Journal of Computer Information Systems

ISSN: 0887-4417 (Print) 2380-2057 (Online) Journal homepage: http://www.tandfonline.com/loi/ucis20

Managers’ and Employees’ Differing Responses to Security Approaches

Puzant Balozian , Dorothy Leidner & Merrill Warkentin

To cite this article: Puzant Balozian , Dorothy Leidner & Merrill Warkentin (2017): Managers’ and Employees’ Differing Responses to Security Approaches, Journal of Computer Information Systems, DOI: 10.1080/08874417.2017.1318687

To link to this article: http://dx.doi.org/10.1080/08874417.2017.1318687

Published online: 24 May 2017.

JOURNAL OF COMPUTER INFORMATION SYSTEMS
https://doi.org/10.1080/08874417.2017.1318687

Taylor & Francis
Taylor & Francis Group

Managers' and Employees' Differing Responses to Security Approaches

Puzant Balozian [a], Dorothy Leidner [b], and Merrill Warkentin [c]

[a]Lebanese American University, Beirut, Lebanon; [b]Baylor University, Waco, TX, USA; [c]Mississippi State University, Mississippi State, MS, USA

ABSTRACT

Modern organizations face significant information security threats, to which they respond with various managerial techniques. It is widely believed that "one size does not fit all" for achieving employee information security policy compliance; nevertheless, it is yet to be determined which techniques work best to different organizational employees. We further this research stream by finding that different levels of users might be effectively motivated by different types of coercive and empowering techniques that are suitable to their level and position in the organizational chart. Our results suggest that participation in the ISP decision-making process might prove to be a more effective approach to motivate lower-level employees toward compliance and that enhancing the meaningfulness of policy compliance could be the preferred method among higher levels of management. Members within each level of the organization can be effectively influenced to comply with ISPs when such strategies are customized for their level.

KEYWORDS

Behavioral intention; coercive approach; compliance techniques; empowering approach; organizational position; security; security compliance

Introduction

On July 20, 2015, the Ashley Madison website's customer data were stolen, the systems were compromised, large quantities of supposedly confidential data were appropriated, and a small percentage of user account secret affairs data with matching credit card transactions were exposed to the public [8]. The hackers threatened to post more data online until the website closed. The company's negligent insider(s) probably clicked on a phishing email and thus unintentionally assisted the hackers [8], costing the company $370,000. The CEO resigned and two customers committed suicide after the hackers exposed their infidelity [65, 82]. Studies have consistently indicated that current employees are responsible for over 50% of reported security breaches [63]. Employees remain the most cited perpetrators of security incidents and their crimes tend to be more costly to their firms than those perpetrated by external sources [63]. Recent survey results found that employees were responsible for 57% of attacks against organizational digital assets, with 38% of these attacks caused by carelessness or lack of awareness [28]. These figures underscore the perennial mandate of decreasing the risk of negligent—as well as opportunistic and malicious—insiders in organizations. In view of these threats, the recent Cybersecurity Act of 2015 signed by President Barrack Obama gave network operators sweeping powers to monitor their own networks to catch both hackers and insiders alike [44].

Research about external security threats includes technical capabilities against security attacks [13], information disclosure [50], and spoofing [46]. Internal security threat research includes information sharing among peers [38], security factors in decisions pertaining cloud-based solutions [56], information message risk perceptions [58], and security adoption [66]. We focus on internal sources, otherwise known as insider threat. We define insiders as "…employees or others who have (1) access privileges and (2) intimate knowledge of internal organizational processes that may allow them to exploit weaknesses" [81]. A disgruntled employee who plants a logic bomb in the server to destroy data after he/she leaves the organization is an example of a malicious insider who can inflict great harm.

In contrast, other insiders may pose an information security threat by engaging in negligent behaviors not motivated by malice, acting either non-volitionally or volitionally for opportunistic purposes [69, 81]. An example of a non-volitional negligent insider is an employee who forgets to back up his/her data. An example of a volitional negligent insider is an employee who neglects updating his desktop's security software because he has deadlines to meet. Although non-malicious, these opportunistic insiders may nevertheless pose indirect threats to the information security of their organization. Negligent insiders can be categorized into two subcategories according to their ability and willingness: *willing but unable* to comply (naïve acts caused by lack of awareness or training) and *able but unwilling* to comply (opportunistic acts caused by competing goals or lack of motivation). The absence of malicious intent to harm the company is what differentiates these two subcategories from malicious insiders. For an expanded discussion of these categories of behavior, see [31, 61, 81].

Given that organizations must contend with all insider threats, ensuring information security policy (ISP) compliance by employees is a key component for realizing and maintaining information security. Many studies, such as [10, 18], examine the issue of insider threat mitigation by seeking to understand employee compliance with ISPs. Until recently, the primary theoretical lens for studying information security compliance behavior has been deterrence theory wherein

CONTACT Merrill Warkentin ✉ m.warkentin@msstate.edu Mississippi State University, Department of Management and Information Systems, College of Business, P.O. Box 9581, Mississippi State, MS 39762, USA.

studies examine how organizations can deter insiders from engaging in behaviors that threaten the organization's information security [19]. Recent studies have focused on persuasion theory (e.g., [11, 39]). Virtually no study has used both lenses simultaneously to investigate ISP compliance. Our study does just this. We investigate whether different levels of users (managers and employees) are affected by the same approaches (coercive vs. empowering) to ISP compliance. In so doing, our research makes an incremental advancement to information security research that is both novel and important in three ways. First, we contextualize theories––Theory X and Theory Y––and three relevant "empowerment" constructs from management, and test them in the important evaluation of ISP compliance behavior. Second, we test security research in a new cultural context (Middle Eastern) and we challenge the dominant coercive approach by contrasting it with empowering approaches, and we find that the latter is a promising way to approach security research in that particular culture. Third, we reveal that different levels of users may be affected by different types of coercive and empowering techniques in the context of information security compliance. We next present our model and hypotheses, followed by our methodology, findings, implications and conclusions.

Theoretical lens

Coercive vs. empowering approaches

Organizational management approaches toward compliance depict the attitude of managers toward the insider threat in organizations and reflect the driving beliefs behind how to address the threat effectively. The approach can take the form of coercive power (fear and punishment) or empowering motivation (nurture and development). These two approaches are consistent with McGregor's theory of motivation from organizational psychology. Theory X and Y describe two types of management styles: the coercive or authoritarian style, referred to as Theory X, and the enabling or participative style, referred to as Theory Y [55]. The coercive management style assumes that average people dislike work and need to be coerced into performing adequately [55] whereas the enabling style assumes that average people are willing, if enabled, to perform so as to achieve organizational objectives.

Drawing from McGregor's Theory X and Y we suggest that some managers may operate under the assumption that the average user has an inherent dislike of responsibility and will avoid compliance where possible [55]. Managers holding this assumption may apply coercion, command-and-control, and the threat of punishment for noncompliance. Other managers may operate under the assumption that users are self-directing, self-controlling responsible beings in the service of objectives to which they are committed [55]. Under this assumption, training and empowerment are essential elements in achieving organizational objectives. The IS discipline is rich in training [42] and awareness [27] research, but empowerment research has yet to be explicitly developed. In this study, we will develop an empowerment construct. We next describe how the coercive and empowering approaches may influence employee motivation to commit to ISP compliance.

Coercive approach

Rooted in the seminal work of criminologists such as Beccaria, Bentham, and Hobbes, general deterrence theory is the foundation of the coercive approach for controlling security behaviors [74]. General deterrence focuses on the indirect (or general) prevention of crime by making examples of specific perpetrators by quickly inflicting a severe and certain sanction on them. The severity of sanctions refers to the severity of the punishment that may be inflicted on noncompliant employees. The certainty of sanctions refers to the likelihood of getting caught and punished. Sanctions are only effective if employees are well informed about the penalties for breaching security [74]. This fear of sanctions has a deterrent effect in various contexts, and because deterrence impacts actual compliance [69], information security may be enhanced by conveying the potential for strong sanctions such as employment termination or criminal prosecution [21, 26]. Such severe sanctions are typically applied only to malicious insiders in cases of fraud, espionage, or purposeful disclosures, but not to negligent violators. However, in the absence of the threat of punishment, the policies and codes of ethics themselves offer minimal deterrence value [34]. More recently, Hsu, Lee and Straub [37] validated that coercive force increases IS security management adoption and assimilation. Consistent with this extant foundational literature, we offer our first two hypotheses.

H1: Certainty of sanctions is positively related to information security policy compliance intention.

H2: Severity of sanctions is positively related to information security policy compliance intention.

Empowering approach

In contrast to deterrence, empowerment has not attracted much attention in ISP compliance research [67]. Empowering users might be an alternative to sanctions in eliciting ISP compliance. Empowering leadership is defined as "sharing power with employees with a view toward enhancing their motivation and investment in their work" [83]. Empowerment confers greater authority to employees than they would otherwise enjoy [16]. When the leadership empowers employees, the latter become creative [83] and/or more productive [3].

Forms of empowerment as a motivational approach include fostering participation in decision-making, enhancing the meaningfulness of work, expressing confidence in high performance, and providing autonomy from bureaucratic constraints [83]. One form of empowerment that has already been studied in the context of ISP compliance is the whistleblowing policy [52]. Therefore, we limit our study to the first three forms of empowerment, as identified in Zhang and Bartol [52], namely, (1) fostering participation in decision-making, (2) enhancing the meaningfulness of work, and (3) expressing confidence in high performance.

Effect of participation in decision-making on intention to comply

Given that effective information security is dependent on user awareness of the risks to information security, user participation might be useful in achieving this awareness [71]. User participation is the extent to which users or their representatives take part in systems development [6]. Extending this notion to ISP, we define user participation in ISP decision-making as the extent to which users or their representatives take part in decisions during the formulation of ISPs.

Employees' participation in decision-making can be manifested in different policy-making initiatives ranging from implementing or adopting a new system to ISP development [53,71]. Markus and Mao [53] suggest that users who exert effort and exercise influence in systems development projects perceive the new system to be more important and relevant than do users who are not involved. This perception positively influences not just their attitudes but also their system usage level [35].

Spears and Barki [71] found that user participation in information security risk analysis and control design directly raised the perception of improvements in the policies, procedures, safeguards, and countermeasures that prevent, detect, or minimize a security breach. Although important in terms of empowerment research, their study did not assess the impact of user participation on ISP compliance intention. We argue that when employees are exposed to security risks and are invited to contribute to the formulation and writing of policies, they will be more likely to comply with these policies. This is a form of empowerment. Therefore, we hypothesize the following:

H3: User participation in decision-making regarding security policies is positively related to the information security policy compliance intention.

Effect of enhancing meaningfulness on intention to comply

Zhang and Bartol [83] defined enhancing the meaningfulness of work as helping an employee understand the importance of his/her contribution to the overall organizational effectiveness. In the information security context, we conceptualize the meaningfulness of ISP compliance as helping an employee understand the importance of his/her contribution to the overall organizational information security through his policy compliance.

In the broader management context, work meaningfulness and corporate citizenship positively impact each other [47]. When employees see and understand why they are doing the work they are doing, they cultivate a stronger sense of responsibility and loyalty toward the employer and even increase their work performance. Experienced meaningfulness refers to the sense of meaning an individual draws from engaging in work activities [25], which positively affects work outcomes such as work engagement and commitment to the task at hand [7].

Applying these concepts to ISP compliance, we suggest that similar psychological forces influence user compliance, such that users may experience a sense of significance and feel that they are doing something beneficial for the organization, community, or world if they understand the purpose of the behaviors entailed in ISP compliance. When users understand why they should comply with ISPs, they will commit themselves more fully to compliance.

Thus, we argue that management should not only demand policy compliance, for example, by disabling computer access if a password is not changed on schedule. Rather, management needs to make a concerted effort to explain to employees, in practical terms and by including the technical details if needed, *why* regularly following policy mandates, such as regularly changing a password, is important and how this behavior may affect the employee's daily work life and work files. In addition, management can be transparent in informing employees of security breaches and illustrate how many of the breaches could have been thwarted had each user obliged the policy. In so doing, ISP compliance may become more meaningful to the users. Thus, we hypothesize the following:

H4: Enhancing the meaningfulness of information security policy compliance is positively related to the information security policy compliance intention.

Effect of expressing confidence on intention to comply

When leaders express confidence in employees and have high expectations of them, employees experience feelings of empowerment and increased levels of performance [16]. In the context of ISP compliance, we define the empowerment approach of expressing confidence as the managerial-level belief and verbal or behavioral expressions of confidence toward employees' high-level performance and competence regarding ISP compliance. One of the primary reasons that managerial expressions of confidence in employees have a positive impact on employee performance is because these increase employees' self-efficacy. External cues and organizational support have been shown to enhance compliance self-efficacy, which in turn has been shown to increase compliance intentions [79]. Moreover, managerial expressions of confidence in employees are an important form of managerial feedback. Managerial feedback benefits employees in terms of individual as well as team performance and morale [2]. Such feedback may strengthen the confidence of the employees in what they are doing and increase their self-efficacy.

With regard to information use and policy compliance, the perception of self-efficacy refers to the perception held by an individual of his ability to effectively use a system or, in the case of policy compliance, effectively abide by the policy. Tangible expressions from management about employees' high-level performance ability may cause higher perceptions of self-efficacy, thereby contributing to an increase in compliance intention [79]. Positive feedback from management about users' ability to protect the organization's systems and data from security breaches may increase the confidence of users in the importance of compliance and in their ability and intent to comply with security policies. Thus, we hypothesize the following:

H5: Expressions of managerial confidence toward users' high-level performance regarding information security compliance is positively related to the information security policy compliance intention.

Testing both punishments and rewards together are contrasted with the results from testing either punishment or rewards alone [4]. Within IS research, Son [70] tested deterrence (extrinsic model) along with perceived legitimacy and congruence (intrinsic model) and found that only the intrinsic model was significant. Although deterrence is a well-established significant construct, testing it with another approach yields different results. We test coercion with an empowering approach, which is an important yet seldom investigated in information security research. While positive approaches have been evaluated, they are not empowerments per se. For example, Bulgurcu et al. [12] tested intrinsic benefits (defined as contentment, satisfaction, and accomplishment), safety (perception that IT resources at work are safeguarded because of compliance), and rewards (tangible and intangible compensation in return for compliance). Son [70] tested the intrinsic model (perceived legitimacy and perceived congruency). These emerging positive approaches are not empowering, i.e., things that management can do to practically empower users. Our focus on empowerment approaches is an important extension to the IS security policy compliance research.

On the left side of our research model (see Figure 1), we show sanction certainty and severity, which together comprise the coercive approach. On the right side, we show the constructs of the empowering approach: participation in decision-making, enhancing the meaningfulness of ISP compliance, and expressing confidence in high performance regarding compliance. We also control the model for the position of the user (managers vs. employees).

Research methodology

We utilized a survey research design that drew data from multiple organizations. We adapted previously validated scales to measure the constructs in our research model. Suitable scales were found in two seminal works in management (see Appendix A for the measurement items). To retain the psychometric properties of the measures, each item in the questionnaire was measured in its respective original scale with 5-, 7-, or 11-point Likert scales. After data collection, we normalized and transformed these measures to an 11-point Likert scale format to increase the variance of the data [22, 23]. This type of normalization does not harm the data in terms of the mean scores and measures of dispersion and shape [22, 23].

An expert panel comprised of 11 IT professionals and academicians evaluated the content validity of the items. After several iterations and changes regarding wording, the panel reached a consensus that the items were relevant, realistic, genuine, and clearly written. IT professionals in the country where we conducted data collection were also contacted to verify the relevancy of some of our technical questions in the environment of the primary data respondents (e.g., relevance and/or existence of periodic audits of unauthorized software use on organizational computers in the country). Furthermore, a panel of 10 respondents from the same data collection sample pool read the items to evaluate their content relevancy and clarity. In summary, all the individuals in the academic and professional expert panels reached a consensus that the items were relevant, genuine, and readable, thereby confirming the content validity.

Pilot test and primary data collection

We pretested the survey with 30 employees and professionals from our primary data sample pool. The reliability of the measurement items as well as the discriminant and convergent validity for the reflective constructs were evaluated using AVE, composite reliability, Cronbach's alpha, and factor loadings.

Primary data for this research were collected by administering a survey to young professionals attending an educational program in Lebanon, a Middle Eastern country. All respondents were either employees or managers in their workplaces (60% and 40%, respectively) representing more than 22 different organizations. To increase the voluntary participation rate, we offered the employees four prizes of US$100 through a raffle, while retaining the anonymity of the survey itself.

We used both paper-based and online data collection, thereby mitigating the common method bias from a single

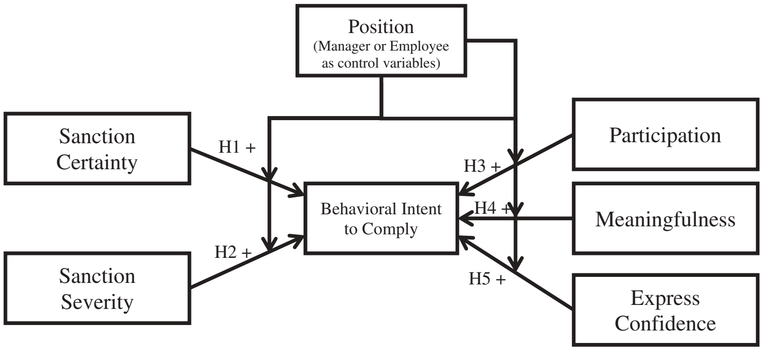

Figure 1. Research model.

data collection method [60]. In total, 187 usable surveys were gathered from 380 professionals for a response rate of 49%. The sample is more than three times the required sample size (60) to evaluate our model according to the rule of ten heuristic [5]. Appendix B shows the descriptive statistics of the primary data. We controlled for gender, age, industry and size of organization. These control variables did not alter the analysis results.

Common method variance

Common method variance, which can lead to systematic error and wrong conclusions about the relationships between constructs, is a bias caused by the method of collecting the data rather than by the constructs and measurement items [60]. We observed Podsakoff et al.'s [60] recommendations to decrease the sources of common method variance, including several procedural remedies, as indicated in Appendix C. We also performed statistical tests to further mitigate these concerns. We performed Harman's one-factor test [60], which consists of entering all the items in an unrotated factor analysis to see if a single factor will emerge or explain the majority of the variance, which can indicate common method bias. In our study, 16 factors emerged, the largest of which accounted for 23% of the variance. Second, the test of partial correlation was applied, in which a marker variable is introduced into the model to see if it makes a difference in the relationships [60] (see Appendix A for the marker variable items). The relationships were altered neither in their significance nor in their direction with and without the marker variable. Therefore, common method bias is not a significant issue in this study.

Model analysis

We analyzed our theoretical model using partial least squares analysis [64]. We chose the component-based (PLS) rather than covariance-based SEM technique to facilitate valid model development [5,15]. We used SmartPLS version 2.0 (M3) Beta [64] with 5000 bootstrapping for the analysis and determination of the paths' significance in the model.

The measurement model test comprises internal reliability and convergent and discriminant validity of the measurement items. Table 1 shows the internal consistency reliabilities. All constructs but one, scored >.7, which is the recommended threshold of Cronbach's alpha [33]. The composite reliability exceeds the recommended thresholds of .7 [30].

The items demonstrated satisfactory convergent and discriminant validity. Convergent validity is satisfied when the average extracted variance of each construct is >.5 [30]. Discriminant validity is achieved when the square root of AVE of each construct in the diagonal is greater than the variance of all the other constructs [15]. The items showed satisfactory levels of discriminant validity. Discriminant and convergent validity are further tested in the loadings and cross loadings. Generally, item loadings greater than 0.6 on their related factor are considered acceptable [5]. As expected, the loadings within the construct met the threshold, and they were higher than the loadings across constructs. In sum, the psychometric properties are met, and the scales show acceptable convergent and discriminant validity.

Table 1. Reliability measures.

Construct	AVE	Composite reliability	Cronbach's alpha
Intention to comply	0.673	0.861	0.758
Certainty	0.556	0.789	0.601
Severity	0.649	0.880	0.830
Meaningfulness	0.704	0.877	0.790
Participation	0.641	0.842	0.727

Expressing confidence in high performance was a formative construct for which the outer loadings are assigned beta weights in a regression formula [59]. The weight for each item signifies the item's contribution to the construct. The weights of the items are .75, .59, and −.06. According to Hair et al. [32], the non-significance of the beta weights are not enough to make an informed statistical decision on whether to drop an item. Two other indicators should be consulted in the following order: if the outer weight is significant, the items should be kept. If they are not significant, the outer loadings should be consulted. The latter, also known as the absolute contribution (vs. relative contribution of beta weights), should be above .5. If a formative item has a high beta weight and an outer loading >.5, then the item should be kept. If the beta weight is significant but the outer loading is <.5, there are two options. Either the outer loading is not significant, in which case dropping the item is advised, or the outer loading is significant, in which case the researchers have to choose whether they want to keep the item. In our data, none of the items had an insignificant outer loading. Table 2 displays the test results and the decision process of outer weights of our formative construct.

The structural model (Figure 2) estimates the path coefficients, which are the measures of the relationship strengths between dependent and independent variables, and the coefficient of determination (R^2), which is the amount of variance accounted for by the independent variables. Figure 2 shows the paths and prediction levels of the model. Both the coercive and the empowering approaches predict ~26.4% of the variance in the intention to comply. The structural model supported two of the five hypothesized relationships. Enhancing the meaningfulness of ISP compliance and expressing confidence in effective compliance are positively related to the intention to comply (H4: $\beta = .225$, $p < .01$ and H5: $\beta = .402$, $p < .001$, respectively). Fostering participation in decision-making was significant but unexpectedly negative (H3: $\beta = -.133$, $p < .05$). Thus, H3 was not supported. The paths of coercive approach techniques when considered vis-a-vis empowering approach techniques were also not supported (H1: certainty of sanctions and H2: severity of sanctions).

Results

Having tested coercive and empowering approaches in the same model, we observe that the coercive approach is not significant when empowerment is in place. We note that the severity and certainty of sanctions tested alone are significant; however, when the whole model is tested together, the coercive approach loses its significance and power. Thus, our first

Table 2. Outer weights' significance testing results.

			Step B: Outer loadings (absolute contribution) >.5	
Formative construct		Step A: Outer weights (relative contribution)	Step C: Significance	Suggestion – Decision
Expressing confidence in high performance	Conf1	0.303768 ***	0.517239 ***	Definitely keep - Kept
	Conf2	0.467041 ***	0.777867 ***	Definitely keep - Kept
	Conf3	−0.057694	0.441515 ***	Consider removing – Removed

***p < 0.001.

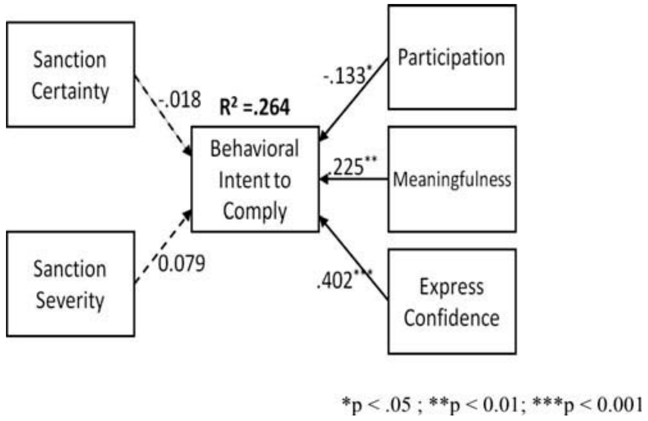

Figure 2. Structural model (managers and employees together without controlling for user position). *p < .05; **p < 0.01; ***p < 0.001

major finding is that the coercive approach becomes insignificant when tested with the empowering approach. Previous studies have typically looked at either coercive or empowering approaches separately with an emphasis on coercive approaches for ensuring compliance. By examining both approaches in the same model, we shed light on the relative effectiveness of each. Our results should encourage future researchers to continue delving further into empowering approaches.

The three components of the empowering approach are significant. However, the unexpected negative sign of one of them, participation in decision-making, warrants mention. In management studies of participation, it has been observed that, although rare, participation sometimes has negative consequences. For example, McClean et al. [54] found that voice may sometimes lead to exit/turnover. In their study, voice served as a measure of the engagement of employees in challenging the status quo to improve the work setting. Interestingly, making their voice heard is positively related to turnover (voice leads to exit) if their direct managers are not able or willing to engage in change. In a similar vein, recent IS research has demonstrated that employees participating in IS strategy development were only satisfied with the result if they were involved in the development of highly innovative strategies; when they were involved in developing conservative IS strategies, they expressed dissatisfaction with the result and did not see the value of the strategy [49]. Perhaps something similar is at play in our study of compliance, where participation in decision-making apparently led to dissatisfaction, or, more specifically, the intent to not comply. It is possible that users involved in security policy decision-making try to make a case for less rigid policies; however, their voices are ignored and the policies remain rigid. In such cases, they may be unhappy and report low intention to comply. Having a voice is not the same as being heard. At his point, we can only speculate as to why users who were involved in security policy decisions would express the intent to not comply with the policies. Future research should delve more deeply into this paradoxical issue.

To further probe this issue with our own data, we conducted a post-hoc analysis. We divided our sample into those who reported managerial experience (whom we label as managers) and those who reported no managerial experience (whom we label as employees). Recent literature indicates significant differences between managers and employees across a plethora of technology-related domains, including the response to and use of HRM systems [45] and the symbolic and behavioral response to enterprise social media systems [43].

Post-hoc analysis and discussion

Our post-hoc analysis investigates whether employee status, specifically managers versus employees, plays a role in IS compliance intention. Managers and employees constituted 60% (112 participants) and 40% (75 participants) of our sample data, respectively. This categorization was based on a question asking the number of years of work experience followed by a question asking the number of years of management experience.

Figures 3a and 3b show the paths and prediction levels of the employees-only vs. managers-only. The employees-only model and the managers-only model predict ~33.3% and ~28.4% of variance, respectively. The figures demonstrate that the two groups have different significant antecedents for compliance intention. Whereas employees are motivated by participation in decision-making and expressing confidence (H3: β = .189, p < .05 and H5: β = .506, p < .001, respectively), managers are motivated by the severity of sanctions and enhancing the meaningfulness of compliance (H2: β = .132, p < .05 and H4: β = .379, p < .001, respectively) as well as expressions of confidence in their high performance (H5: β = .286, p < .001). Table 3 gives the summary of the findings.

The first insight from this analysis is that participation in decision-making was significant only for employees. We suggest that subordinates are grateful for an opportunity to be heard and will strive to make their opinions and voices count [54]. Thus, a managerial approach that empowers users to participate in forming, developing, and improving ISPs may

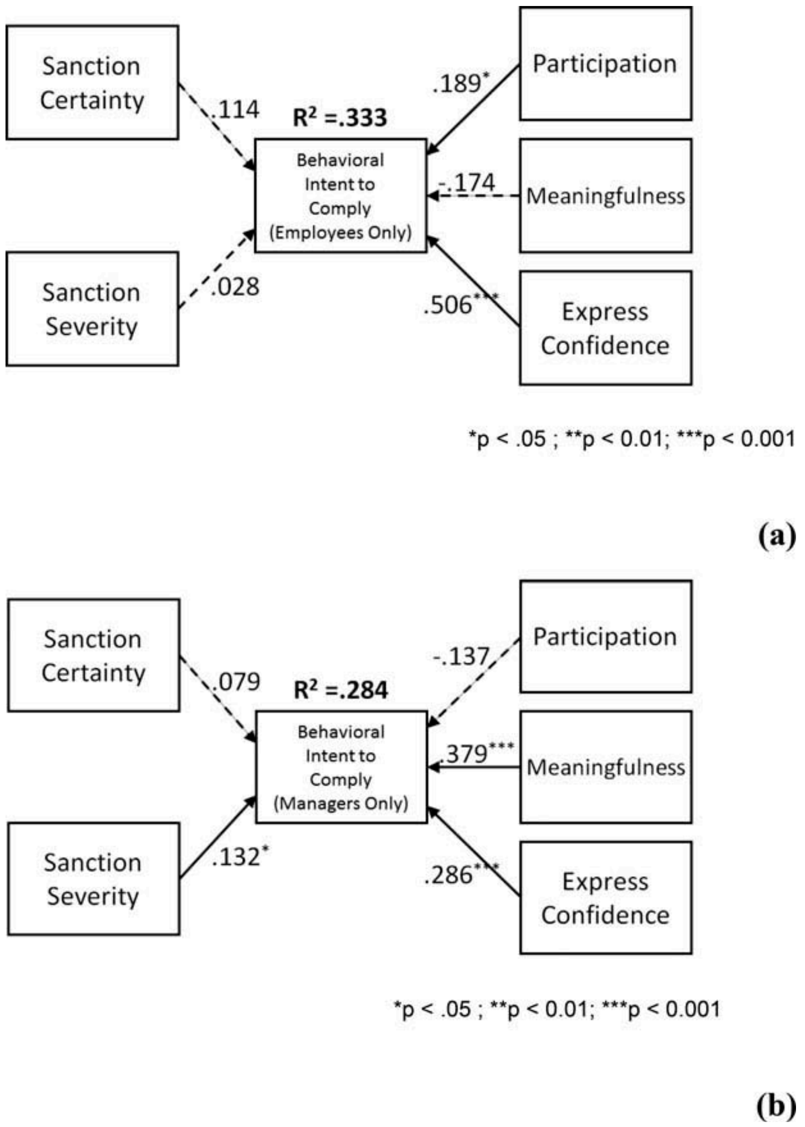

Figure 3. Post-hoc analysis for (a) employees and (b) managers.

Table 3. Summary of findings.

Research model	Path and significance	Hypothesis support
Main (R^2 = .264)		
Certainty to Intention (H1)	-.018	No
Severity to Intention (H2)	.079	No
Participation to Intention (H3)	-.133*	No
Meaningfulness to Intention (H4)	.225**	Yes
Expressing Confidence to Intention (H5)	.402***	Yes
Post-Hoc (Employees) R^2 = .333		
Certainty to Intention (H1′)	.114	No
Severity to Intention (H2′)	.028	No
Participation to Intention (H3′)	.189*	Yes
Meaningfulness to Intention (H4′)	-.174	No
Expressing Confidence to Intention (H5′)	.506***	Yes
Post-Hoc (Managers) R^2 = .284		
Certainty to Intention (H1″)	.079	No
Severity to Intention (H2″)	.132*	No
Participation to Intention (H3″)	-.137	No
Meaningfulness to Intention (H4″)	.379***	Yes
Expressing Confidence to Intention (H5″)	.286***	Yes

*$p < .05$; **$p < 0.01$; ***$p < 0.001$.

appeal to employees and increase their motivation toward higher compliance intention. However, this approach does not appeal to managers. This could be attributable to several reasons. Managers may already be so involved with decisions of various natures that policy compliance decisions do not strike them as an appropriate use of their time. Possibly, like the managers in the study on participation and involvement in IS strategy decisions, managers in our study only wish to be involved in decisions outside of their functional unit when those decisions are highly innovative or of strategic importance to the organization. Furthermore, while IS managers would undoubtedly label security policy compliance decisions as strategically important, general managers may not share this view and may go so far as to resent having to spend time on what they might consider as largely mundane decision-making in another functional unit. Alternatively, the managers may have had such high confidence in the IS department's ability to make security policy decisions that they did not feel the need to be involved and even felt that their involvement signaled a lack of competence of the IS management. We cannot be certain as to why employees, but not managers, respond favorably to involvement in IS security policy compliance. It is an interesting contrast that merits future research attention.

Second, enhancing the meaningfulness of compliance appealed more to managers than to employees, which may be partly explained by the contrast between "digital natives" (the younger employees in our study) and "digital immigrants" (the older managers) [62], in which younger individuals are quicker to adopt the new technologies available during their youth than are their elders, who tend to stick with their habitual ways of doing things until their technologies are virtually obsolete [29, 57]. Younger "employees" exhibit greater knowledge of technology, so may accept IS security policies more readily than managers. Another explanation lies in work roles. It is tenable to consider that non-managerial employees might be accustomed to simply following instructions, are less inclined to challenge policies, and, consequently, are less in need of justifications for policies as a motivation to abide by them. In contrast, managers are accustomed to greater job autonomy and might be inclined to disregard policies that they perceive as interfering with their ability to perform at a high level. In this case, managers would need to be convinced of the meaningfulness of the policies in order to gain their compliance. Future research is necessary to theorize and further examine the differences in response of the empowerment approach to policy compliance based on work roles.

A third insight from our analysis is that while the severity of the punishment for managers is significantly related to their intention to comply, it is not significant for employees. Although the severity of punishment could have been eclipsed in the perception of employees by a more positive empowering approach, the idea of punishment is still relevant and a powerful force to motivate managers toward compliance intention. Straub and Nance [73] tested the offender position and severity of discipline and found that high-privilege users (including organizational managers and IT senior executives) receive milder discipline than medium- or low-privilege employees. They conclude that organizations should stop this favored treatment because it diminishes the deterrent effect on other employees. Our data show that this only seems to be a problem for managers and not for employees. Employees are not affected by the severity of the punishment; instead, they are only affected by the potential of punishment. In contrast, more severe punishments are necessary to motivate managers to comply. This suggests that managers may have an elevated view of their own value and may assume a certain carte blanche with respect to policies that they do not wish to follow. They are motivated to abide by such policies only when the potential punishment is quite substantial.

In comparing managers' and employees' responses to coercive and empowering approaches to ISP compliance, we observe only one common motivational factor for both groups—the expression of confidence by immediate supervisors for effective compliance. Perhaps this attests to the power of positive reinforcement across hierarchical levels in organizations.

In summary, our post-hoc analysis provides vivid indications of substantial differences in responses to motivational ploys depending on individuals' organizational role. While it may not always be feasible for an IS department to target different user groups with different motivational approaches to encourage compliance, at the very least, managers should be aware of these differences in responses and work to formulate a security compliance policy that will align best with the targeted users [41, 77]. Future research is needed to examine specific aspects of security policies and how IS departments can vary their motivational approach depending on the predominant users of the systems in question.

Contributions

This study contributes to information security research in at least three important ways. First, it expands the nomological net by applying relevant constructs from reference disciplines, including those from the theoretical lens of Theory X and Y, and tests them in the information security context, where they are found to be relevant. Second, it challenges the coercive approach overemphasized in ISP research and contrasts it with empowering approaches, and it finds the latter a more effective avenue for security in a Middle Eastern context, an under-researched region. Third, it reveals that different levels of users may be affected by different types of coercive and empowering techniques regarding ISP compliance.

Corley and Gioia [17] argue that a theoretical contribution brings with it novelty and usefulness. Our research model is new in that it incorporates both coercive and empowering approaches and introduces several new variables—participation in ISP decision-making, awareness of the meaningfulness of security policy compliance, and supervisor expression of confidence in the compliance behavior of subordinates—to ISP compliance research. Such findings provide useful insights into both future research and managerial practice. At the same time, our model is an extension of the existing ISP compliance research that has drawn heavily from the criminology theory of general deterrence. Moreover, our study makes a solid empirical contribution, rather than a purely theoretical one. As recently argued by Agerfalk [1], empirical contributions do not need to rely exclusively on "a priori conceptualizations" but should reveal novel insights into a phenomenon. Our finding that the empowering antecedents may be more appealing to users than the more coercive approaches sheds new light into security research, and may inform other disciplines [9]. Moreover, by discovering that different levels of users (managers vs. employees) may need different blends of techniques to motivate them to compliance, we provide new and important insights into the phenomenon of IS security policy compliance. Future research is advised to explore the needs of even different levels of managers (high, middle, low).

This study also has considerable implications for practice. Middle Eastern managers, including information security managers, should be aware that coercive approaches are sometimes not the best approaches to adopt when encouraging ISP compliance. This is an important finding in a region where the culture is a relatively more hierarchical and inclined to high distance than those of western countries. Sometimes, other more positive techniques can go a long way toward motivating users to comply with the existing policies. Managers should be aware of the variety of positive empowerment techniques. In this study, we proposed, and found useful, three such empowerment techniques. Another contribution to practice is the empirical observation that one approach does not suit all users equally well. Different user groups may respond differently to the range of positive and coercive techniques based on their needs. This finding is consistent with the literature where we find that multiple interventions at various levels may be necessary to address IS security threat [14]. Future research should investigate the effectiveness of other techniques, especially empowering ones, not just in the case of conventional organizations but also increasingly in the contractual case between outsourcing firms and the outsourcers commonly called managed security service providers (MSSPs) [48].

Limitations

The present investigation was conducted in a single country, presenting research advantages and disadvantages. Though the generalizability to other countries may be questioned, our findings are strengthened because (1) the cultural environment represents a new research context where research and knowledge development is much needed and (2) IS theories and research models should be tested in different cultures to assess theories' boundary conditions and to discover if the variance models hold true in milieus other than western cultures (see, for example, [36]).

Further, as with nearly all empirical studies in the information security behavior domain, our dependent variable was related to specific *password policies* instead of general security policies. However, both managerial data and academic research have shown that the password-policy scales are acceptable forms of DVs and are effective indicators and representation of general compliance questions. At the managerial level, *CIO Magazine* recently reported that when IT managers were asked what their number one organizational IT security priority was, they responded that it was the increasing enforcement of security policies on employees [24]. Specifically, "password policies" made the top 5 list in their security policies (44% of respondents) right after paying attention to vulnerable web applications (55%), overall security awareness (51%), updating security patches (50%) and encrypting PCs and sensitive data (47%) [24]. Of these issues, only password policy compliance is an employee-focused (not IT department) responsibility. Thus, password policy compliance serves as an effective proxy for general employee security policy compliance.

More significantly, academic research results support this focus on password security as a valid measure of overall IT security policy compliance, and has been the focus of numerous empirical investigations (see, for example, [20, 69, 72]. The latter two studies as well as a study by Johnston et al. [40] found no significant difference between password-policy questions and other specific security policy questions.

Finally, our dependent variable measured the intention to comply rather than actual compliance. Although measuring actual compliance behaviors is often difficult, if not impossible [18, 78], future research efforts should seek creative ways to collect objective data for the dependent variable. The use of NeuroIS measures is proving to be an effective tool to study actual security behavior [76, 80]. Future NeuroIS lab experiments on managers and employees could be used to confirm (or not) these results in an objective way, all the way opening the door to some more unconventional and probably controversial results.

Conclusion

As reported in our Results and Discussion sections, our study tested and compared coercive and empowering managerial approaches with regard to their impacts on employee compliance with IS security policies. We discovered that positive empowering approaches can be more effective than coercive approaches. Furthermore, we discovered that different managers and employees have different responses to the empowering approaches. On the one hand, we found that managers are more persuaded to comply when they have been convinced of the meaningfulness of compliance. On the other hand, our data suggest that employees are more persuaded to comply when they are given the chance to participate in forming and developing IS security policies. We strongly suggest that future compliance research take these differences into account and explore what are the best approaches to motivate different levels of employees or managers (high, middle, and low) regarding compliance among different types of insider threats (negligent, opportunistic, or malicious). In addition, research could examine the relative presence of negligent versus opportunistic users across different levels and determine whether negligent users may be more motivated by a certain empowering (or coercive) approach, whereas opportunistic users may be motivated by a different approach. Regardless of the specific avenue for research chosen, we strongly encourage IS security researchers to consider the empowering approach as a promising technique to inculcate greater IS security policy compliance.

ORCID

Puzant Balozian http://orcid.org/0000-0002-8410-1188
Dorothy Leidner http://orcid.org/0000-0002-7159-6273
Merrill Warkentin http://orcid.org/0000-0001-7435-7676

References

[1] Agerfalk PJ. Insufficient theoretical contribution: a conclusive rationale for rejection. Eur J Inf Syst. 2014;23(6):593–599.

[2] Aguinis H, Gottfredson RK, Joo H. Delivering effective performance feedback: the strengths-based approach. Bus Horiz. 2012;55(2):105–111.

[3] Ahearne M, Mathieu J, Rapp A. To empower or not to empower your sales force? An empirical examination of the influence of leadership empowerment behavior on customer satisfaction and performance. J Appl Psychol. 2005;90(5):945–955.

[4] Andreoni J, Harbaugh WT, Vesterlund L. The carrot or the stick: rewards, punishments and cooperation. Am Econ Rev. 2003;93(3):893–902.

[5] Barclay D, Higgins C, Thompson R. The partial least squares (PLS) approach to causal modeling: personal computer adoption and use as an illustration. Technol Stud. 1995;2(2):285–309.

[6] Barki H, Hartwick J. Measuring user participation, user involvement, and user attitude. MIS Q. 1994;18(1):59–82.

[7] Barrick MR, Mount MK, Li N. The theory of purposeful work behavior: the role of personality, higher-order goals, and job characteristics. Acad Manag Rev. 2013;38(1):132–153.

[8] BBC News. Ashley Madison infidelity site's customer data stolen., 2015 Jul 20 [cited Apr 9, 2016]. Available from http://www.bbc.com/news/technology-33592594

[9] Beath C, Berente N, Gallivan MJ, Lyytinen K. Expanding the frontiers of information systems research: introduction to the special issue. J Assoc Inf Syst. 2013;14(4):1–16.

[10] Boss SR, Kirsch LJ, Angermeier I, Shingler RA, Boss RW. If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. Eur J Inf Syst. 2009;18(2):151–164.

[11] Boss SR, Galletta DF, Lowry PB, Moody GD, Polak P. What do users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. MIS Q. 2015;39(4):837–864.

[12] Bulgurcu B, Cavusoglu H, Benbasat I. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Q. 2010;34(3):523–548.

[13] Cavusoglu H, Raghunathan S, Cavusoglu H. Configuration of and interaction between information security technologies: the case of Firewalls and intrusion detection systems. Inf Syst Res. 2009;20(2):198–217.

[14] Chatterjee S, Sarker S, Valacich JS. The behavioral roots of information systems security: exploring key factors related to unethical IT use. J Manag Inf Syst. 2015;31(4):49–87.

[15] Chin WW. The partial least squares approach to structural equation modeling. Mod Methods Bus Res. 1998;295(2):295–336.

[16] Conger JA, Kanungo RN. The empowerment process: integrating theory and practice. Acad Manag Rev. 1988;13(3):471–482.

[17] Corley KG, Gioia DA. Building theory about theory building: what constitutes a theoretical contribution? Acad Manag Rev. 2011;36(1):12–32.

[18] Crossler RE, Johnston AC, Lowry PB, Hu Q, Warkentin M, Baskerville R. Future directions for behavioral information security research. Comput Secur. 2013;32:90–101.

[19] D'Arcy J, Herath T. A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. Eur J Inf Syst. 2011;3(6):643–658.

[20] D'Arcy J, Herath T, Shoss MK. Understanding employee responses to stressful information security requirements: a coping perspective. J Manag Inf Syst. 2014;31(2):285–318.

[21] D'Arcy J, Hovav A, Galletta D. User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. Inf Syst Res. 2009;20(1):79–98.

[22] Dawes J. Five point vs. eleven point scales: does it make a difference to data characteristics? Australasian J Market Res. 2002;10(1):1–17.

[23] Dawes JG. Do data characteristics change according to the number of scale points used? An experiment using 5 point, 7 point and 10 point scales. Int J Market Res. 2008;50(1):61–77.

[24] DeMetz A. The #1 information security policy that IT managers would change. CIO Magazine, 2015. Available from http://www.cio.com/article/2899927/security0/the-1-information-security-policy-that-it-managers-would-change.html

[25] DeShon RP, Gillespie JZ. A motivated action theory account of goal orientation. J Appl Psychol. 2005;9(6):1096–1127.

[26] Dhillon G, Torkzadeh G. Value-focused assessment of information system security in organizations. Inf Syst J. 2006;16(3):293–314.

[27] Dinev T, Hu Q. The centrality of awareness in the formation of user behavioral intention toward protective information technologies. J Assoc Inf Syst. 2007;8(7):386–408.

[28] Ernst & Young. Get ahead of cybercrime. EY's global information security survey, 2014, [cited Mar 2015]. Available from http://www.ey.com/Publication/vwLUAssets/EY-global-information-security-survey-2014/$FILE/EY-global-information-security-survey-2014.pdf

[29] European Commission. Information society: introduction, 2011, [WWW document] Luxemburg. [cited Mar 2015]. Available from http://epp.eurostat.ec.europa.eu.ezproxy.baylor.edu/portal/page/portal/information_society/introduction/

[30] Fornell C, Larcker DF. Evaluating structural equation models with unobservable variables and measurement error. J Marketing Res. 1981;18(1):39–50.

[31] Guo KH, Yuan Y, Archer NP, Connelly CE. Understanding non-malicious security violations in the workplace: a composite behavior model. J Manag Inf Syst. 2011;28(2):203–236.

[32] Hair JF Jr, Hult GTM, Ringle C, Sarstedt M. A primer on partial least squares structural equation modeling (PLS-SEM). Los Angeles, CA: Sage Publications; 2014.

[33] Hair JF, Black WC, Babin BJ, Anderson RE, Tatham RL. Multivariate data analysis. Upper Saddle River, NJ: Pearson Prentice Hall; 2009.

[34] Harrington SJ. The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. MIS Q. 1996;20(3):257–278.

[35] Hartwick J, Barki H. Explaining the role of user participation in information system use. Manage Sci. 1994;40(4):440–465.

[36] Hovav A, D'Arcy J. Applying an extended model of deterrence across cultures: an investigation of information systems misuse in the US and South Korea. Inf Manag. 2012;49(2):99–110.

[37] Hsu C, Lee J, Straub DW. Institutional influences on information systems security innovations. Inf Syst Res. 2012;23(3):918–939.

[38] Johnson ME. Information risk of inadvertent disclosure: an analysis of file-sharing risk in the financial supply chain. J Manag Inf Syst. 2008;25(2):97–124.

[39] Johnston AC, Warkentin M. Fear appeals and information security behaviors: an empirical study. MIS Q. 2010;34(3):549–566.

[40] Johnston AC, Warkentin M, Siponen M. An enhanced fear appeal rhetorical framework: leveraging threats to the human asset through sanctioning rhetoric. MIS Q. 2015;39(1):113–134.

[41] Johnston AC, Warkentin M, McBride M, Carter LD. Dispositional and situational factors: influences in IS Security Policy Violations. Eur J Inf Syst. 2016;25(3):231–251.

[42] Karjalainen M, Siponen M. Toward a new meta-theory for designing information systems (IS) security training approaches. J Assoc Inf Syst. 2011;12(8):518–555.

[43] Karoui M, Dudezert A, Leidner DE. Strategies and symbolism in the adoption of organizational social networking systems. J Strategic Inf Syst. 2015;24(1):15–32.

[44] Kerr O. How does the cybersecurity act of 2015 change the internet surveillance laws? 2015. Available from https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/12/24/how-does-the-cybersecurity-act-of-2015-change-the-internet-surveillance-laws/

[45] Krausert A. HRM systems for knowledge workers: differences among top managers, middle managers, and professional employees. Hum Resour Manage. 2014;53(1):67–87.

[46] Kruck GP, Kruck SE. Spoofing–a look at an evolving threat. J Comput Inf Syst. 2006;47(1):95–100.

[47] Lavine M. Exploring the relationship between corporate social performance and work meaningfulness. J Corporate Citizenship. 2012;46:53–70.

[48] Lee CH, Geng X, Raghunathan S. Contracting information security in the presence of double moral hazard. Inf Syst Res. 2013;24 (2):295–311.

[49] Leidner DE, Milovich M. Middle management and information systems strategy: the role of awareness and involvement. Paper presented at the Forty Seventh Annual Hawaii International Conference on System Sciences (HICSS); 2014; Honolulu, HI.

[50] Li DC. Online security performances and information security disclosures J Comput Inf Syst. 2015;55(2):20–28.

[51] Lo J, Leidner D. Extending the IS strategy typology: an assessment of strategy impacts on capabilities development and performance. Paper presented at the Thirty Third International Conference on Information Systems; 2012; Orlando, FL.

[52] Lowry PB, Moody GD, Galletta DF, Vance A. The drivers in the use of online whistle-blowing reporting systems. J Manag Inf Syst. 2013;30(1):153–190.

[53] Markus ML, Mao J. Participation in development and implementation-updating an old, tired concept for today's IS contexts. J Assoc Inf Syst. 2004;5(11):514–544.

[54] McClean EJ, Burris ER, Detert JR. When does voice lead to exit? It depends on leadership. Acad Manag J. 2013;56(2):525–548.

[55] McGregor D. The human side of enterprise. 1st ed. New York, NY: McGraw-Hill; 1960.

[56] Menard P, Gatlin R, Warkentin M. Threat protection and convenience: antecedents of cloud-based data backup. J Comput Inf Syst. 2014;55(1):83–91.

[57] Niehaves B, Plattfaut R. Internet adoption by the elderly: employing iS technology acceptance theories for understanding the age-related digital divide. Eur J Inf Syst. 2014;23(6):708–726.

[58] Ormond D, Warkentin M. Is this a joke? The impact of message manipulations on risk perceptions. J Comput Inf Syst. 2015;55 (2):9–19.

[59] Petter S, Straub D, Rai A. Specifying formative constructs in information systems research MIS Q.. 2007;31(4):623–656.

[60] Podsakoff PM, MacKenzie SB, Lee J, Podsakoff NP. Common method biases in behavioral research: a critical review of the literature and recommended remedies. J Appl Psychol. 2003;88 (5):879–903.

[61] Posey C, Roberts T, Lowry PB, Bennett B, Courtney J. Insiders' protection of organizational information assets: development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. MIS Q. 2013;37(4):1189–1210.

[62] Prensky M. Digital natives, digital immigrants part 1. Horizon. 2001;9(5):1–6.

[63] PWC, PricewaterhouseCoopers. Managing cyber risks in an interconnected world: key findings from the global state of information security survey. 2015. Available from http://www.pwc.com/gsiss2015.

[64] Ringle CM, Wende S, Will A. Smart PLS 2.0. Hamburg (Germany): University of Hamburg; 2005. Available from http://www.smartpls.de

[65] Sharp A. Two people may have committed suicide after ashley madison hack: police. 2015, Aug 24. [cited Apr 9, 2016]. Available from http://www.wired.com/2015/08/ashley-madison-ceo-resigns-wake-hack-news-affairs/

[66] Shropshire JD, Warkentin M, Johnston AC. Impact of negative message framing on security adoption. J Comput Inf Syst. 2010;51 (1):41–51.

[67] Siponen MT, Oinas-Kukkonen H. A review of information security issues and respective research contributions. ACM SIGMIS Database. 2007;38(1):60–80.

[68] Siponen M, Pahnila S, Mahmood MA. Compliance with information security policies: an empirical investigation. Computer. 2010;43(2):64–71.

[69] Siponen M, Vance A. Neutralization: new insights into the problem of employee information systems security policy violations. MIS Q. 2010;34(3):487–503.

[70] Son J. Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. Inf Manag. 2011;48(7):296–302.

[71] Spears JL, Barki H. User participation in information systems security risk management. MIS Q. 2010;34(3):503–522.

[72] Stanton JM, Stam KR, Mastrangelo P, Jolton J. Analysis of end user security behaviors. Comput Secur. 2005;24(2):124–133.

[73] Straub DW, Nance WD. Discovering and disciplining computer abuse in organizations: a field study. MIS Q. 1990;14(1):45–60.

[74] Straub DW, Welke RJ. Coping with systems risk: security planning models for management decision making. MIS Q. 1998;22 (4):441–469.

[75] Tyler TR, Blader SL. Can businesses effectively regulate employee conduct? The antecedents of rule following in work settings. Acad Manag J. 2005;48(6):1143–1158.

[76] Vance A, Anderson BB, Kirwan CB, Eargle D. Using measures of risk perception to predict information security behavior: insights from electroencephalography (EEG). J Assoc Inf Syst. 2014;15 (10):679–722.

[77] Warkentin M, McBride M, Carter L, Johnston A. Exploring the role of individual employee characteristics and personality on employee compliance with cybersecurity policies. Paper presented at the Eighteenth Americas Conference on Information Systems; 2012a; Seattle, WA.

[78] Warkentin M, Straub D, Malimage K. Measuring secure behavior: a research commentary. Paper presented at the Seventh Annual Symposium on Information Assurance & Secure Knowledge Management; 2012b; Albany, NY.

[79] Warkentin M, Johnston AC, Shropshire J. The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. Eur J Inf Syst. 2011;20 (3):267–284.

[80] Warkentin M, Walden EA, Johnston AC, Straub DW. Neural correlates of protection motivation for secure IT behaviors: an fMRI exploration. J Assoc Inf Syst. 2016;17(3):194–215.

[81] Willison R, Warkentin M. Beyond deterrence: an expanded view of employee computer abuse. MIS Q. 2013;37(1):1–20.

[82] Zetter K. Ashley Madison CEO Resigns in Wake of Hack. News of Affair, 2015, Aug 28, [cited Apr 9, 2016]. Available from http://www.wired.com/2015/08/ashley-madisons-business-growing-company-says/

[83] Zhang X, Bartol KM. Linking empowering leadership and employee creativity: the influence of psychological empowerment, intrinsic motivation, and creative process engagement. Acad Manag J. 2010;53(1):107–128.

Appendix A

Table A1. Measurement scales.

Constructs	Items
Certainty of Sanctions (adapted from Tyler & Blader [75])	How closely is your IS security policy compliance monitored by your supervisor? (5 pt. Likert––partially anchored - from “not at all” to “very much”) How often is your supervisor paying attention to whether or not you follow the IS security policy compliance rules? (5 pt. partially anchored Likert from “never” to “very often”)
Severity of Sanctions (adapted from Tyler & Blader [75])	If you are caught breaking an IS security policy compliance rule, how much does it hurt your pay? (5 pt. partially anchored Likert from “very little” to “a lot”) If you fail to comply with your organization’s IS security policies, how much does that hurt your pay? (5 pt. partially anchored Likert from “very little” to “a lot”) If you fail to comply with your organization’s IS security policies, how much does that hurt your benefits? (5 pt. partially anchored Likert from “very little” to “a lot”)
Fostering participation in Decision Making (adapted from Zhang & Bartol [83])	My manager asks my opinion on the departmental implementation of IS security policy compliance decisions that may affect me. (5 pt. fully anchored Likert from “strongly disagree” to “strongly agree”) My manager often consults me on tactical decisions regarding how to effectively implement IS security policy compliance practices in our department. (5 pt. fully anchored Likert from “strongly disagree” to “strongly agree”)
Enhancing meaningfulness of IS Security Policy Compliance (adapted from Zhang & Bartol [83])	My manager helps me understand how my IS security policy compliance objectives and goals relate to the company’s IS security. (5 pt. fully anchored Likert from “strongly disagree” to “strongly agree”) My manager helps me understand the importance of my IS security policy compliance to the overall information security effectiveness of the company. (5 pt. fully anchored Likert “strongly disagree” to “strongly agree”)
Expressing Confidence in High Performance (adapted from Zhang & Bartol [83])	My manager believes in my ability to improve when I make mistakes for the first time regarding IS security policy compliance practices (ex: plugging in and opening a personal USB on the work-related desktop without scanning the USB first) even if the training session has covered that practice in the past? (5 pt. fully anchored Likert from “strongly disagree” to “strongly agree”) My manager believes that I can handle IS security policy compliance practices even in the midst of demanding tasks. (5 pt. fully anchored Likert from “strongly disagree” to “strongly agree”)
Behavioral Intention to Comply	I intend to comply with the requirements of the password change policies of my organization in the future. (7 pt. fully anchored Likert from “strongly disagree” to “strongly agree”) I intend to carry out my responsibilities prescribed in the password change policies of my organization when I use information and technology in the future. (7 pt. fully anchored Likert from “strongly disagree” to “strongly agree”) I intend to protect information and technology resources according to the requirements of the password change policies of my organization in the future. (7 pt. fully anchored Likert from “strongly disagree” to “strongly agree”)
Marker Variables (adapted from Lo & Leidner [51])	Please rate how quickly your IT department is able to detect changes in customer demand: (5 pt. partially anchored Likert from “no extent” to “very great extent”) Please rate how swiftly your IT department is able to detect advances in technology that are relevant to the business: (5 pt. partially anchored Likert from “no extent” to “very great extent”)

Appendix B

Table B1. Descriptive statistics.

Industry	
Agriculture	1%
Audit	5%
Banking and finance	11%
Education	16%
Communications	2%
Consumer products	2%
Construction	4%
Electronics	1%
Energy	1%
Fashion	2%
General services	1%
Government military	2%
Health care	15%
Information technology	2%
IT services	2%
Insurance	4%
Logistics	4%
Manufacturing	5%
Nonprofit	2%
Professional services	2%
Real estate	1%
Retail, wholesale	5%
Other	12%
Size of organization	
Small size (1–200 emp.)	49%
Medium size (201–1000 emp.)	25%
Large size (over 1000 emp.)	26%
Gender	
Female	52%
Male	48%
Tenure	
Average years in current position	3.41
Average years with current organization	4.7
Average years of work experience	5.2
Average years of management experience	1.99
Min age	21
Max age	59
Mean age	29
Department	
Accounting	11%
Customer service	8%
Finance	8%
Human resources	3%
Inventory	1%
Information technology	12%
Legal	2%
Management	10%
Operations	2%
Production or manufacturing	2%
Purchasing	3%
Quality assurance	1%
Research and development	4%
Sales or marketing	13%
Security	2%
Other	18%

Appendix C

Table C1. Procedural remedies of common method variance.

Common method variance source	Description	Remedy used in this research
1) Item demand characteristics	Items may convey hidden cues as to how to respond to them	Expert panel of 8 academicians
2) Item ambiguity	Responding to them randomly or systematically using their own heuristics	Expert panel of 8 academicians
3) Common scale formats	Artificial covariation produced by the use of the same scale format	Different scale format (5-, 7-, and 11-point Likert scales)
4) Common scale anchors	Repeated use of the same anchor points	Different use of anchor points (agree-disagree; never-very often; very little-a lot…) and anchor types (drop down list; single answer horizontal)
5) Context-induced mood	When the first question or set of questions induces a mood for responding to the remainder of the questionnaire	Randomized items within blocks and randomized blocks in both paper-based and online versions
6) Reducing social desirability	Protecting respondent anonymity and reducing evaluation apprehension	In the introductory section, some statements tackled the preservation of anonymity, assured there are no right and wrong answers, and encouraged respondents to answer questions honestly to benefit academic research.
7) Improving scale items	Define ambiguous terms; keep questions simple, specific and concise	Expert panel of 8 academicians

Source: Podsakoff et al. [60]).

Appendix D

Table D1. Cross correlations.

	Comp.	Express confidence	Certainty	Meaningfulness	Participation	Severity
Intent 1	0.833	0.422	0.029	0.165	0.349	0.125
Intent 2	0.795	0.304	0.166	0.238	0.258	0.124
Intent 3	0.801	0.375	0.237	0.242	0.320	0.135
Conf 1	0.461	0.999	0.272	0.317	0.326	0.161
Conf 2	0.087	0.879	0.301	0.425	0.211	0.276
Certain 1	0.172	0.262	0.993	0.498	0.386	0.445
Certain 2	0.021	0.201	0.867	0.484	0.278	0.455
Mngf 1	0.231	0.268	0.483	0.894	0.521	0.206
Mngf 2	0.231	0.303	0.466	0.894	0.503	0.262
Part. 1	0.205	0.211	0.425	0.525	0.709	0.253
Part 2	0.348	0.299	0.365	0.547	0.921	0.113
Severity 1	0.057	0.158	0.394	0.257	0.183	0.743
Severity 2	0.048	0.198	0.487	0.216	0.054	0.739
Severity 3	0.186	0.122	0.408	0.223	0.127	0.954