Employee Information Security Policy Compliance During and After Covid-19 Pandemic: A Decision Based on Activated Social Norms

Completed paper

Dailin (Ellen) Zheng
University of Colorado Denver
Dailin.zheng@ucdenver.edu

Zhiping Walter
University of Colorado Denver
Zhiping.walter@ucdenver.edu

ABSTRACT

This study highlights the role of rule appraisal in information systems security policy compliance when compliance behavior is not observed by other colleagues. We develop a model of information security policy compliance from the recognition-based decision-making perspective that incorporates social norm activation theory, social learning theory, and coping appraisal.

Keywords

Recognition-based decision-making, social norm activation theory, social learning theory, information security policy compliance

INTRODUCTION

Most of the existing research assumes that employees' decisions on information systems security policy (ISSP) compliance are based on cost-benefit analysis. For example, deterrence theory implies that employees follow ISSPs when the cost of punishment exceeds the benefit of rewards for ISSP violation (Gibbs 1968). Protection motivation theory (PMT) implies that employees

follow ISSPs when they believe that such recommended response would bring more benefits in mitigating or eliminating the threat than the response cost (Rogers 1975). The calculation of all possible costs and benefits requires much cognitive effort from decision makers. People usually conduct such calculations when they are making instrumental decisions, such as big financial investments, that have severe consequences on themselves and the decision maker is totally responsible for those consequences (Weber and Linemann 2007).

However, the consequences caused by an ISSP violation are mainly on the organization, not on the employee. Thus, ISSP compliance is an ethical decision. When making the ethical decision whether to follow ISSPs for the organizational benefit, employees tend to use heuristics (Bicherri 2006). When taking the heuristic route, employees make decisions based on their stored rules that are automatically triggered in that situation, rather than on the careful calculation of all possible benefits and costs (Bicchieri 2006).

The Covid-19 pandemic has brought many employees to work from home. Such remote-working mode is predicted to continue even after the pandemic as many employees are now reluctant to return to the workplace. In the remote-working mode, even the ISSP violation behaviors that could be easily caught in a shared workplace, such as writing down the password and keeping the account logged on while not attended, become private and could hardly be monitored, observed, and causing formal or informal sanctions as a result.

PMT is based on consequence-oriented decision-making and assumes people appraise the possible negative consequences of the external threat. The fear of the appraised negative consequences, along with the coping appraisal of the recommended action, motivates people to take recommended actions to protect themselves from those negative consequences, such as protecting their safety from natural disasters and protecting their health from diseases. In ethical decisions

such as ISSP compliance, employees evaluate the rule of ISSP compliance applied to the current situation. The feeling of responsibility based on the rule appraisal, along with the confidence in ability, motivates people to follow the rules.

Social norms are behavioral rules in the organization. In a company, all employees are required to follow organizational policies, including ISSPs. However, each individual has their own evaluation of the existence of the ISSP compliance norm based on their expectations of whether a sufficient number of employees in the company follow ISSPs and expect each individual to follow ISSPs as well. When working on-site, people are motivated to follow social norms out of the fear of social sanctions, the desire to please others, and the beliefs that such social norms are legitimate and well-founded (Bicchieri 2006). In a private environment, however, the negative consequences of social sanctions on ISSP violation and the positive consequences of pleasing others are no longer effective in motivating employee ISSP compliance since the compliance or violation behavior is not observed. Instead, when employees believe that they are expected to follow ISSPs by a sufficient number of colleagues in the company, they tend to perceive that such expectations from other colleagues are legitimate and thus they internalize this expectation into their own responsibility to follow ISSPs. Such expectations of other colleagues' conformation behavior can not only be formed by directly observing conforming behavior, but also by other cues such as the consequences of the conforming behavior (Bicchieri 2006). For example, private behaviors such as premarital sex cannot be directly observed. But if people observe the consequences of the low rate of teen pregnancy, they may infer that the practice of avoiding premarital sex is widely practiced (Bicchieri 2006).

In addition to inferring from the consequences of conforming behavior, employees develop expectations of other colleagues' actual compliance based on their own behavior and observation

in the past. As social learning theory implies, an employee's past experience of success in ISSP compliance and their observation of other employees' successes are the most two effective sources of the confidence in their own capabilities in ISSP compliance (Bandura 1997). The recognition of responsibility as the rule appraisal and the confidence in one's own capability in ISSP compliance, together, give rise to the motivation of ISSP compliance.

In sum, we investigate how activated social norms affect remote workers' appraisals of the responsibility and coping capacity of following ISSPs, and in turn, lead to their compliance intention.

RELATED WORK

Employee ISSP violation refers to intentional violation of organizational ISSPs without malicious intent to cause damage (Guo et al. 2011). An employee may intentionally violate an ISSP to save time and effort without maliciously intending to hurt their organization. Nevertheless, such behavior could cause damage or security risk to their organization. Most of the current models of employee compliance originated from behavioral models in social sciences assume that employees make decisions based on rationality, such as deterrence theory and PMT (e.g., Hsu et al. 2015; Menard et al. 2017; Moody et al. 2018).

According to deterrence theory and rational choice theory, employees calculate the possible costs and benefits of ISSP violation and tend to comply with ISSPs when the cost of punishments exceeds the benefit of rewards for ISSP violation (Gibbs 1968; Becker 1974). However, empirical results about the deterrent effects of punishments on violation intention have been mixed. Some studies found significant impact of perceived punishment severity and perceived enforcement certainty on compliance intention (e.g., Chen et al. 2012). Other studies found significant impact

of informal sanctions but nonsignificant impact of formal sanctions on compliance intention (Johnston et al. 2015).

Deterrent effects can be reduced or even eliminated when individuals adopt neutralization techniques to rationalize their behavior (Rogers and Buffalo 1974). Siponen and Vance (2010) found that sanctions had no significant impact on violation intention when neutralization techniques were deployed. Similarly, Teh and colleagues (2015) found significant impact of neutralization techniques on ISSP violation intention. A meta-analysis of deterrence theory in ISSP compliance research showed that deterrence theory explained ISSP compliance better in the context of malicious attacks than in the context of non-malicious attacks (Trang and Brendel 2019).

Health belief model and PMT predict that people are motivated to take protective actions out of fear of perceived threat (Becker 1974; Rogers 1975). PMT also assumes that protection motivation depends on individuals' evaluation of the possible negative consequence of the threat and the possible benefits of taking the recommended action, such as the effectiveness in protecting the followers from the threat. PMT is widely used in ISSP compliance research although empirical results have been mixed. For example, Bulgurcu and colleagues (2010) found significant impact of perceived threat vulnerability, perceived threat severity (a component of noncompliance cost tested in their model), self-efficacy, and response cost on compliance intention. Hina and colleagues (2019) also found significant impact of perceived threat vulnerability, perceived threat severity, and self-efficacy on ISSP compliance but didn't find significant impact of response cost. However, Menard and colleagues (2018) did not find any significant impact of threat severity, threat vulnerability, response efficacy, or self-efficacy on noncompliance intention after incorporating collectivism and psychological ownership in the model, although they did find significant impact of response cost on noncompliance intention. A recent meta-analysis study of

PMT in ISSP compliance research showed mixed impacts of threat appraisal on employee ISSP compliance across different situations such as workplace context versus personal context and mandatory compliance behavior versus voluntary protection behavior (Mou et al. 2022). We argue that those mixed results stem from the fact that employees decide whether to follow ISSPs based on rules instead of rational calculation.

The role of social influence was investigated in employee ISSP compliance research. Consistent with the theory of planned behavior, social norms and normative beliefs were found to impact compliance intention (Johnston et al. 2015; Hu et al. 2012; Siponen et al. 2010). Social norms impact employee ISSP compliance intention via social pressure and information for ISSP compliance as appropriate behavior in the company (Bicchieri 2006, Sowden et al. 2018).

Social pressure only works when the ISSP violation behavior can be observed by other colleagues. Due to the Covid-19 pandemic, many employees have been working remotely and many companies are considering making remote working a long-term strategy. In the remote working mode, employee ISSP compliance is not driven by social pressure as it is not observed by other colleagues. Instead, employees internalize social norms and feel personal responsibility to follow ISSPs out of benevolence.

Some ISSP compliance research discussed the role of intrinsic motivations in explaining employee ISSP compliance such as self-determination theory (Deci and Ryan 1980). Self-determination theory also implies that intrinsically motivated behaviors are based on the need of self-determination and competency. Empirical results showed that self-determined factors including autonomy, relevance, and competency were found to significantly impact compliance intention and offset the impact of most PMT factors (Menard et al. 2017). In our context, we argue that employees evaluate social norms and internalize those external rules as their own responsibility

(i.e., self-determination) and beliefs on their own capability (i.e., competency) in ISSP compliance, and thus develop intrinsic motivations to compliance.

In this paper, we propose an ISSP compliance model that examines how social norm activation affects remote workers' appraisal of the rule and coping capacity of ISSP compliance, and their compliance intention in turn.

THEORETICAL BACKGROUND

Decision-Making Modes

Weber and her colleagues (e.g., Weber et al. 2005; Weber and Linemann 2007) have distinguished decision modes including calculation-based decision making, affect-based decision making, and recognition-based decision making.

Calculation-based decisions include analytical thought (Weber and Linemann 2007). People tend to use calculation-based decision-making mode when making instrumental decisions with assessment-oriented motives (Weber et al. 2005).

Affect-based decisions are governed by conscious or unconscious drives or feelings (Weber and Linemann 2007). The affect-based decision-making modes are usually triggered by the psychological needs of decision makers and are selected when the decisions are based on romantic relationships (Weber and Linemann 2007; Weber et al. 2005).

Recognition-based decisions involve recognition of the situation as one of a type for which the decision maker knows the appropriate action (Weber and Linemann 2007).

Most of the existing ISSP compliance research assumes calculation-based decision making and investigates the external motivation to avoid the cost such as the sanctions imposed on and the negative consequences caused by ISSP violation (e.g., deterrence theory, protection motivation

theory, etc.) Calculation-based decision-making requests much cognitive effort from decision makers to calculate all possible costs and benefits. Such calculation-based decision-making is usually adopted when people are making instrumental decisions such as financial investment. However, whether to follow ISSPs is not a pure instrumental decision as it involves moral issues especially when compliance behavior is not observed. In this case, employees may choose to follow ISSPs to protect their values of following organizational rules and protecting the organization, regardless of the compliance cost borne by themselves (Bennis et al. 2010). In real life, employees usually don't spend much cognitive effort to make careful and thorough analysis when deciding whether to follow ISSP or not. Thus, calculation-based decision-making mode may not be the primary selection in the ISSP compliance context.

Protection Motivation Theory (PMT)

Rogers (1975) initially proposed protection motivation theory (PMT) based on the assumption of rational decision-making process. Under this assumption, people first appraise the possible consequences of the threat, especially the possible consequences on the decision maker themselves. When people see the need to cope with the threat based on their appraisal of those possible consequences, they evaluate the recommended coping mechanism and then decide whether to take the recommended protective behavior (Mou et al. 2022).

PMT has been found effective in explaining people's behavioral intention when the threat is targeted to themselves (e.g., Mahmoodabad et al. 2018). When the decision makers bear the consequences of their action, they are willing to take cognitive effort to calculate possible outcomes before making the decision. However, in the context of ISSP compliance in a private environment, employees' ISSP violation behavior is not observed, monitored, or sanctioned. In this case, ISSP compliance is an ethical decision to protect the company from information security

incidents but has little consequences on the employee as decision makers. When confronting ethical decisions for others' benefit, people tend to use heuristics and make decisions based on their rules, not on the calculation of outcomes (Bicchieri 2006). In our context, the ethical decision on whether to follow ISSPs to protect the company is a recognition-based decision facing which employees evaluate the appropriate rule to be applied in that situation, instead of a calculation-based decision facing which employees evaluate the possible consequences on themselves.

Social Norms

Social norms represent the rule of acceptable behavior in a social group (Fishbein and Ajzen 2010). Each individual interprets social norms based on their own understanding and forms their own perceived norms, which could vary from person to person even in the same social group. Perceived norms are classified into descriptive norms, which refer to beliefs about what most other people in the same social group would do in a particular situation, and injunctive norms, which refer to beliefs about what one ought to do in a similar situation as expected by most other people in the same social group (Lapinski and Rimal 2005).

The influence of perceived norms on an individual's behavior is called social influence. Social influence includes both normative influence and informational influence (Sowden et al. 2018, Bicchieri 2006). Normative influence is the personal and interpersonal processes that compel an individual to behave according to their perceived injunctive norm about a behavior within the social group; it occurs out of an individual's desire to be accepted by the group. Informational influence is the interpersonal processes that establish or challenge an individual's beliefs about a behavior; it occurs when individuals look to others for evidence of the prevalence behavior in the group (Sowden et al. 2018).

The cognitive dissonance theory suggests that individuals are motivated to adjust their behavior to conform to social norms in order to avoid sanctions from or maintain their moral self-image in the social group (Fointiat 2004). However, the coping theory implies that when people evaluate a situation as stressful and feel low controllability in such a situation, they turn to emotional-focused coping such as frustration. Those emotions drive them to adopt neutralization techniques to rationalize their norm violation instead of following norms (D'Arcy et al. 2014). Empirical research reported mixed results when investigating the impact of the expectation from colleagues on ISSP compliance. While Onumo and his colleagues (2021) proved the significant positive influence of employees' subjective norms on their intention to comply with a cybersecurity control measure, Grassegger and Nedbal (2021) didn't find significant impact of subjective norms on employees' intention to resist social engineering attacks. While most existing IS research focuses on normative influence when investigating social influence on ISSP compliance, a few studies examined the impact of descriptive norms but empirical results have been mixed as well. Chen and colleagues found that descriptive norms significantly impact employee ISSP compliance but Yazdanmehr and Wang (2016) found that the impact of descriptive norms on personal norms is insignificant. Many of the ISSP compliance behaviors are not observable by other colleagues such as using strong passwords and changing passwords regularly. Therefore, we focus on the informational influence of social norms on employee ISSP compliance.

Social Norm Activation

Even though social norms exist at the collective level in a company, each employee shows different preferences for the social norms. Bicchieri (2006) proposed a social norm activation model and posits that when an individual recognizes that a social norm exists and applies, most others conform and expect conformance to the norm in a similar situation, contingency condition,

empirical expectations condition, and normative expectations condition are all met, an individual will exhibit a preference for the social norm and thereby experience positive utility for conformance and negative utility for non-conformance. Specifically, empirical expectation refers to an individual's belief that most other people in the group follow the social norm. Normative expectation refers to an individual's belief that most other people in the group expect the individual to follow the social norm. Contingency condition means that the social norm exists and applies to the current situation.

As a member of the company, an employee's expectations and beliefs on social norms in the organization affect their personal beliefs such as the evaluation of their own ability.

Social Learning Theory

Social learning theory implies that mastery experiences and modeling or witnessing others' mastery experiences are the most two effective methods of developing self-efficacy beliefs (Bandura 1977; Gallagher 2012). When seeing others perform threatening activities without adverse consequences, individuals persuade themselves that they should be able to improve their performance at least. Empirical expectations are usually based on observations of others' behavior and own experiences in the past, which are two of the major sources of self-efficacy (Bandura 1997; Bicchieri 2006). Thus, we argue that employees with high empirical expectations tend to perceive high self-efficacy. In the empirical results, Kim and his colleagues (2021) have found that self-efficacy mediates the impact of descriptive norms on physical activity behaviors. In our context, we argue that, when employees believe most other colleagues successfully overcome the difficulties and comply with ISSPs, those employees tend to have confidence in their own capabilities in achieving similar success.

Identification

As a member of the company, an individual employee's evaluation of their working ability is affected by their relationship with the company. Identification, with an organization or anything else, is an active process by which individuals link themselves to elements in the social scene (Cheney 1987). It refers to the overlap between an employee's self-image and his or her image of the organization (Riketta and Dick 2005). Thus, we used identification to measure how employees view the organization as similar to themselves.

Tajfel's (1978) defined social identity as ''that part of an individual's self-concept which derives from their knowledge of their membership of a social group (or groups) together with the value and emotional significance attached to that membership''. Cameron (2004) further proposed a three-dimensional model of social identity including cognitive centrality, ingroup ties, and ingroup affect.

Cognitive centrality reflects the perceived importance of the social group and is usually measured with the amount of time an individual spent thinking about their membership with one social group when they belong to multiple social groups (Gurin and Markus 1989; Cameron 2004). Since employees are required to focus on their working in the company during their working hours and live on that salary, regardless of what other social groups they belong to. Thus, cognitive centrality doesn't really reflect employees' identification with the company that they work for and we exclude this dimension from our study.

Ingroup ties refer to the extent to which individuals feel part of or bound to particular social groups (Cameron 2004). Employees who perceive strong ingroup ties see themselves emotionally closed to the company. Such emotional closeness has been further measured with a sense of belonging with the group, along with perceptions that one "fits in", has strong ties, and shares a common

bond with the group or other group members. When employees perceive their coworkers as similar models to themselves, they tend to believe that they can achieve the same success as their coworkers have done and thus increase self-efficacy.

Ingroup affect refers to the specific emotions such as being glad or regretful that arise from group membership (Cameron 2004). Employees who feel strong ingroup affect have a positive evaluation of the social group and are happy with their group membership. Such employees tend to perceive high competence in coworkers. People actively seek proficient models who possess the competencies to which they aspire. Competent models teach observers knowledge, effective skills, and serviceable strategies. Such model performances not only provide controllability by demonstrating effective strategies for coping with threats in different situations, but they also provide predictability which reduces stress and increases the preparedness of feared persons in threatening activities.

Bandura (1997) argues that model competence overrides similarity in influencing individuals' self-efficacy as individuals believe that they can learn more from competent models than from similar models. He also argues that coping models are more influential than mastery models to observers' self-efficacy. Mastery models refer to those who perform calmly and faultlessly while coping models usually begin timorously but gradually overcome their difficulties by determined coping efforts. In addition, he argues that the multiplicity and diversity of modeling are both persuasive factors to increasing observers' self-efficacy. By observing similar success by many individuals (multiplicity of modeling) and the success of individuals with widely various characteristics (diversity of modeling), people have a reasonable basis for increasing their self-efficacy.

RESEARCH MODEL AND HYPOTHESES DEVELOPMENT

People tend to make ethical decisions based on their recognition of appropriate rules. In the organization, employees evaluate the rule of ISSP compliance, along with coping capacity, based on their beliefs about the social norm on ISSP compliance. Therefore, we propose to incorporate social norm activation theory into rule appraisal and coping appraisal. Our compliance model is shown in Figure 1. As discussed earlier, we used identification to capture the similarity factor in social learning theory that fits the organizational ISSP compliance context.

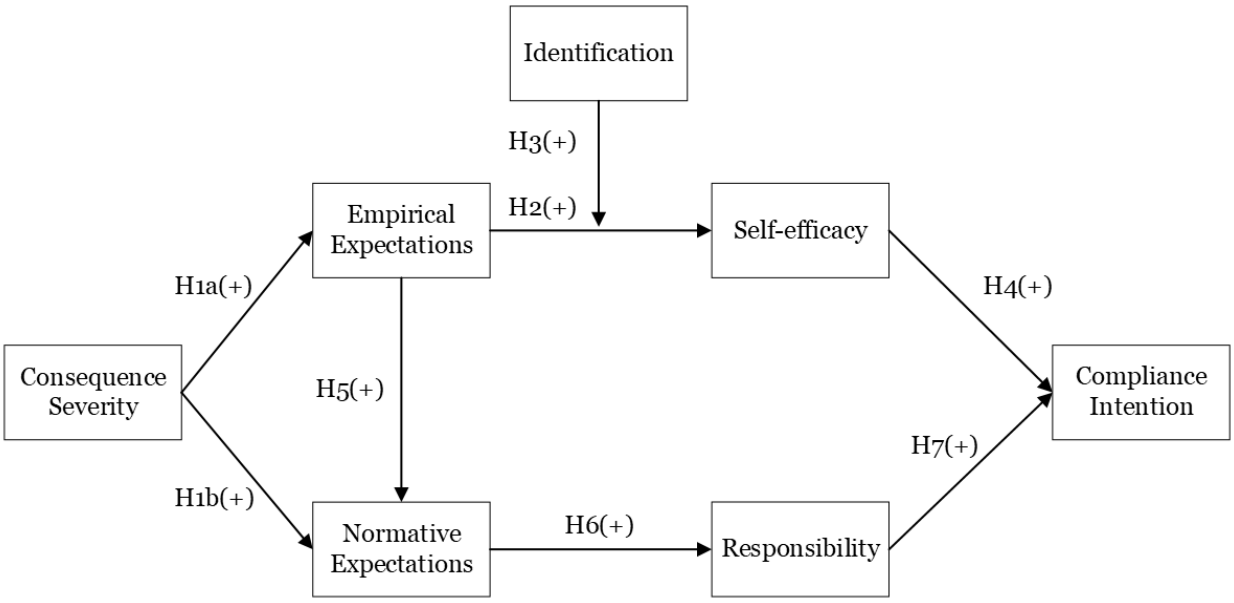

Figure 1. Research Model

In an organization, employees evaluate social norms from empirical expectations and normative expectations (Bicchieri 2006). Even in the same context, people may develop different expectations and beliefs depending on their subjective interpretation of situational cues (Bicchieri 2006). Norm activation theory implies that the damages to the company caused by IS incidents are a cue that organizational information systems are in need of protection (Schwartz 1977). The

need cue is salient to employees when they perceive the damages are serious, and thus has strong impact on employees' normative expectations and empirical expectations of ISSP compliance (Schwartz 1977; Bicchieri 2006). Thus, we hypothesize the following:

H1a: Consequence severity has a positive relationship with empirical expectations of employee ISSP compliance.

H1b: Consequence severity has a positive relationship with normative expectations of employee ISSP compliance.

Social comparison theory posits that people make assessments about their abilities by comparing themselves with others in the social midst (Rimal and Real 2005; Frestinger 1954). In the same vein, the social learning theory implies that mastery experience and vicarious experience are major sources of self-efficacy (Bandura 1977). When an employee has followed ISSPs themselves and observed other colleagues following ISSPs in similar situations, they tend to anticipate that most employees in the company to follow ISSPs in the current situation, and thus feel confident in their own ability to follow ISSPs in the current situation as they have done and observed before. In the empirical results, Kim and his colleagues (2021) have found that self-efficacy mediates the impact of descriptive norms on physical activity behaviors. In our context, we argue that, when employees believe most other colleagues successfully overcome the difficulties and comply with ISSPs, those employees tend to have confidence in their own capabilities in achieving similar success, and thus intend to follow ISSPs. Thus, we hypothesize the following:

H2: Empirical expectations of ISSP compliance have a positive relationship with self-efficacy.

Both social cognitive theory and social learning theory imply that employees' evaluation of their abilities is more affected by colleagues who are perceived as similar to employees themselves than by those who are perceived as divergent (Frestinger 1954; Bandura 1977). Bandura (1977) has discussed the similarity to performance and to attributes such as age, sex, educational and socioeconomic level, race, and ethnic designation. However, many other factors affect the influence of model similarity on observers' self-efficacy.

When the model characteristics are irrelevant to the task, their influence on observers' self-efficacy is weak. When people observe similar successes of many people and different people mastering difficult tasks, their self-efficacy is more likely to be affected compared to observing a single case. Also, observers may benefit more from seeing models overcome their difficulties by continuous effort than from seeing an ideal example. In aspirational modeling, people actively select and learn what they aspire to become from competent models, regardless of dissimilarity in attributes (Bandura 1977).

In literature, the empirical results of similarity's impact have been mixed (Kim et al. 2021; Priebe and Spink 2014). It could be explained by the inconsistency in the choices of similarity dimensions across studies including age, gender, values, way of thinking, etc. While working in the organization, employees' relationship with the organization inevitably more or less affects employees' perceptions and behavior. Thus, we incorporate identification to capture such influence.

Social learning theory also implies that people tend to pay attention to attractive and rewarding models and extract information from them (Bandura 1986). Employees with strong ingroup affect tend to observe the coping process of overcoming difficulties and achieving final success.

Recent empirical research revealed in their results that when observing others' performance, individuals who identify with the group tend to focus on the good examples of compliance while those who don't identify with the group are more likely to be affected by the bad examples of violation (Bicchieri et al. 2022). In summary, we argue that employees with high identification are more likely to increase self-efficacy compared to those with low identification through observing coworkers' ISSP compliance behavior. Thus, we hypothesize the following:

H3: Identification positively enhances the positive impact of empirical expectations of ISSP compliance on self-efficacy.

It has been widely approved in the literature that self-efficacy has a significant positive impact on employee ISSP compliance intention (Mou et al. 2022). Here we include this relationship as a control.

H4: Self-efficacy has a positive relationship with employee ISSP compliance intention.

In addition to imposing social pressure on meeting others' expectations in a social group, social norms also provide information about the appropriate behavior in a social situation (Bicchieri 2006, Sowden et al. 2018). In the organization, employees infer other colleagues' expectations of ISSP compliance from the empirical evidence of actual compliance around them. Also, out of reciprocity, when employees expect others to follow ISSPs, they tend to believe that other colleagues have the same expectations as well. Thus, we hypothesize the following:

H5: Empirical expectations of ISSP compliance have a positive relationship with normative expectations of ISSP compliance.

Jones (1991) proposed that the extent of social consensus, which is the social agreement on whether the action in question is ethical or not, affects individuals' judgment on the morality of

the action and then in turn affects their behavioral intention and actual behavior. Bicchieri (2006) summarized three major motivations for following others' expectations including the fear of negative sanctions, the desire to please others, and the acceptance that such expectations are well-founded and legitimate. In our context, employees' compliance with or violation of ISSPs is private and not monitored or observed by others. In this case, employees are motivated to comply with ISSPs when they accept that the expectations from other colleagues are legitimate and internalize such expectations as their own responsibility, not out of the fear of negative sanctions and the desire to please others. Thus, we hypothesize the following:

H6: Normative expectations of ISSP compliance have a positive relationship with responsibility of ISSP compliance.

Cognitive dissonance theory implies that people tend to act according to what they believe is right to avoid the cognitive dissonance between their beliefs and actions (Fointiat 2004). When employees believe that they have the responsibility to follow ISSPs, they tend to behave in line with their own beliefs. Norm activation theory also implies that employees tend to follow ISSPs when they feel themselves obligated to do so. Thus, we hypothesize the following:

H7: Responsibility has a positive relationship with employee ISSP compliance intention.

RESEARCH METHODOLOGY

We conducted a scenario-based survey to test our model and hypotheses. Three scenarios were newly developed and used. The first scenario was about sharing the password of an office computer with an outside technician. The second scenario was about opening an unsafe email attachment. The third scenario was providing confidential customer contact information to an outside friend. All those three behaviors, one in each scenario, were against organizational ISSPs but no

punishment was explicated. All scenarios were written in the third person to reduce social desirability bias (D'Arcy et al. 2014).

Measurements, Subjects, and Data Collection

Measurement scales were mostly adapted from existing items in the literature except for empirical expectations and responsibility. Consequence severity and normative expectations were adapted from Shawver and Miller (2017): Consequence severity was measured with a single 7-point Likert scale item and normative expectations was measured with three 7-point Likert scale items and two semantic differential scale items. Empirical expectations and Responsibility were self-developed by definition: Empirical expectations was measured with two semantic differential scale items and responsibility was measured with a single 7-point Likert scale item. Identification was adapted from Cameron (2004) and measured with four 7-point Likert scale items. Self-efficacy was adapted from Johnson and Warkentin (2010) and measured with three 7-point Likert scale items.

The data set was collected from Amazon Mechanic Turk (MTurk). The target population is current employees in the United States. We chose MTurk because the MTurk population is considered representative of the U.S. working population (Paolacci et al. 2010). The huge MTurk population also allows us to perform random sampling (Lowry et al. 2016).

A respondent was allowed to participate in only one batch of data collection. Each approved response received $0.75 in compensation. We received 1,536 responses in total. We used screening questions to exclude unqualified respondents who are under 18 years old, currently not employed, and have no access to company confidential data. The dataset was collected during the lockdown when most employees were working from home. To improve data quality, we disapproved responses that finished in an unreasonably short duration, failed embedded attention checking

questions (e.g., reporting a wrong answer as compared with the facts described in the given hypothetical scenario), or provided abnormal responses (e.g., one-end choices). Also, we only allowed high-performing survey takers (HIT approval rate >= 95%) to participate in our survey (Lowry et al. 2016). No responses contained missing data because a response to each question was mandatory. After data cleaning, the final study sample contained 833 responses. Table 1 describes the demographic information of our final sample.

Variable	Range	Frequency
Age	18-25 26-35 36-45 46-55 >55	81 337 214 126 75
Gender	Male Female Other	445 381 7
Education	Some college 2-year college degree 4-year college degree Postgraduate degree	122 73 439 199

Table 1. Sample Demographics (N=833)

Data Analyses and Results

Participation in the survey was fully voluntary and respondents were assured of anonymity. Following Aurigemma and Mattson (2017), we have taken both pre-hoc countermeasures and post-hoc analysis to mitigate and assess the potential impact of common method bias on our results. For post-hoc statistical analysis, we conducted Harman's single factor test and no single factor was found to account for most of the variance.

We used SmartPLS 3.0 for assessing the psychometric properties of constructs and for hypothesis testing. SmartPLS 3.0 utilizes partial least squares approach to structural equation modeling.

	Cronbach's Alpha	rho_A	Composite Reliability	Average Variance Extracted (AVE)
RSP	-	-	-	-
CNS	-	-	-	-
EE	0.93	0.93	0.96	0.93
IDN	0.98	1.13	0.98	0.94
NE	0.93	0.93	0.95	0.78
SE	0.80	0.85	0.88	0.71
INT	0.93	0.93	0.96	0.88

Note: RSP=responsibility; CNS=consequence severity; EE=empirical expectations; IDN=identification; NE=normative expectations; SE=self-efficacy; INT=intention.

Table 2. Reliability

As seen in Table 2, composite reliability, rho_A scores, and Cronbach's Alpha scores were all higher than 0.80. Average Variance Extracted (AVE) values for reflective constructs ranged from 0.71 to 0.94.

As seen in Table 3, item loadings ranged from 0.74 to 0.98 and were higher than all cross loadings. Item loadings between empirical expectations and normative expectations were slightly high ranging from 0.60 to 0.74, which is consistent with our hypothesis that there is a positive relationship between these two constructs. According to Fornell and Larcker (1981), differentiation is satisfied when the cross-correlations are lower than the within-construct correlations and convergence is satisfied when AVE is greater than 0.5.

	RSP	CNS	EE	IDN	NE	SE	INT
RSP	-	0.36	0.31	0.01	0.40	0.63	0.75
CNS	0.36	-	0.29	0.15	0.35	0.28	0.42
EE1	0.27	0.27	**0.96**	0.06	0.71	0.24	0.32
EE2	0.33	0.29	**0.97**	0.05	0.74	0.31	0.37
IDN1	0.02	0.16	0.05	**0.97**	0.03	-0.04	0.02
IDN2	-0.01	0.16	0.05	**0.98**	0.03	-0.07	-0.01
IDN3	0.04	0.12	0.05	**0.96**	0.04	-0.02	0.03
IDN4	0.02	0.12	0.06	**0.97**	0.05	-0.04	0.01
NE1	0.37	0.32	0.62	0.02	**0.88**	0.42	0.48
NE2	0.38	0.30	0.60	0.03	**0.88**	0.37	0.44
NE3	0.33	0.27	0.64	0.01	**0.86**	0.34	0.41
NE4	0.34	0.31	0.73	0.05	**0.89**	0.33	0.40
NE5	0.34	0.33	0.73	0.04	**0.90**	0.32	0.40
SE1	0.59	0.24	0.23	-0.06	0.33	**0.89**	0.61
SE2	0.42	0.12	0.15	-0.04	0.22	**0.74**	0.41
SE3	0.56	0.32	0.31	-0.03	0.42	**0.89**	0.66
INT1	0.78	0.39	0.32	0.01	0.43	0.61	**0.92**
INT2	0.65	0.39	0.34	-0.01	0.46	0.65	**0.94**
INT3	0.66	0.40	0.34	0.03	0.45	0.67	**0.95**

Note: RSP=responsibility; CNS=consequence severity; EE=empirical expectations; IDN=identification; NE=normative expectations; SE=self-efficacy; INT=intention.

Table 3. Loadings And Cross Loadings

As seen in Table 4, the square root of AVE for each construct ranged from 0.84 to 0.97 and was larger than the construct's correlations with other constructs. Results from Tables 2-4 together indicated acceptable convergent validity and discriminant validity (Nunnally and Bernstein 1994).

	Mean	SD	RSP	CNS	EE	IDN	NE	SE	INT
RSP	5.23	1.16	-						
CNS	4.00	1.60	0.36	-					
EE	4.33	1.12	0.31	0.29	**0.96**				
IDN	3.20	2.12	0.01	0.15	0.05	**0.97**			
NE	4.51	1.12	0.40	0.35	0.75	0.04	**0.88**		
SE	5.11	1.02	0.63	0.28	0.29	-0.05	0.40	**0.84**	
INT	5.02	1.28	0.75	0.42	0.36	0.01	0.48	0.68	**0.94**

Note: RSP=responsibility; CNS=consequence severity; EE=empirical expectations; IDN=identification; NE=normative expectations; SE=self-efficacy; INT=intention.

Table 4. Fornell-Larcker Criterion Results

For hypothesis testing, we used the PLS algorithm to estimate coefficients and ran the bootstrapping re-sampling algorithm with 1,000 re-samples to estimate t-statistics and p-values.

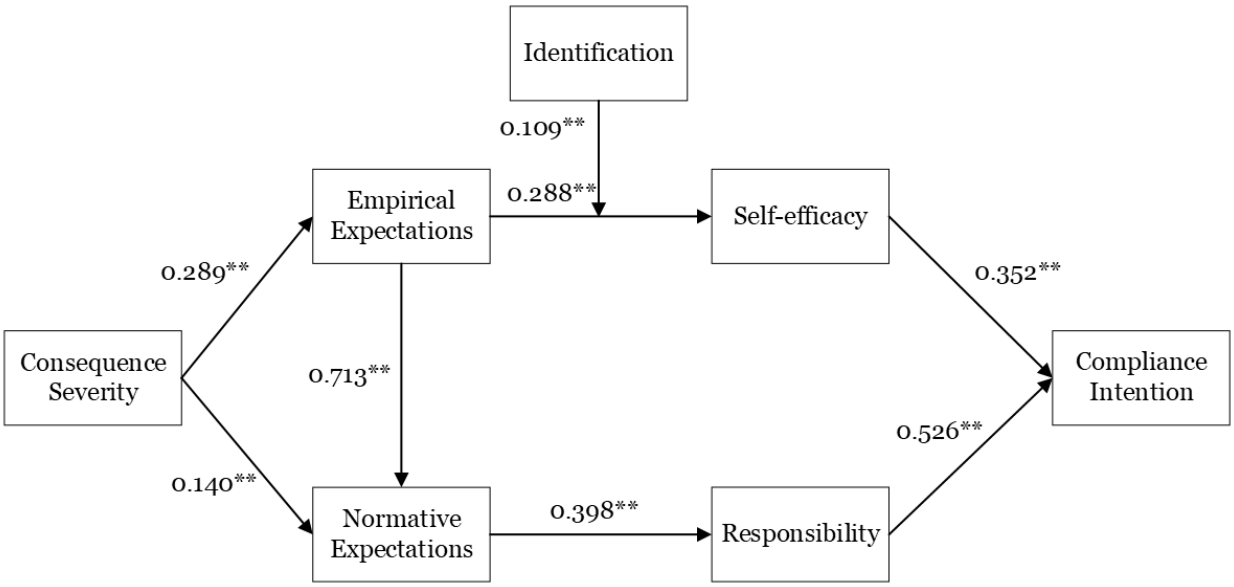

Figure 2. Model Testing Results

Paths	Coefficient	Bias-corrected CI [10%, 90%]	Result
CNS → EE	0.29	[0.24, 0.34]	Supported
CNS → NE	0.14	[0.11, 0.18]	Supported
EE →SE	0.29	[0.24, 0.34]	Supported
EE*IDN → SE	0.11	[0.06, 0.16]	Supported
SE → INT	0.35	[0.29, 0.41]	Supported
NE → RSP	0.40	[0.35, 0.44]	Supported
RSP →INT	0.53	[0.47, 0.59]	Supported

Note: RSP=responsibility; CNS=consequence severity; EE=empirical expectations; IDN=identification; NE=normative expectations; SE=self-efficacy; INT=intention.

Table 5. Summary of Hypotheses Testing

As seen in Figure 2 and in Table 5, our model explains 63.3% variance in compliance intention and all the hypotheses have been supported with significant results. Consequence severity has a

significant positive impact on both empirical expectations (β=0.289, p<0.01) and normative expectations (β=0.140, p<0.01). Therefore H1a and H1b are both supported. Empirical expectations have a significant positive impact on both self-efficacy (β=0.288, p<0.01) and normative expectations (β=0.713, p<0.01). Therefore H2 and H4 are both supported. Identification has a significant moderating impact on the relationship between empirical costs and self-efficacy (β=0.109, p<0.01). Therefore H3 is supported. Normative expectations have a significant positive impact on responsibility (β=0.398, p<0.01). Therefore H5 is supported. Responsibility has a significant positive impact on compliance intention (β=0.526, p<0.01). Therefore H6 is supported.

DISCUSSIONS

Many existing ISSP compliance theories and models, such as PMT and deterrence theory, assume employees use calculation-based decision-making when deciding whether to follow ISSPs. PMT, for example, implies that employees make decisions based on their calculation of the possible negative consequences caused by IS incidents (i.e., threat severity and threat vulnerability) and possible return and cost brought by compliance (i.e., response efficacy and response cost). However, employees usually don't take the cognitive effort to calculate all the possible costs and benefits when their ISSP compliance behavior has little consequences on themselves, especially when such behavior is not observed. Instead, employees tend to use the heuristic recognition-based decision-making mode and simply follow the rules as they see appropriate in that situation.

Our model explained 63.3% of the variance in compliance intention. We found that both responsibility and self-efficacy, as intrinsic motivations, significantly impact compliance intention. Specifically, we found that responsibility, as the recognized rule, has a higher impact on

compliance intention than self-efficacy which affects the possibility to get the desired consequences. These results have confirmed our argument that employees' decisions on ISSP compliance are driven by their recognized rules rather than calculated consequences.

As a member of the organization, each employee evaluates the appropriate rule and their own ability based on their interpretation of the situation. We found that employees' attention to situational cues, such as the seriousness of the damages caused by ISSP violation behavior, effectively activates employees' normative and empirical expectations of the ISSP compliance norm. Further, we found that normative expectations have high and strong impact on responsibility. These results show that employees internalize external rules of ISSP compliance into their own behavioral rule of ISSP compliance, which intrinsically motivate their compliance behavior.

As to enhancing the impact of empirical expectations on employees' self-efficacy, our results point to increasing employees' identification with the organization. Employees who perceive strong identification with the organization tend to perceive the norm followers around them are similar to themselves and in turn are more likely to increase self-efficacy through observing successful examples of those followers.

We acknowledge a few limitations. First, all items were self-reported. Second, we used a scenario-based survey. Unlike real life, the ethical dilemma described in the scenarios lacks details and complexity, which might cause bias in reported ISSP compliance intention. Future research could re-examine the model in experiments.

CONCLUSIONS

Existing ISSP compliance models based on rationality assume employees calculate all possible benefits and costs before making decisions on ISSP compliance. As many employees have been working remotely since Covid-19 pandemic, ISSP violation behavior is not observed by other colleagues and causes little consequences on employees as decision makers. However, employee ISSP compliance behavior still protects the organization from IS incidents. Such unobserved ISSP compliance behavior which benefits others rather than the decision maker is an ethical behavior by definition. When deciding whether to conduct an ethical behavior, people usually make decisions based on recognized rules rather than the evaluation of consequences. Since social norms represent the appropriate behavioral rule and affect individuals' beliefs and behaviors in a social group, we developed a model that examines how activated social norms affect employees' appraisals of their responsibility and coping capacity of ISSP compliance and in turn lead their compliance intention. Empirical results supported all our hypotheses. Our study contributes to employee ISSP compliance literature by highlighting the role of rule appraisal in employee ISSP compliance. Our study results also contribute to the application of social learning theory in employee ISSP compliance context by incorporating identification factor.

REFERENCES

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

Bandura, A. 1977. "Self-efficacy: toward a unifying theory of behavioral change," *Psychological Review* (84:2), pp. 191-215.

Bandura, A. 1986. *Social foundations of thought and action: a social cognitive theory*, Englewood Cliffs, New Jersey: Prentice Hall

Bandura, A. 1997. *Self-Efficacy: The Exercise of Control*, Macmillan.

Becker, M. H. 1974. "The Health Belief Model and Personal Health Behavior," *Health education monographs* (2), pp. 324-473.

Bennis, W. M., Medin, D. L., and Bartels, D. M. 2010. "The costs and benefits of calculation and moral rules," *Perspectives on Psychological Science* (5:2), pp. 187-202.

Bicchieri, C. 2006. *The grammar of society: The nature and dynamics of social norms*, Cambridge University Press.

Bicchieri, C., Dimant, E., Gächter, S., and Nosenzo, D. 2022. "Social proximity and the erosion of norm compliance," *Games and Economic Behavior* (132), pp. 59-72.

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

Cameron, J. E. 2004. "A three-factor model of social identity," *Self and identity* (3:3), pp. 239-262.

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

Cheney, G. 1983. "On the various and changing meanings of organizational membership: A field study of organizational identification," *Communications Monographs* (50:4), pp. 342-362.

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

Deci, E. L., and Ryan, R. M. 1980. "The empirical exploration of intrinsic motivational processes," *Advances in experimental social psychology* (13), pp. 39-80. Academic Press.

Festinger, L. 1954. "A theory of social comparison processes," *Human Relations* (7), pp. 117- 140.

Fishbein, M., and Ajzen, I. 2010. *Predicting and Changing Behavior: The Reasoned Action Approach*, New York: Psychology Press.

Fointiat, V. 2004. "'I Know What I Have To Do, But……'When Hyprcrisy Leads to Behavioral Change," *Social Behavior and Personality* (32:8), pp. 741-746.

Fornell, C., and Larcker, D. F. 1981. "Structural equation models with unobservable variables and measurement error: Algebra and statistics," pp. 382-388.

Gallagher, M. W. 2012. "Self-efficacy," pp. 314-320.

Gibbs, J. P. 1968. "Crime, Punishment, and Deterrence," *The Southwestern Social Science Quarterly*, pp. 515-530.

Grassegger, T., and Nedbal, D. 2021. "The role of employees' information security awareness on the intention to resist social engineering," *Procedia Computer Science* (181), pp. 59-66.

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

Gurin, P., and Markus, H. 1989. "Cognitive consequences of gender identity," In *The social identity of women*, S. Skevington and D. Baker (eds.), London: Sage, pp. 152 – 172.

Hina, S., Selvam, D. D. D. P., and Lowry, P. B. 2019. "Institutional Governance and Protection Motivation: Theoretical Insights into Shaping Employees' Security Compliance Behavior in Higher Education Institutions in the Developing World," *Computers & Security* (87) 101594, pp. 1-15.

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

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

Johnston, A. C., and Warkentin, M. 2010. "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly* (34:3), pp. 549-566.

Johnston, A. C., Warkentin, M., and Siponen, M. 2015. "An Enhanced Fear Appeal Rhetorical Framework," *MIS Quarterly* (39:1), pp. 113-134.

Jones, T. M. 1991. "Ethical Decision Making by Individuals in Organizations: An Issue-Contingent Model," *Academy of Management Review* (16:2), pp. 366-395.

Kim, J., Eys, M., and Robertson-Wilson, J. 2021. "'If they do it, so can I': a test of a moderated serial mediation model of descriptive norms, self-efficacy, and perceived similarity for predicting physical activity," *Psychology & Health*, (36:6), pp. 701-718.

Lapinski, M. K., and Rimal, R. N. 2005. "An explication of social norms," *Communication Theory* (15:2), pp. 127-147.

Lowry, P. B., D'Arcy, J., Hammer, B., and Moody, G. D. 2016. "'Cargo Cult' Science in Traditional Organization and Information Systems Survey Research: A Case for Using Nontraditional Methods of Data Collection, Including Mechanical Turk and Online Panels," *The Journal of Strategic Information Systems* (25:3), pp. 232-240.

Mazloomy Mahmoodabad, S. S., Sadeghi, R., Fallahzadeh, H., Rezaeian, M., Bidaki, R., and Khanjani, N. 2018. "Validity and Reliability of the Preventing Hookah Smoking (Phs) Questionnaire in Adolescents Based on the Protection Motivation Theory," *International Journal of Pediatrics (6:10)*, pp. 8327-8337.

Menard, P., Bott, G. J., and Crossler, R. E. 2017. "User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-Determination Theory," *Journal of Management Information Systems* (34:4), pp. 1203-1230.

Menard, P., Warkentin, M., and Lowry, P. B. 2018. "The Impact of Collectivism and Psychological Ownership on Protection Motivation: A Cross-Cultural Examination," *Computers & Security* (75), pp. 147-166.

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

Mou, J., Cohen, J. F., Bhattacherjee, A., and Kim, J. 2022. "A Test of Protection Motivation Theory in the Information Security Literature: A Meta-Analytic Structural Equation Modeling Approach," *Journal of the Association for Information Systems* (23:1), pp. 196-236.

Nunnally, J. C., and Bernstein, I. H. 1994. *Psychometric theory*. New York: McGraw-Hill.

Onumo, A., Ullah-Awan, I., and Cullen, A. 2021. "Assessing the moderating effect of security technologies on employees compliance with cybersecurity control procedures," *ACM Transactions on Management Information Systems (TMIS)* (12:2), pp. 1-29.

Paolacci, G., Chandler, J., and Ipeirotis, P. G. 2010. "Running Experiments on Amazon Mechanical Turk," *Judgment and Decision Making* (5:5), pp. 411-419.

Priebe, C. S., and Spink, K. S. 2014. "Blood, sweat, and the influence of others: The effect of descriptive norms on muscular endurance and task self-efficacy." *Psychology of Sport and Exercise* (15:5), pp. 491-497.

Riketta, M., and Van Dick, R. 2005. "Foci of attachment in organizations: A meta-analytic comparison of the strength and correlates of workgroup versus organizational identification and commitment," *Journal of Vocational Behavior* (67:3), pp. 490-510.

Rimal, R. N., and Real, K. 2005. "How behaviors are influenced by perceived norms: A test of the theory of normative social behavior," *Communication Research* (32), pp. 389–414.

Rogers, J. W., and Buffalo, M. 1974. "Neutralization Techniques: Toward a Simplified Measurement Scale," *Pacific Sociological Review* (17:3), pp. 313-331.

Rogers, R. W. 1975. "A Protection Motivation Theory of Fear Appeals and Attitude Change," *The Journal of Psychology* (91:1), p. 93-114.

Schwartz, S. H. (1977). Normative influences on altruism. In *Advances in experimental social psychology* (10), pp. 221-279. Academic Press.

Shawver, T. J., and Miller, W. F. 2017. "Moral Intensity Revisited: Measuring the Benefit of Accounting Ethics Interventions," *Journal of Business Ethics* (141:3), pp. 587-603.

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

Siponen, M., Pahnila, S., and Mahmood, M. A. 2010. "Compliance with Information Security Policies: An Empirical Investigation," *Computer* (43:2), pp. 64-71.

Sowden, S., Koletsi, S., Lymberopoulos, E., Militaru, E., Catmur, C., and Bird, G. 2018. "Quantifying compliance and acceptance through public and private social conformity," *Consciousness and Cognition* (65), pp. 359-367.

Tajfel, H. 1978. *Differentiation between social groups*, London: Academic Press.

Teh, P.-L., Ahmed, P. K., and D'Arcy, J. 2015. "What Drives Information Security Policy Violations among Banking Employees?: Insights from Neutralization and Social Exchange Theory," *Journal of Global Information Management (JGIM)* (23:1), pp. 44-64.

Trang, S., and Brendel, B. 2019. "A Meta-Analysis of Deterrence Theory in Information Security Policy Compliance Research," *Information Systems Frontiers* (21:6), pp. 1265-1284.

Weber, E. U., and Lindemann, P. G. 2007. "From intuition to analysis: Making decisions with our head, our heart, or by the book," *Intuition in judgment and decision making*, pp. 191-208.

Weber, E. U., Ames, D. R., and Blais, A. R. 2005. "'How do I choose thee? Let me count the ways': A textual analysis of similarities and differences in modes of decision-making in China and the United States," *Management and Organization Review* (1:1), pp. 87-118.

Yazdanmehr, A., and Wang, J. 2016. "Employees' information security policy compliance: A norm activation perspective," *Decision Support Systems* (92), pp. 36-46.