevant in certain situations than in others. For instance, employees might not intend to open a suspicious email, but then end up doing it due to spontaneous curiosity or inattentiveness. Third, we focused on the hospital industry to keep the sample as consistent as possible. This restriction might limit the generalizability of our results. Organizational factors and governance structure should be considered when transmitting these results to other contexts.

Finally, we used a generic measure to assess the intention to comply with ISP, which means we asked for general compliance instead of focusing on phishing emails. We did so because: 1) we were interested in the general assessment of their own intention to comply; and 2) we did not want to influence the response by drawing attention towards phishing specifically. Siponen and Vance (2014) and Moody et al. (2018) discuss how a generic measure causes a problem, since researchers cannot fully predict what respondents may focus on when they answer questions. Furthermore, respondents might not perceive their behavior as non-compliant because they define the term differently. To illustrate this, Siponen and Vance (2014) use the example of driving over the speed limit and breaking the law. Although speeding is technically a break of law, only a few people would define it that way. However, we think that a generic measure is justified in this situation because employees in the investigated hospitals are expected to know about phishing email regulations. In all the hospitals we investigated, information security staff had already raised

awareness of this issue among the employees—all hospitals had anti-phishing email training. Therefore, we did not want to draw additional attention on this matter, but pose a broader question about general compliance.

CONCLUSION

Employees' compliance with policies is a key concern in information security research. This study focused on factors influencing employees' compliance intention and their actual compliance (i.e., not clicking on phishing links). Through the lens of the theory of planned behavior, we investigated the role of trust both in management in technology as an influence on attitudes, subjective norms, and perceived behavioral control. We found a positive effect between collective felt trust and attitudes toward compliance and subjective norms. Trust in technology had a strong effect on perceived behavioral control.

Furthermore, attitudes, subjective norms, and perceived behavioral control all significantly influenced the compliance intention. Surprisingly, we did not find an effect between the intention to comply and the actual compliance behavior. However, we found that a higher workload increased non-compliant behavior. This finding suggests that, in the context of phishing emails, cognitive components only play a minor role.

A major strength of this study is that we separated data collection for the dependent (clicking behavior) and the independent (personal and organizational) variables. This is one of the few studies in information security literature that observed the compliance behavior rather than assessing it in a questionnaire. This approach enabled us to obtain more reliable outcomes. We hope that our findings motivate the information security community to improve current training programs and design effective interventions to increase information security compliance.

ACKNOWLEDGMENTS

Financial support for this study was provided by Cybersecurity at MIT Sloan, also known as MIT $(IC)^3$—the Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity.

REFERENCES

Ajzen, I., & Fishbein, M. (1980). *Understanding Attitudes and Predicting Social Behavior*. NJ: Prentice Hall.: Cliffs, Englewood.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179–211. Retrieved January 14, 2019.

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.

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

Chen, Z. X., Aryee, S., & Lee, C. (2005). Test of a mediation model of perceived organizational support. *Journal of Vocational Behavior, 66*(3), 457–470.

Colquitt, J. A., Scott, B. A., & LePine, J. A. (2007). Trust, trustworthiness, and trust propensity: a meta-analytic test of their unique relationships with risk taking and job performance. *The Journal of applied psychology, 92*(4), 909–927.

Crossler, R., & Bélanger, F. (2014). An Extended Perspective on Individual Security Behaviors. *ACM SIGMIS Database, 45*(4), 51–71.

D'Arcy, J., Hovav, A., & Galletta, D. F. (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. (2017). Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal, 29*(1), 43–69.

Davies, M. A.P., Lassar, W., Manolis, C., Prince, M., & Winsor, R. D. (2011). A model of trust and compliance in franchise relationships. *Journal of Business Venturing, 26*(3), 321–340.

Deery, S. J., Iverson, R. D., & Walsh, J. T. (2006). Toward a better understanding of psychological contract breach: a study of customer service employees. *The Journal of applied psychology, 91*(1), 166–175.

Deutsch Salamon, S., & Robinson, S. L. (2008). Trust that binds: the impact of collective felt trust on organizational performance. *The Journal of applied psychology, 93*(3), 593–601.

Dirks, K. T., & Ferrin, D. L. (2002). Trust in leadership: Meta-analytic findings and implications for research and practice. *Journal of Applied Psychology, 87*(4), 611–628.

Fife-Schaw, C., Sheeran, P., & Norman, P. (2007). Simulating behaviour change interventions based on the theory of planned behaviour: Impacts on intention and action. *The British journal of social psychology, 46*(Pt 1), 43–68.

Fishbein, M., & Ajzen, I. (1975).*Belief Attitude, Intention and Behavior: An Introduction to Theory and Research.* MA: Addison-Wesley.: Reading.

Fulmer, C. A., & Gelfand, M. J. (2012). At What Level (and in Whom) We Trust. *Journal of Management, 38*(4), 1167–1230.

Hair, J. F. (2010). *Multivariate data analysis: A global perspective* (7. ed., global ed.). Upper Saddle River, NJ: Pearson.

Han, W., Ada, S., Sharman, R., & Rao, H. R. (2015). Campus Emergency Notification Systems: An Examination of Factors Affecting Compliance with Alerts. *MIS Quarterly, 39*(4), 909–929.

Herath, T., & Rao, H. R. (2009a). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154–165.

Herath, T., & Rao, H. R. (2009b). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106–125.

Hernández-Ortega, B. (2011). The role of post-use trust in the acceptance of a technology: Drivers and consequences. *Technovation, 31*(10-11), 523–538.

Ho, S. M., Ocasio-Velázquez, M., & Booth, C. (2017). Trust or consequences? Causal effects of perceived risk and subjective norms on cloud technology adoption. *Computers & Security, 70*, 581–595.

Holtz, B. C. (2013). Trust Primacy. *Journal of Management, 39*(7), 1891–1923.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture*. *Decision Sciences, 43*(4), 615–660.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security, 31*(1), 83–95.

Jalali, M. S. (2014). How Individuals Weigh Their Previous Estimates to Make a New Estimate in the Presence or Absence of Social Influence. In D. Hutchison, T. Kanade, & J. Kittler (Eds.), *Lecture Notes in Computer Science. Social Computing, Behavioral-Cultural Modeling and Prediction. 7th International Conference, SBP 2014, Washington, DC, USA, April 1-4, 2014. Proceedings* (pp. 67–74). Cham: Springer International Publishing.

Jalali, M. S., & Kaiser, J. P. (2018). Cybersecurity in Hospitals: A Systematic, Organizational Perspective. *Journal of Medical Internet Research, 20*(5), e10059.

Jalali, M. S., Razak, S., Gordon, W., Perakslis, E., & Madnick, S. (2018). Health care and cybersecurity: a bibliometric analysis of the literature (Preprint). *Journal of Medical Internet Research*.

Jalali, M. S., Russell, B., Razak, S., & Gordon, W. J. (2019). EARS to cyber incidents in health care. *Journal of the American Medical Informatics Association : JAMIA, 26*(1), 81–90.

Jarvenpaa, S. L., Shaw, T. R., & Staples, S. D. (2004). Toward Contextualized Theories of Trust: The Role of Trust in Global Virtual Teams. *Information Systems Research, 15*(3), 250–267.

Johnston, & Warkentin (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly, 34*(3), 549.

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.

Kankanhalli, A., Teo, H.-H., Tan, B. C.Y., & Wei, K.-K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management, 23*(2), 139–154.

Kim, G., Shin, B., & Lee, H. G. (2009). Understanding dynamics between initial trust and usage intentions of mobile banking. *Information Systems Journal, 19*(3), 283–311.

Kim, W. C., & Mauborgne, R. A. (1993). Procedural Justice, Attitudes, and Subsidiary Top Management Compliance with Multinationals' Corporate Strategic Decisions. *The Academy of Management Journal, 36*(3), 502–526.

Krosgaard, M. A., Brodt, S. E., & Whitener, E. M. (2002). Trust in the face of conflict: The role of managerial trustworthy behavior and organizational context. *Journal of Applied Psychology, 87*(2), 312–319.

Lankton, N., McKnight, D. H., & Tripp, J. (2015). Technology, Humanness, and Trust: Rethinking Trust in Technology. *Journal of the Association for Information Systems, 16*(10), 880–918.

Lankton, N. K., McKnight, D. H., Wright, R. T., & Thatcher, J. B. (2016). Research Note—Using Expectation Disconfirmation Theory and Polynomial Modeling to Understand Trust in Technology. *Information Systems Research, 27*(1), 197–213.

Lau, D. C., Lam, L. W., & Wen, S. S. (2014). Examining the effects of feeling trusted by supervisors in the workplace: A self-evaluative perspective. *Journal of Organizational Behavior, 35*(1), 112–127. Retrieved January 14, 2019.

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & H. Breitner, M. (2014). Information security awareness and behavior: a theory-based literature review. *Management Research Review, 37*(12), 1049–1092.

Lewicki, R. J., & Bunker, B. B. (1996). Developing and maintaining trust in work relationships. In *Trust in organizations: Frontiers of theory and research* (pp. 114–139).

Li, H., Zhang, J., & Sarathy, R. (2010). Understanding compliance with internet use policy from the perspective of rational choice theory. *Decision Support Systems, 48*(4), 635–645.

Lowry, P. B., Dinev, T., & Willison, R. (2017). Why security and privacy research lies at the centre of the information systems (IS) artefact: proposing a bold research agenda. *European Journal of Information Systems, 26*(6), 546–563.

Lowry, P. B., Posey, C., Bennett, R. B. 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.

Lowry, P. B., Zhang, D., Zhou, L., & Fu, X. (2010). Effects of culture, social presence, and group composition on trust in technology-supported decision-making groups. *Information Systems Journal, 20*(3), 297–315.

Maguire, S., & Phillips, N. (2008). 'Citibankers' at Citigroup: A Study of the Loss of Institutional Trust after a Merger. *Journal of Management Studies, 45*(2), 372–401.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An Integrative Model of Organizational Trust. *The Academy of Management Review, 20*(3), 709–734.

Mayer, R. C., & Gavin, M. B. (2005). Trust in Management and Performance: Who Minds the Shop while the Employees Watch the Boss? *The Academy of Management Journal, 48*(5), 874–888.

McEvily, B., & Tortoriello, M. (2011). Measuring trust in organisational research: Review and recommendations. *Journal of Trust Research, 1*(1), 23–63.

McKnight, D. H., Carter, M., Thatcher, J. B., & Clay, P. F. (2011). Trust in a specific technology. *ACM Transactions on Management Information Systems, 2*(2), 1–25.

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a Unified Model of Information Security Policy Compliance. *MIS Quarterly, 42*(1), 285–311.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., & Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems, 18*(2), 126–139.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' Behavior towards IS Security Policy Compliance. In R. H. Sprague (Ed.), *40th Annual Hawaii International Conference on System Sciences, 2007. HICSS 2007 ; Jan. [3 - 6], 2007, [Waikoloa, Big Island, Hawaii* (1-10). Los Alamitos, Calif.: IEEE Computer Society.

Pavlou, P. A., & Fygenson, M. (2006). Understanding and Predicting Electronic Commerce Adoption: An Extension of the Theory of Planned Behavior. *MIS Quarterly, 30*(1), 115–143.

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: a critical review of the literature and recommended remedies. *The Journal of applied psychology, 88*(5), 879–903.

Puhakainen, P., & Siponen, M. (2010). Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. *MIS Quarterly, 34*(4), 757–778.

Rafaeli, A., Sagy, Y., & Derfler-Rozin, R. (2008). Logos and Initial Compliance: A Strong Case of Mindless Trust. *Organization Science, 19*(6), 845–859.

Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Introduction to Special Topic Forum: Not so Different after All: A Cross-Discipline View of Trust. *The Academy of Management Review, 23*(3), 393–404.

Rutner, P. S., Hardgrave, B. C., & McKnight, D. H. (2008). Emotional Dissonance and the Information Technology Professional. *MIS Quarterly, 32*(3), 635–652.

Safa, N. S., Solms, R. von, & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security, 56*, 70–82.

Siponen, M., Mahmood, A. M., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management, 51*(2), 217–224.

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.

Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy compliance. *Information Management & Computer Security, 22*(1), 42–75.

Srivastava, S. C., & Chandra, S. (2018). SOCIAL PRESENCE IN VIRTUAL WORLD COLLABORATION: AN UNCERTAINTY REDUCTION PERSPECTIVE USING A MIXED METHODS APPROACH. *MIS Quarterly, 42*(3), 779-803.

Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research, 1*(3), 255–276.

Talaulicar, T., Grundei, J., & Werder, A. v. (2005). Strategic decision making in start-ups: the effect of top management team organization and processes on speed and comprehensiveness. *Journal of Business Venturing, 20*(4), 519–541.

Warkentin, M., Johnston, A. C., & Shropshire, J. (2011). The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. *European Journal of Information Systems, 20*(3), 267–284.

Weibel, A., Den Hartog, D. N., Gillespie, N., Searle, R., Six, F., & Skinner, D. (2016). How Do Controls Impact Employee Trust in the Employer? *Human Resource Management, 55*(3), 437–462.

Whitener, E. M. (2001). Do "high commitment" human resource practices affect employee commitment? *Journal of Management, 27*, 515–535.

Workman, M. (2009). How perceptions of justice affect security attitudes: suggestions for practitioners and researchers. *Information Management & Computer Security, 17*(4), 341–353.

Zhang, J., Reithel, B. J., & Li, H. (2009). Impact of perceived technical protection on security behaviors. *Information Management & Computer Security*, *17*(4), 330–340.