Think and Act Positively: A Motivational Organizational Citizenship Behavior Approach Towards Information Security Policy Compliance

Emergent Research Forum (ERF)

Joseph Manga
University of Texas Rio Grande Valley
joseph.manga01@utrgv.edu

Nan Xiao
University of Texas Rio Grande Valley
nan.xiao@utrgv.edu

Emmanuel Ayaburi
University of Texas Rio Grande Valley
emmanuel.ayaburi@utrgv.edu

Introduction

Studies on information security policy (ISP) compliance have been focusing on approaches that evoke fears and impose sanctions in order to influence employees’ compliance behaviors. For example, some of them have relied on theories of deterrence (Bulgurcu et al. 2010) and fear appeal (Boss et al. 2015; Johnston and Warkentin 2010) to minimize non-compliant behaviors.

One of the limitations of this approach is that it may lead to a tense work environment and reduce employees’ morale and motivation, so employees may be less likely to display trustworthiness and be unwilling to put in extra efforts in complying with ISPs. Therefore, our study embraces a more positive, motivational, and ethical approach to ISP compliance.

This paper seeks to address the following question: what motivational distinctiveness do employees value and how can organizations leverage on them to improve ISP compliance? Drawing on organizational citizenship behavior (OCB) literature (Organ 1989), our study identifies three factors that motivate employees to maximize their intentions to comply with ISPs, including job satisfaction, leadership support, and rewards. We propose that a satisfied job setting with management support and incentives are essential to encourage employees to act more responsibly and proactively towards achieving security compliance.

Literature Review

Information Security Policy

ISP compliance is the “degree to which an employee has a positive or negative evaluation of compliance behavior towards his or her organization’s ISP,” (Hu et al. 2012; D’Arcy and Lowry 2017, p. 47). Most scholarly works on ISP compliance adopt approaches that (1) instill fear appeals and threat to compel employees to comply (Boss et al. 2015; Johnston et al. 2015), (2) use sanction, punishment, and controls to deter employees from committing computer security violations (Siponen and Vance 2010), and (3) practice safe computing via protection motivation and coping techniques to avoid getting into security troubles (Anderson and Agarwal 2010; Wang et al. 2017). These studies have focused on sanctions and fears to prevent non-compliance. Some studies have discussed positive facilitators (e.g., rewards) of ISP compliance (e.g., Liang et al. 2013), however, they fail to categorize rewards as formal or informal. Thus, grounded on OCB theory, we focus on the factors that enhance employees’ morale towards compliance.

Organization Citizenship Behavior (OCB)

The theory of organizational citizenship behaviors (OCB) suggests that employees willingly contribute to the overall success of their organization. OCBs includes five components: altruism (helping another
person with a relevant task), conscientiousness (carrying out role behaviors beyond the minimum required levels), sportsmanship (refraining from complaints or grievances), courtesy (making efforts to prevent a problem) and civic virtue (showing interest in the organization; defend rules) (Organ 1989). Past research has identified job satisfaction, dispositions, employee attitudes, organizational commitment, and leadership supportiveness as some of the antecedents of OCB (Jahangir et al. 2004). Furthermore, two types of OCB behaviors are suggested: (1) active positive contributions or commissions (e.g., helping others) and (2) avoiding to engage in behaviors that are harmful to others or to one’s organization (e.g., not abusing others’ rights). (Farh et al. 1997).

We consider ISP compliance as an OCB behavior for the following two reasons. First, an employee’s compliance behaviors benefit the organization, including keeping the organization more competitive, avoiding any financial loss from negligence, and minimizing organizational risks that may originate from legal lawsuits and fines. Second, from the employees’ perspective, they have to make an extra effort to comply. For example, compliance may cost employees their time and efforts and cause inconvenience to them. Also, compliance trainings they may have to attend could affect their productivity. Therefore, we adopt the framework of OCB to study factors that motivate employees to comply with security policies.

Theoretical Model and Hypotheses Development

As shown in Figure 1, we propose that job satisfaction, leadership support, and rewards (formal and informal) have a positive impact on ISP compliance. The following model provides rational for developing our hypotheses.

![Diagram showing the relationship between Job Satisfaction, Leadership Support, Rewards, and ISP Compliance]

**Figure 1: Conceptual Model and Hypotheses**

**Job Satisfaction**

Job satisfaction refers to “a positive emotional state of feeling resulting from jobs, thus, fulfilled individuals’ value towards their jobs,” (Locke 1976; Kian et al. 2014, p. 96). According to this definition, an employee can derive affection (the individual’s emotional state of feeling good) and cognition (individual’s experience from the appraised work. Furthermore, when an individual completes a job, there is an extra sense of fulfillment that goes with it (Kian et al. 2014). We conceptualize job satisfaction as an inner fulfillment individuals display from carrying out their tasks and which causes them to take positive or desired actions for the benefit of the organization. If employees feel a sense of satisfaction carrying out their work, it drives them to take positive actions that are beneficial to the organization. Employees who are more satisfied with their job are those whose needs of safety, belonging, esteem, fulfilment, and their basic physiological needs are met. They tend to be more motivated because they are happy, and they feel good about their job. As a result, they think positively and develop a sound mind towards others and towards their organization’s policies and procedures. Dissatisfied employees develop feelings of anger and
aggression towards others and exhibit some sort of negative attitudes towards obeying the rules and policies in place and are demotivated to take positive steps towards policy engagements.

In line with the OCB literature, individuals who are affectionately attached to and appraise their job will demonstrate some degree of conscientiousness (carrying out role behaviors well beyond the minimum required levels). In addition, literatures on motivation theories suggest a strong connection between motivation and job satisfaction. When job-related needs are strong in a person, satisfaction in receiving the particular needs has higher potential to motivate behavior (Kian et al. 2014).

Connecting the above thoughts to security compliance, one study has argued that the degree that employees will comply with the guidelines will involve factors that “can generate positive social and emotional outcomes, such as happiness (Siponen and Ilvani 2006),” (Cram et al. 2017, p. 616). In relation to ISP compliance behavior, security-related stress has a negative outcome (D’Arcy et al. 2014). Thus, employees who have a general feeling of satisfaction as a consequence of work-related conditions will feel more motivated to take on role behaviors that are beyond the company’s expectations as these align with their perceptions of fulfillment, happiness, and success in carrying out the organization’s goals and objectives. Conversely, dissatisfied employees are unhappy, demotivated, and will likely disregard any feeling that drives them towards policy compliance. Thus, we hypothesize that:

H1: Job satisfaction positively affects intentions to comply with information security policy.

Leadership Support (of compliance)

We define leadership or management support as the ability to exert influence on people and driving change by empowering and motivating them to take positive moves as exemplified by the leader. Leadership or management support for policy compliance goes beyond just writing the policies and expecting employees to sign their consent to playing by the rules without additional help.

In line with OCB, leadership support can be characterized as courtesy where the leader takes proactive steps to prevent attitudes of non-compliance in employees and guide them in the right direction. Leadership support is shown through clarifying employee’s expectations, be emotionally attached to and showing concern for the employee’s wellbeing, and motivating employees by inspiring them towards high performance achievements (Zhang 2011). A leader’s support goes past the level of just focusing on the policy to focusing on the individual, until compliance to ISPs becomes part of the employee’s daily habits.

Employees will be more compliant when they have a strong relationship with the leader. When there is a disconnect between the employee and the leader, the employee may tend to comply only when the leader is around. Otherwise, they will violate in the absence of the leader. But when leaders provide a strong support system, for example, getting to know how their employees are faring, motivating them to perform beyond their normal expectations, giving employees the right resources and training opportunities, and conducting security education and training awareness (SETA) programs, then the employees will be more proactive and pushful in their compliance behaviors than just being reactive.

However, when there is little or no support system, the employee develops a laissez-faire attitude; that is, when they feel as to comply, they will do, but when they do not feel motivated, they tend to violate. The more the leadership support, the more the employee is empowered to take positive actions. Past study has shown that “stronger perceived top management participation in information security initiatives leads to stronger positive attitude towards compliance with information security policies,” (Hu et al. 2012, p. 630). We posit that when employees get the support that goes beyond just focusing on the policy rules to include a focus on the employees psychological, emotional, and cognitive state of mind, they are more likely to comply with ISPs. Thus:

H2: Leadership support positively affects intentions to comply with information security policy.

Rewards (Formal and Informal)

We categorize reward as: formal reward and informal reward. Formal reward is defined as showing gratitude in the form of appreciations, recognition, promotion, bonuses, and financial incentives where the element of gratitude - a positive moral emotion that arises when individuals feel they have benefited
from gifts, kindness, support, or favors, (Grant and Gino 2010) is key to determining a positive response from the gratitude recipient.

In the OCB literature, gratitude has been explicitly hypothesized to generate an action tendency to be helpful (McCullough et al. 2001) and is a uniquely suited antecedents of OCB (Spence et al. 2014). Gratitude is two-way with the gratitude giver (the person expressing the gratitude) on one end and the gratitude receiver (the person to whom gratitude is shown) on the other end.

Prior research suggests that reward provides needed incentive and motivation for compliance; and when an employee is rewarded for compliance with ISP, this positively affects the perceived benefit of compliance, Bulgurcu et al. (2010). Employees will most likely generate a positive response that is helpful to security compliance when management formally and openly recognize them before others. They feel pumped up and tend to show behaviors that are consistent with that of good citizens in the organization. A natural tendency in people is to reciprocate the favor others show to them. In response, employees tend to do things that will please the others (the organization) – comply with the organization’s policies. So, employees who receive more rewards, tend to give more back (show more gratitude).

**Informal reward (IR)** on the other hand refers to the unexpected and spontaneous gestures that someone does to uplift and boost morals (i.e., gestures that stimulate or hold high principles for proper conduct). IR can take the form of verbal expressions (such as, ‘thank you,’ or ‘you did great today,’ or ‘you are doing well,’ or ‘keep up the good work,’ or ‘you are appreciated’). These casual ways of appreciating people create feelings of engagements with the organization. People tend to stay connected with those who value and appreciate them (Spence et al. 2014). Employees will show proper conducts towards ISP compliance when employers uplift their morals through unexpected compliments.

In summary, the manner in which reward (formal or informal) is shown is very important. If it is used as a medium to control behaviors, then the resulting effect on compliance will be short-lived. But if exercised in a genuine way, it will shape attitudes, engage employees to generate behaviors that are helpful, and act as extra motivators to complying with ISPs. Thus, we hypothesize that:

**H3: Formal rewards positively affects intentions to comply with information security policy.**

**H4: Informal rewards positively affects intentions to comply with information security policy.**

**Implications for Research and Practice**

Leveraging the organizational citizenship behavior concept, we examined the effects of job satisfaction, leadership support, and rewards on ISP compliance. We expect that our results will have both theoretical and practical applications for these reasons: First, we argued that individuals who are satisfied with their job will take on extra-role behaviors towards policy compliance than their dissatisfied counterparts. So, managers should create work environments that reduce stress and boredom. In doing so, the organization will prevent noncompliance and will spend less time solving compliance issues that would have surfaced due to negligence, thereby converting the saved time into money, which is a huge cost saving strategy to an organization’s business models. Second, leadership support is very important in influencing behavioral change and enhancing proactiveness in employees. While leadership support influences employees’ behaviors towards security compliance, employees may resort to policy violations if they perceive a lack of involvement by management. So, leadership support adds an extra push by creating positive attitudes towards compliance even in the absence of the leader. Managers should invest more on developing skills that create bond and trust between them and the employees. Third, rewards are very strong predictors of policy compliance depending on how it is applied. If it is dished out as a means of control, then failure to comply is inevitable. But, when employees perceive that the company always finds a way to boost their morals, they will remain motivated to take positive actions towards compliance. Studying compliance behavior via the OCB lens provides valuable insights to research and theory in that OCB forms the foundation on which employees and organizations can demonstrate a sense of patriotism to the stated rules (policies) and to one another and can be a basis from which necessary constructs can be inferred to study compliance behaviors.
REFERENCES


