Multidimensional Employee Compliance with Security Policies: A Dynamic Conceptual Framework

Early stage paper

Weijie Zhao
The University of Alabama
wzhao19@crimson.ua.edu

Allen C. Johnston
The University of Alabama
ajohnston@cba.ua.edu

Yuanyuan Chen
The University of Alabama
ychen200@cba.ua.edu

ABSTRACT

Employees' failure to comply with organizational security policies has been a key issue for organizations and scholars. Unlike previous information systems (IS) studies that conceive and operationalize security policy compliance as a unidimensional construct, we consider it as a multidimensional one. We develop a dynamic framework to investigate three security policy compliance dimensions: self-engagement, response, and behavioral consistency. We propose a concept mapping approach to investigate these dimensions of security policy compliance and verify our dynamic framework from practitioners' perspectives. Our multidimensional framework will extend and enrich our understanding of security policy compliance and help develop this multidimensional construct's measurements.

Keywords

Insider Threats, Security Policy Compliance, Self-engagement, Response, Behavioral Consistency.

INTRODUCTION

Employees' failure to comply with organizational security policies has been a critical issue for organizations for many years (Siponen et al., 2010). Even as information security technologies have evolved and improved to curb the external threats to some extent, the challenge of insider threats persists, becoming more frequent and causing progressively more severe losses to organizations (van Zadelhoff，2016). According to a survey conducted in 2022, insider threat incidents in the world have increased by 44 percent since 2020, raising the average cost associated with insider attacks to $15.38 million (Ponemon Institute, 2022). Insider threat is an information security issue that organizations urgently need to address.

An insider threat happens when a threat involves negligent, accidental, or purposefully malicious employee actions (Willison and Warkentin, 2013). Organizations generally reduce insider threats through a range of security controls, including behavioral controls such as acceptable use policies, employee privacy rights policies, and trainings (Guo and Yuan, 2012), technical controls such as employee surveillance and monitoring tools and data loss preventions solutions (Straub, 1990), and environmental controls (e.g., subject norms and security cultures) (Balozian and Leidner, 2017). Security policies are widely used behavioral controls designed to protect an organization's physical and digital assets from insider threats. Organizations usually specify procedures, rules, and norms that employees are required to abide by to fulfill the requirements of the policies. The extent to which employees match the policy requirements indicates the security policy compliance (Bulgurcu et al., 2010). Yet, despite the effort of security personnel to develop and implement these policies, employees continue to violate them (Posey and Shoss, 2022), keeping the attention of scholars and practitioners squarely on the insider threat phenomenon.

Prior IS research has conceived and operationalized security policy compliance as a unidimensional concept (D'Arcy and Teh, 2019; D'Arcy and Lowry, 2019; Humaidi, 2013; Jaafar and Ajis, 2013; Karlsson et al., 2017; Ormond et al., 2019; Silic and Lowry, 2020; Siponen et al., 2010; Siponen et al., 2014). Most of the studies are built on the assumption of full compliance and focus on examining the completeness of compliance (Karjalainen et al., 2019). In contrast, the compliance literature in psychology and sociology suggests that compliance may take different forms and completeness is only one. For example, people may comply with a policy passively or actively (Robinson and McNeill, 2008); they may respond to the policy compliance vocally or remain silent (Van Dyne et al., 2003); or they may adhere to the policy at the early stage or the late stage (Bottoms, 2013). Therefore, it is necessary to account for different dimensions of employees' security policy compliance in workspaces, including what they do and how they respond (i.e., their expression). Furthermore, an individual's compliance behavior may change in different working environments (Li et al., 2021). Without considering the timeline issue in security policy compliance, we cannot study employees' compliance behavior consistency.

To fill these research gaps, we develop a dynamic conceptual framework that conceives security policy compliance as a multi-dimensional construct. With the dynamic framework, we answer two questions: what are the salient dimensions of security policy compliance? And how are these dimensions instantiated in policy compliance behaviors?

Our study contributes to the IS research in the following three ways. First, this study extends and enriches our understanding of security policy compliance by conceptualizing it as a multidimensional construct. As far as we know, our research is the first study that defines and measures security policy compliance from multiple dimensions. Second, our framework accounts

for how individuals change their compliance behavior contingent on the role image or commitments. Third, we use a novel method--the brainstorming format of the concept mapping approach--to investigate the multidimensional aspects of security policy compliance from the practitioners' perspective.

The rest of the paper is organized as follows. First, we review the current studies on the definitions and measurements of security policy compliance and distinguish it from other alternative terms in different disciplines. Then, we define and describe three different dimensions (i.e., self-engagement, response, and behavioral consistency) of compliance in the context of security policies. Next, we develop a dynamic framework to define security policy compliance in the above three dimensions in a changeable context. Following this, we suggest concept mapping as a proposed research method to be used as a subsequent empirical investigation. Finally, we discuss the contribution of our conceptual framework and its limitations and suggestions for further research**.**

DEFINITIONS OF COMPLIANCE

Compliance in the security policy context has been studied in the past 30 years since Straub (1990) first used "compliance with security directives" in his study of deterring computer users' misconducts (Straub 1990, p. 272). Bulgurcu et al.'s (2010) definition of security policy compliance is well accepted in the current IS studies. Security policy compliance requires employees to 1) follow the requirements in security policies, 2) protect information assets and appropriately use information resources of their organizations, and 3) adhere to a set of security-related roles and responsibilities in participating security activities (Bulgurcu et al., 2010). However, with multiple perspectives to describe compliance behavior in security policy context, a single term is no longer sufficient to reflect employees' actual compliance behavior

comprehensively. Different terms with similar meaning of compliance have been used in current security policy compliance studies. It is a tricky issue to distinguish compliance from other terms such as conformity, cooperation, acquiescence, and adherence.

Conformity reflects how people comply with their beliefs and personal norms (Foorthuis, 2020; Rowe, 2005), which are not necessarily existing policies (Cialdini and Goldstein, 2004; Foorthuis, 2012). In an organizational security compliance context, employees form up their beliefs and norms about security protection and behave accordingly. Even more, employees gain social approval from others, building beneficial relationships with them to enhance self-esteem (Cialdini and Goldstein, 2004). As forcing individuals to comply with security policies can cause unsatisfactory behavior, early conformance by employees to security policies can better reduce implementation costs and protect the organization's information assets (Bélanger et al., 2017).

Beyond performing their own security policy compliance behaviors, employees may also recommend or assist others in complying with security policies to protect the organization's information resources (Hsu et al., 2015). Such behavior involves employees' cooperation with others in activities related to security policies. Cooperation to security policies focuses on the mutuality of employees' behavior in security activities. Mutuality is defined as "a connection with or understanding of another that facilitates a dynamic process of joint exchange between people. The process of being mutual is characterized by a sense of unfolding action that is shared in common, a sense of moving toward a common goal, and a sense of satisfaction for all involved" (Henson, 1997; p. 80). Employees will interact with their work environment to achieve the common objectives of security policies. This interactive cooperation allows employees to move from a passive role to an active role in security policy activities, gradually creating a secure work environment (Hus et al., 2015).

Furthermore, compliance is defined as a passive response - in the same sense as acquiescence - to a request. (Cialdini and Goldstein, 2004). However, unlike acquiescence, which reflects only the individual's response to stimuli, attitudes, and events, compliance serves as a behavior that involves action. In operation management, employee acquiescence is defined as a deep form of employee silence based on resignation where employees lack the self-efficiency to make a difference (Pinder and Harlos, 2001; Van Dyne et al., 2003; Brinsfield, 2013; Knoll and Dick, 2013). Acquiescence tends to be a behavior in which employees express passive acceptance of an event and allow it to happen, with or without agreement.

Adherence is a common substitution of compliance in the current IS studies to describe employees' behavior in fulfilling security policies or rules (Myyry et al., 2009; Siponen et al., 2014; Sikolia et al., 2016; Kuo et al., 2021). However, these studies did not distinguish between "compliance" and "adherence" to specific differences in employee behavior. In healthcare, adherence focuses on the timing, dose, frequency, and periods of medication consumption by health professionals (Settineri et al., 2019). Compliance is not always conducted on behalf of maintaining the desired outcome. Patients may follow the orders of healthcare professionals (Kyngas et al., 2000). In contrast to compliance, adherence occurs after the initial compliance behavior and emphasizes the consistency of individual compliance behavior over time. Therefore, while describing employee security policy compliance behavior, it is also important to consider compliance as a process rather than just a fixed time behavior.

Based on the above review of definitions of compliance. Employees' behavior is defined as 1) an action that employees engage themselves into completing tasks required by the security policies; 2) a response that employees keep silent or speak out along with actions to express their inner feelings and thoughts to security policies; 3) a process that employees’ behavior may change

based on time and security contexts. Thus, we argue that security policy compliance has multiple dimensions in terms of manifesting employee behavior. Next, we will further investigate its dimensions from the measurements of the current IS studies.

MEASUREMENTS OF SECURITY POLICY COMPLIANCE

In the investigation of security policy compliance, compliance behavior is measured in both quantitative and qualitative approaches. Current IS studies typically measure compliance behavior through self-reported surveys (e.g., Boss et al., 2009; Crossler et al., 2014; D'Arcy and Lowry, 2019), interview or case narrative-based data (Hedström et al., 2011; Karjalainen et al., 2019; Karjalainen et al., 2020; Kolkowska and Dhillon, 2013; Posey et al., 2014), and observed compliance behavior (Johnston et al., 2019; Liang et al., 2013; Liu et al., 2020; Ormond et al., 2019; Silic and Lowry, 2020; Warkentin et al., 2016). These studies mainly focus on measuring whether an individual's behavior is aligned with the requirements of security policies.

Common self-reported surveys to measure security policy compliance follow the instruments developed by Bulgurcu et al. (2010) from the Theory of Planned Behavior (Ajzen, 1991) to investigate employees' compliance behavior in requirement compliance, employees' responsibility, and information technology and resources protection (e.g., Cox, 2012; D'Arcy and Teh, 2019; D'Arcy and Lowry, 2019). Compliance behavior was identified through employees' reports of their work routines to achieve the objectives of security policies (Kolkowska and Dhillon, 2013). In addition, researchers investigate employee engagement in security activities in conducting security behavior and raising security awareness to meet the organization's security requirements (Boss et al., 2009; Burns et al., 2019; Myyry et al., 2009).

Employees' cooperation behavior in security policy compliance has also been investigated based on the Theory of Reasoned Action (Fishbein, 1980). During the compliance process, employees are asked about actual compliance behavior that involves not only fulfilling the organization's requirements by themselves but also advising and assisting others in complying with security policies (Humaidi and Balakrishnan, 2015; Humaidi and Balakrishnan, 2018; Siponen et al., 2010; Siponen et al., 2014; Turel et al., 2020).

Even more, employees' vocal responses to security policies are surveyed (Hsu et al., 2015). Employees may speak up their opinions and ideas about security policies and make recommendations to organizations. Besides researchers investigated employee compliance or noncompliance with security policies at the same time in their daily work (Yazdanmehr and Wang, 2016; Yazdanmehr et al., 2020; Chen et al., 2020). Highlighting compliance behavior is a dynamic process changing over time, and the changing factors can trigger new compliance decisions for employees, which initiates a process of reevaluating (Karjalainen et al., 2019; Karjalainen et al., 2020). Viewing compliance as dynamic behavior, continued engagement of security behavior was observed in employees' work environment (Warkentin et al., 2016). Specifically, the impact of employee sentiment change on compliance was measured in the observation of employee password sharing and document sharing (Ormond et al., 2019).

Based on the above review, security policy compliance has been measured as a dynamic behavior focusing on employee self-engagement in security activities, sound response to security policies, and behavioral consistency in complying with security policies. However, no study systematically aggregates the above three dimensions in a framework. This study will develop a dynamic framework to define a multidimensional concept for security policy compliance.

DIMENSIONS OF SECURITY POLICY COMPLIANCE

No matter from definition or measurement, security policy compliance has been investigated from multiple perspectives. Based on previous studies, we conceptualize security policy compliance into three dimensions: self-engagement, response, and behavioral consistency. Next, we will discuss how these dimensions manifest security policy compliance in a dynamic framework.

Self-engagement and Security Policy Compliance

Engaging the self in work allows the individual to achieve outstanding outcomes in completing the requirements, and this engagement has an impact on motivation, emotion, and performance (Britt et al., 2007). Employees have the self-control to decide whether complete the requirements of security policies. Security policy compliance is usually conceptualized from one of two perspectives: the rational perspective or the normative perspective (Bulgurcu et al., 2010; Hsu et al., 2015). Under these two perspectives, the assumptions behind employee self-engagement in security activities are different.

A rational perspective focuses on balancing benefits and costs in security policy compliance, which assumes that employees' behavior is determined by an assessment of the personal benefits and costs of complying with or violating security policies. Scholars investigate such action under the command-and-control approach that employees follow what the organization requires them to do (Tyler and Blader, 2005). Three basic types of security policy compliance – formal compliance, substantive compliance, and responsible compliance – are developed based on the rational mechanism in this study (see Table 1).

Formal compliance is defined as employees technically fulfilling the minimum requirements of security policies (Bulgurcu et al., 2010; Robinson and McNeill, 2008). Employees only complete security tasks that they think are necessary to satisfy the policy owners but not protect organizations' information assets. From the policy owner's perspective, employees have complied with all the requirements of security policies, but actually, employees have ignored the parts they consider unimportant. Employees do not want to waste time and effort on security activities, nor do they want to be sanctioned. Such compliance behavior contributes minimal positive security outcomes to organizations. However, employees do not intend to violate security policies. They may be in the process of fulfilling all the requirements.

Substantive compliance is defined as employees achieving the primary objectives of security policies to protect the information and technology resources of their organizations (Bulgurcu et al., 2010; Robinson and McNeill, 2008). Substantive compliance focuses on the effectiveness of the compliance behavior to security policies in the short term. Employees are always evaluating the opportunity cost of security policy compliance. Even though substantive compliance coincides with the organization's security goals for implementing security policies, employees have less awareness of their security behavior in an assessment. Rather, employees are concerned about the personal benefits they can derive from compliance with the security policy. For example, suppose the organization's security goals conflict with employees' personal goals (including job duties), and the rewards of compliance are insufficient to compensate for their losses. In that case, employees will violate the organization's security policy to safeguard their benefits (DiBenigno, 2018).

Responsible compliance is defined as employees carrying out their responsibilities prescribed in security policies when they use information and technology (Bulgurcu et al., 2010). Responsible

compliance also focuses on the effectiveness of employee compliance behavior in the long term. Employees frequently check their compliance behavior to be consistent with requirements. However, employees do not intend to improve their security knowledge and skills. Therefore, all assessment behavior is done to avoid sanctions rather than company security.

In contrast, a normative perspective focuses on forming beliefs and enhancing cooperation to encourage security policy conformity, which assumes that employees are willing to participate in the development and implementation of security policies by contributing their ideas and assistance. Under the normative perspective, consciously believing or accepting a set of norms guides employees to act in a particular way (Bottoms, 2013). Scholars investigate such action under a self-regulatory approach that employees' behavior is affected by social value judgment in activities related to rule or policy following, where personal benefits or costs are not a primary consideration (Tyler and Blader, 2005). Usually, employees have placed the organization's norms and security goals as their primary consideration in accomplishing the effectiveness of security policies (Safa et al., 2019). Two extended types of security policy compliance – normative conformity and altruistic cooperation – are developed based on the normative mechanism.

Normative conformity is defined as employees aligning their behaviors and beliefs with the organization's security policy, leading them to adhere to security policy no matter whether there is a policy requirement or not (Bottoms, 2013; Cialdini and Goldstein, 2004; Robinson and McNeill, 2008). Here, we use " conformity" instead of " compliance" because the employee is not a passive participant in security activities. Employees have already formed their security beliefs under the effect of social or organizational security norms and have cultivated security habits in their daily work (Vance et al., 2012). Security policies are no longer needed to constrain

their behavior to achieve its security objectives but rather to conform to its security strategy (Foorthuis, 2020). In normative conformity, employees have self-control over security activities and do not feel pressured to fulfill the requirements of organization's security policies. Employees have developed their security awareness and norms by continuously improving their security behavior in the activities required by security policies.

Altruistic cooperation is defined as employees recommending and assisting others in security policy compliance (Limayem and Hirt, 2003; Hsu et al., 2015). As a result, employees assist their colleagues in fulfilling security policy requirements and achieving positive security outcomes (Siponen et al., 2010; Siponen et al., 2014). Such cooperation behavior not only accomplishes the security tasks required by security policies but also helps create a long-term secure work environment (Hsu et al., 2015).

Response and Security Policy Compliance

Unlike action that focuses on completing a task, response describes individuals' physical and psychological reactions to stimulus, attitudes, or events. Responses are usually combined with actions to form an individual's behavior when completing a task. For example, employees may vocally express their thoughts about the organization's security policies while operationally following their requirements. However, they may say nothing about security policies while participating in security activities. Thus, we divide the response to security policies into voice and acquiescence (see Table 1). Voice represents the employee's expression of thoughts about security policies where employees actively commit to security activities. In contrast, acquiescence means the employee's hiding of thoughts about security policies where employees make a passive commitment to security activities.

Voice happens when employees actively speak up in the organization with their opinions or ideas for new strategies or changes in security policies, which is termed (see Table 1). Response to new security policies or the changes made in current security policies is an individual basic ability to express their feelings, attitudes, and thoughts (Karjalainen et al., 2020). Speaking up opinions or ideas in a workspace is an information exchange process for employees to communicate with others. Although speakers may not get feedback from listeners, they are willing to share their information with others. Sometimes, employees may share their feelings, attitudes, or thoughts about security policies with their colleagues or someone they trust rather than the organization's management. Although employees do not directly respond their thoughts about security policies to the organization, others have heard their voices, which would indirectly contribute to improving current security policies.

In contrast, acquiescence is defined in two scenarios. In the first scenario, employees passively withhold their opinions or ideas about security policies without saying anything (Pinder and Harlos, 2001). Keeping silent is a type of employee response to security policies, but it is difficult to be significantly observed. Sometimes, employees would like to say nothing while complying with security policies. For example, when an employee changes the default account password as required by the password security policy, they notice a flaw in the policy that may expose the organization's accounts to data breaches. However, the employee chooses not to report the fault to security management or complain about the policy to others because they do not believe that their opinions or ideas will make a difference. Acquiescence is not limited to acoustics; it can be an individual's passive internal reaction to attitudes or events (Pinder and Harlos, 2001).

In the second scenario, the response of an employee who goes along with others in voicing agreement with security policies but holds their own opinions or ideas without expressing them is still regarded as acquiescence (Van Dyne et al., 2003). Such acquiescence is described where employees passively accept security policies with speaking agreement but do not express their internal exact feelings and thoughts. This acquiescence allows employees to make a sound that is the same as the voice, but employees' inner feelings and thoughts have not been disclosed. Both scenarios of acquiescence are caused by resignation and low self-efficacy to make a difference (Van Dyne et al., 2003).

Behavioral Consistency and Security Policy Compliance

While describing employee security policy compliance behavior, it is also important to consider compliance as a process rather than just a fixed time behavior. During the compliance process, an individual's actual behavior of individuals may change depending on both time and context (Li et al., 2021). Usually, organizations expect employees to maintain consistent behavior in complying with security policies. To remain consistent with their behavior, individuals must devote effort to adapting to the dynamic security context. Thus, behavioral consistency is essential to investigate and measure the employees' behavioral change over time and across security contexts.

"Adhere" rather than "comply" is used to measure the consistency of employee behavior over time in following security policies (D'Arcy and Teh, 2019). In contrast to compliance, adherence occurs after the initial compliance behavior. Even if employees have not yet formed the behavioral habit of security conformity, employees still strive to fulfill the requirements of security policies, accomplish the organization's security goals, and achieve the effectiveness of security policies. We use behavioral adherence to define security policy compliance as being

consistent over time. There are two scenarios; one is that employee security policy compliance behavior is consistent across time in the same security context, and the other is that employee security policy compliance behaviors are consistent across security contexts (Li et al., 2021).

Based on the above discussion of security policy compliance from three dimensions, we categorize employee security compliance behavior into five types based on self-engagement, two types based on the response, and one type with two scenarios based on behavioral consistency (see Table 1). The following paragraphs will describe in detail the different types of security policy compliance in these three dimensions in a dynamic framework.

Self-Engagement				
Types of Compliance	**Definition**	**Theorical Perspective**	**Stage**	**Commitment**
Formal Compliance	Employees technically fulfill the minimum requirements of security policies.	Rational Perspective	Fulfillment of minimum requirements of organization's security policies	Employees play a passive role in security policy activities.
Substantive Compliance	Employees achieve the primary objectives of security policies to protect the organization's information and technology resources.		Alignment of security goals of organization's security policies	
Responsible Compliance	Employees carry out their responsibilities prescribed in security policies when they use information and technology in the organization.		Fulfillment of responsibilities to check compliance behavior	
Normative Conformity	Employees align their behaviors and beliefs with the organization's security policy, leading them to adhere to security policy no matter whether there is a policy requirement or not.	Normative Perspective	Alignment of compliance behaviors and beliefs with organization's security policies	Employees play an active role in security policy activities.

Altruistic Cooperation	Employees recommend and assist others in security policy compliance.		Assisting others to comply with organization's security policies.	
Response				
Types of Compliance	**Definition**		**Acoustic**	**Commitment**
Voice	Employees actively speak up about their opinions or ideas about new policies or changes in security policies in the organization.		Sound	Active
Acquiescence	Employees passively withhold their opinions or ideas about security policies.		Silence	Passive
	Employees passively accept security policies with speaking agreement but withhold their true feelings and thoughts about the security policies.		Sound	
Behavioral Consistency				
Types of Compliance	**Definition**		**Scenario**	
Behavioral Adherence	Employees' security policy compliance behaviors are consistent across time in the same security context.		Complying with the same security policy across time	
	Employees' security policy compliance behaviors are consistent across different security contexts.		Complying with different security policies across security contexts	

Table 1. Definitions and Dimensions of Security Policy Compliance

DYNAMIC CONCEPTUAL FRAMEWORK

Employees' compliance behaviors can be any of the five stages involving the extent of low to high self-engagement (see Figure 1). The first stage is the fulfillment of minimum requirements of organization's security policies. At this stage, employees technically fulfill the minimum requirements of security policies and contribute to minimal security protection outcomes. For example, an organization's password security policy requires that employees change their work account passwords. However, suppose the password policy does not require strong passwords (e.g., use a combination of numbers, characters, and symbols of at least 8-bit length). Employees

may include personal information in their passwords for easy memorization (Siponen et al., 2010). But hackers can crack such passwords faster and attack the organization's accounts and IS. At this stage, employees merely comply with the password policy at a low level of self-engagement, and their compliance behaviors do not result in the desired objectives of the password policy.

The second stage is the alignment of security goals of organization's security policies, in which employees achieve the primary objectives of security policies to protect their organizations' information and technology resources. For example, employees use strong passwords in their work accounts even though the password policy does not explicitly or implicitly impose a strong password requirement. Employees do that because they care more about their work process and performance being affected by attacks than the time and effort of memorizing strong passwords. At this stage, employees' behaviors comply with password security and result in the desired outcome, protecting the organization's information assets and resources well (Foorthuis, 2012). This stage of compliance instantiates both formal compliance and substantive compliance.

The third stage is the fulfillment of responsibilities to check compliance behavior, in which employees carry out their responsibilities in security policies when using the organization's information and technologies (see Table 1 and Figure 1). Similar to the goal alignment stage behaviors, employees comply with the security policy and use strong passwords in their accounts. However, at this stage of self-engagement, employees worry that they would be penalized if they used a weak password and hackers attack their accounts. Such concerns about personal benefit loss push employees to view password security compliance as their responsibility (Bulgurcu et al., 2010). As a result, employees will assess their security behaviors

regularly, trying to reduce potential security risks. However, employees fulfil their responsibilities passively as they are not interested in organizational norms. When an organization's security goal conflicts with their benefit, they constantly assess whether it is worthwhile to violate the security policy to get their work done quickly. Employees also account for the expected loss from the security threats when evaluating the costs and benefits of compliance in the long run. Thus, compliance behaviors at this stage include all formal, substantive, and responsible compliance features.

The fourth stage is the alignment of compliance behaviors and beliefs with organization's security policies, in which employees develop their beliefs about security policy compliance and change their compliance behavior per their beliefs. At this stage, people adopt consistent compliance behavior even without requirements. For example, employees who receive new work accounts with default passwords actively check the policy requirements and change to strong passwords to ensure account security. Even if an organization's policy requirements are incomprehensive, employees will change their passwords to protect accounts based on their perception of password security, which is more effective for security than the organization's existing security policies. Finally, employees may recommend more comprehensive security practices or policies to the organization. Employees take responsibility for securing their accounts to realize their self-value (Tyler and Blader, 2005). Thus, employees' compliance behaviors at this stage include all formal, substantive, responsible, and normative conformity features.

The fifth stage is assisting others to comply with organization's security policies, in which employees recommend and assist others in security policy compliance. For example, employees who have fulfilled the security policy requirements and changed their account passwords will

recommend and assist their colleagues in conforming to the policy. In this way, they cooperate with others and help shape a secure work environment in the organization (Hsu et al., 2015). Ideally, in a stable security environment, each employee has formed their own security beliefs, and everyone agrees with each other on their security behavior. Thus, security policy compliance at this stage includes all formal, substantive, responsible compliance, normative conformity, and altruistic cooperation features.

In the first three stages, employees' compliance behaviors are formal, substantive, and responsible compliance, which is the essential compliance behavior in the workspace. In contrast, employees have normative conformity and altruistic cooperation in stages 4 and 5. Thus, they perform the additional security duties in developing security awareness, improving security behavior, and creating a secure work environment.

Employee commitments refer to the psychological connections that employees perceive to the work objectives (Klein et al., 2009). Different levels of employees' self-engagement in security policies affect the extent of employee commitments. In the first three stages, employees play a passive role in complying with security policies without spontaneously contributing to positive security outcomes. Employees are guided by security policies to engage in security activities in their daily work. Employees do what the organization requires. In stages 4 and 5, employees play an active role in improving their security behavior via conforming to security policies and even assisting others in security activities related to security policies. These two stages need no security policies to guide employees' security behaviors. Specifically, in the normative conformity stage, employees have the motivation to work with security professionals. They gain security knowledge and improve their skills to protect organization's information resources (Safa et al., 2018; Safa et al., 2019). In the altruistic cooperation stage, employees have extensive

security protection experience to help others in security policy compliance and developing a secure work environment (Hsu et al., 2015). And they do these for the good of the organization.

From the response perspective, employees' response to security policies varies in five stages, from low to high self-engagement (see Figure 1). In the first three stages, employees usually respond to security policies in a passive way of acquiescence where they withhold their thoughts about security policies avoiding any potential sanctions because they don't want to offend management by having a different opinion. In contrast, in the last two stages, voicing recommendations to the organization goes along with normative conformity. Finally, employees respond to security policies actively because they are willing to speak out opinions and ideas about security policies to the management, hoping to improve current security controls.

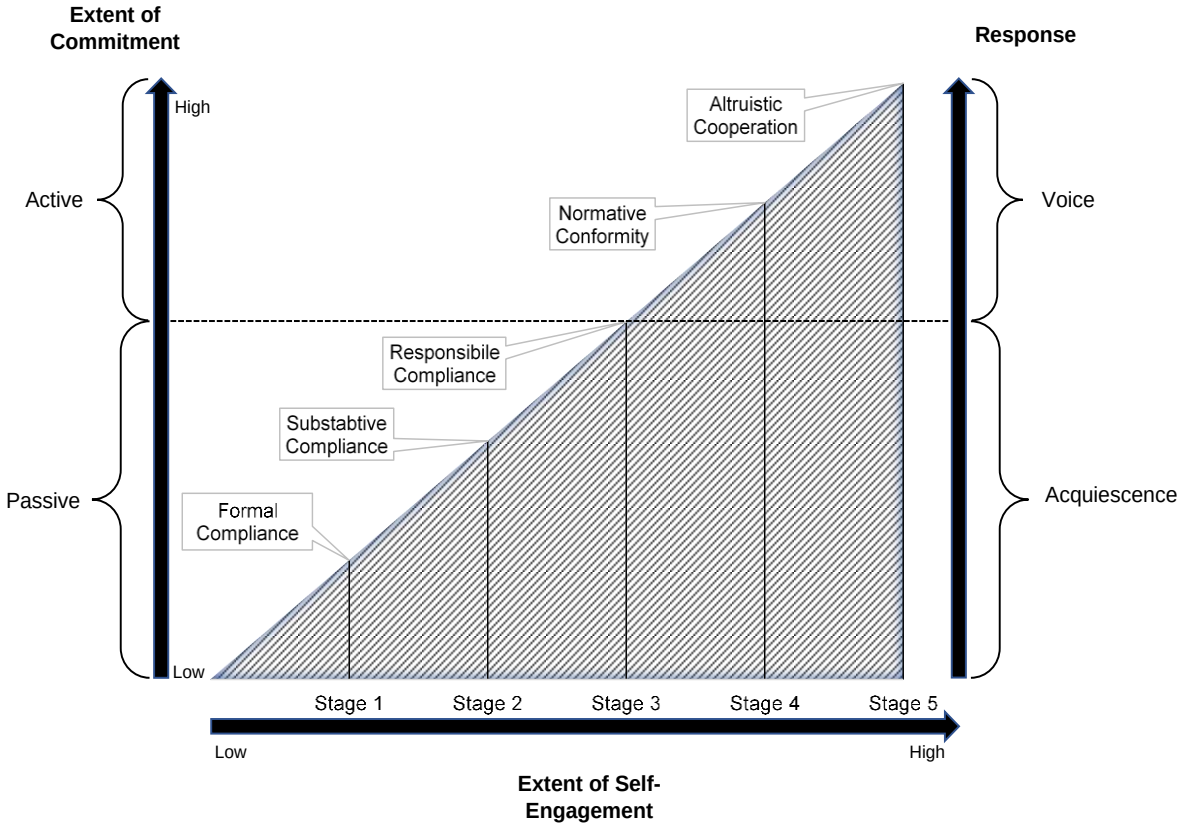

Figure 1. A Multidimensional Dynamic Model of Security Policy Compliance

Furthermore, employees may change their compliance behaviors in the same security context over time. Therefore, investigating why and how employees' compliance behaviors change is necessary to develop and implement security policies. To study the inconsistency of compliance behavior, we categorize three types of behavioral inconsistency in our dynamic conceptual framework.

Type 1 refers to the situation in which employees' compliance behaviors change from security policy compliance to the violation, causing adverse security outcomes for the organization. In Type 2, employees' behaviors downgrade from a high-level to a low-level self-engagement stage, decreasing the effectiveness of the organization's security. For example, an employee changes compliance behaviors from Stage 3 to Stage 1 (i.e., responsible compliance to formal compliance). Although the employee still complies with the security policy, the organization does not want to see this kind of change happens because the employee degenerates their security behaviors and contributes the minimal positive security outcomes. These two types of changes neither align with behavioral consistency nor organizations' expectations. Type 3 behavioral change is from a low-level to a high-level self-engagement stage, increasing the effectiveness of the organization's security. Organizations expect employees to change their compliance behavior as they become more engaged in security policies, particularly from passive compliance to active cooperation.

Behavioral Change	**Definition**	**Change Direction**	**Example**
Type 1	Employees' behavior changes from security policy compliance to violation causing the negative security outcomes to the organization.	Compliance -> Violation	Employees used to comply with security policies but violate them now.

Type 2	Employees' behavior changes from a high-level self-engagement stage to a low-level self-engagement stage, causing a reduction in positive security outcomes to the organization.	Compliance -> Compliance	Employees used to comply with security policies in Stage 3 but have degenerated to Stage 1 now.
Type 3	Employee behavior changes from a low-level self-engagement stage to a high-level self-engagement stage, bringing a promotion in positive security outcomes to the organization.	Compliance -> Compliance	Employees used to comply with security policies in Stage 1 but have improved to Stage 3 now.

Table 2. Behavioral Inconsistency in Security Policy Compliance

PROPOSED RESEARCH METHOD

Besides conceptualizing compliance with security policies from academic perspectives, we will take a concept mapping approach (Trochim,1989) to investigate compliance from professionals' perspectives. Concept mapping is a type of structured conceptualization using a mixed-method approach to define a dominant construct and develop its measurement. A current IS study used this approach in conceptualizing "cyber hygiene" (Vishwanath et al., 2020). We will follow the same steps to conceptualize security policy compliance and investigate its multiple dimensions.

First, we will recruit five panelists to participate in a brainstorming session where we ask them to share their thoughts, feelings, and ideas about security policy compliance. Second, we will use NVivo software to code generated statements and create the cluster maps and concept maps. Third, we will analyze the maps' validity and summarize security policy compliance dimensions. Last, if the results are not significant and valid, we will conduct another brainstorming session with five other panelists to compare the final concept maps. All panelists work in different organizations in the U.S. with various working experiences and backgrounds.

EXPECTED CONTRIBUTION AND CONCLUSION

Security policy compliance has been defined and measured from different perspectives and dimensions (e.g., D'Arcy and Lowry, 2019; Donalds and Osei-Bryson, 2020; Hsu et al., 2015; Karjalainen et al., 2020). However, no research has comprehensively integrated these perspectives and dimensions to measure employees' compliance behaviors in workspaces. Our study fills this research gap and conceptualizes security policy compliance as a multidimensional construct, which examines the compliance behaviors from the dimension of self-engagement, voice response, and temporal consistency. The contributions of this study are threefold.

First, this study extends and enriches our understanding of security policy compliance by conceptualizing it as a multidimensional term. In the previous security policy context, IS studies viewed security policy compliance as unidimensional. Ours is the first study that defines and measures security compliance as a multidimensional behavior in a dynamic process. Second, our study accounts for the changes in the role image (i.e., commitment) of employees when we measure security policy compliance behavior. Third, we use a brainstorming format of the concept mapping approach to investigate the multidimensional aspects of security policy compliance from the practitioners' perspective.

However, this study has serval limitations. First, our model does not account for the impacts of governmental security policies and laws on organizational security. Employees' conformity and cooperation behavior are mainly affected by perceived social beliefs and norms, which shape their social value judgment. Government policies or laws lead to changes in employees' social value judgement, which influences individuals' security perceptions and thus their attitudes and behaviors toward security policies (Zimbardo and Leippe, 1991). Also, formal security policies may not exist in some small or middle size organizations. Future studies can

examine informal security rules, guidelines, or procedures in the organizational security contexts. Second, protecting organizations from insider threats is not limited to individual behaviors; group or organization-level behaviors contributes to security management. For example, employees working together as a group to create a secure work environment can better achieve the objectives and effectiveness of security policies (Hsu et al., 2015). Future research may investigate security policy compliance as group behavior and name it compliance climate to define it and develop measures for it. Third, our model only considers full compliance. Employee compliance is an ongoing process and may not be complete. Partial compliance is also a type of compliance (Karjalainen et al., 2019), where employees do not intend to violate security policies. During the compliance process, employees' actual actions may not catch up with the expected progress, but they still work toward the eventual full compliance. Future research can also examine security policy non-compliance or violation as a multidimensional term in a dynamic model.

REFERENCES

Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes, 50*(2), 179-211.

Balozian, P., and Leidner, D. (2017). Review of IS security policy compliance: Toward the building blocks of an IS security theory. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems, 48*(3), 11-43.

Bélanger, F., Collignon, S., Enget, K., and Negangard, E. (2017). Determinants of early conformance with information security policies. *Information & management, 54*(7), 887-901.

Bond, R., and Smith, P. B. (1996). Culture and conformity: A meta-analysis of studies using Asch's (1952b, 1956) line judgment task. *Psychological bulletin, 119*(1), 111.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., and Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. *European Journal of Information Systems, 18*(2), 151-164.

Bottoms, A. (2013). Compliance and community penalties. In *Community penalties* (pp. 101-130). Willan.

Brinsfield, C. T. (2013). Employee silence motives: Investigation of dimensionality and development of measures. *Journal of Organizational Behavior, 34*(5), 671-697.

Britt, T. W., Dickinson, J. M., Greene-Shortridge, T. M., and McKibben, E. S. (2007). Self-engagement at work. *Positive organizational behavior*, 143-158.

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*, 523-548.

Chan, M., Woon, I., and Kankanhalli, A. (2005). Perceptions of information security in the workplace: linking information security climate to compliant behavior. *Journal of information privacy and security, 1*(3), 18-41.

Chen, Y., Galletta, D. F., Lowry, P. B., Luo, X., Moody, G. D., and Willison, R. (2021). Understanding inconsistent employee compliance with information security policies through the lens of the extended parallel process model. *Information Systems Research, 32*(3), 1043-1065.

Cialdini, R. B., and Goldstein, N. J. (2004). Social influence: Compliance and conformity. *Annu. Rev. Psychol., 55*, 591-621.

Cox, J. (2012). Information systems user security: A structured model of the knowing–doing gap. *Computers in Human Behavior, 28*(5), 1849-1858.

Cram, W. A., D'arcy, J., and Proudfoot, J. G. (2019). Seeing the Forest and the Trees: A Meta-Analysis of the Antecedents to Information Security Policy Compliance. *MIS Quarterly, 43*(2), 525-554.

Crossler, R. E., Long, J. H., Loraas, T. M., and Trinkle, B. S. (2014). Understanding compliance with bring your own device policies utilizing protection motivation theory: Bridging the intention-behavior gap. *Journal of Information Systems, 28*(1), 209-226.

D'Arcy, J., and Lowry, P. B. (2019). Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal, 29*(1), 43-69.

D'Arcy, J., and Teh, P.-L. (2019). Predicting employee information security policy compliance on a daily basis: The interplay of security-related stress, emotions, and neutralization. *Information & management, 56*(7), 103151.

DiBenigno, J. (2018). Anchored personalization in managing goal conflict between professional groups: The case of US Army mental health care. *Administrative Science Quarterly, 63*(3), 526-569.

Donalds, C., and Osei-Bryson, K.-M. (2020). Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents. *International Journal of Information Management, 51*, 102056.

Fishbein, M. (1980). A theory of reasoned action: Some applications and implications. *Nebraska Symposium on Motivation, 27*, 65–116.

Foorthuis, R.M. (2012). *Tactics for Internal Compliance: A Literature Review*. Chapter of "Project Compliance with Enterprise Architecture", pp. 153-198, Doctoral dissertation (PhD thesis), Utrecht University, Center for Organization and Information.

Foorthius, R. (2012). Tactics for Internal Compliance: A Literature Review. Chapter of "Project Compliance with Enterprise Architecture", Doctoral dissertation Utrecht University, 153-198.

Guo, K. H., and Yuan, Y. (2012). The Effects of Multilevel Sanctions on Information Security Violations: A Mediating Model. *Information & Management*, Vol. 49, No. 6: pp.320-326.

Hedström, K., Kolkowska, E., Karlsson, F., and Allen, J. P. (2011). Value conflicts for information security management. *The Journal of Strategic Information Systems, 20*(4), 373-384.

Henson, R. H. (1997). Analysis of the concept of mutuality. *Image--the Journal of Nursing Scholarship, 29*(1), 77-81.

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), 282-300.

Humaidi, N. (2013). Exploratory Factor Analysis of User's Compliance Behaviour towards Health Information System's Security. *Journal of Health and Medical Informatics, 04*(02).

Humaidi, N., and Balakrishnan, V. (2015). The Moderating Effect of Working Experience on Health Information System Security Policies Compliance Behaviour. *Malaysian Journal of Computer Science, 28*(2), 70-92.

Humaidi, N., and Balakrishnan, V. (2018). Indirect effect of management support on users' compliance behaviour towards information security policies. *Health Information Management Journal, 47*(1), 17-27.

Jaafar, N. I., and Ajis, A. (2013). Organizational climate and individual factors effects on information security compliance behaviour. *International Journal of Business and Social Science, 4*(10).

Johnston, A. C., Warkentin, M., Dennis, A. R., and Siponen, M. (2019). Speak their language: Designing effective messages to improve employees' information security decision making. *Decision Sciences, 50*(2), 245-284.

Karjalainen, M., Sarker, S., and Siponen, M. (2019). Toward a theory of information systems security behaviors of organizational employees: A dialectical process perspective. *Information Systems Research, 30*(2), 687-704.

Karjalainen, M., Siponen, M., Puhakainen, P., and Sarker, S. (2020). Universal and culture-dependent employee compliance of information systems security procedures. *Journal of Global Information Technology Management, 23*(1), 5-24.

Karlsson, F., Karlsson, M., and Åström, J. (2017). Measuring employees' compliance–the importance of value pluralism. *Information and Computer Security*. Vol. 25 No. 3, pp. 279-299.

Klein, H. J., Molloy, J. C., and Cooper, J. T. (2009). Conceptual foundations: Construct definitions and theoretical representations of workplace commitments. *Commitment in organizations: Accumulated wisdom and new directions, 1*, 3-36.

Knoll, M., and Van Dick, R. (2013). Do I hear the whistle…? A first attempt to measure four forms of employee silence and their correlates. *Journal of business ethics, 113*(2), 349-362.

Kolkowska, E., and Dhillon, G. (2013). Organizational power and information security rule compliance. *Computers and Security, 33*, 3-11.

Kuo, K. M., Talley, P. C., and Lin, D. Y. M. (2021). Hospital Staff's Adherence to Information Security Policy: A Quest for the Antecedents of Deterrence Variables. *INQUIRY: The Journal of Health Care Organization, Provision, and Financing, 58*(1-12).

Kyngäs, H. (2000). Compliance of adolescents with chronic disease. *Journal of clinical nursing, 9*(4), 549-556.

Li, H., Luo, X. R., and Chen, Y. (2021). Understanding information security policy violation from a situational action perspective. *Journal of the Association for Information Systems*, *22*(3), 5.

Liang, H., Xue, Y., and Wu, L. (2013). Ensuring employees' IT compliance: carrot or stick? *Information Systems Research, 24*(2), 279-294.

Limayem, M., and Hirt, S. G. (2003). Force of habit and information systems usage: Theory and initial validation. *Journal of the Association for information Systems, 4*(1), 3.

Liu, C., Wang, N., and Liang, H. (2020). Motivating information security policy compliance: The critical role of supervisor-subordinate guanxi and organizational commitment. *International Journal of Information Management, 54*, 102152.

Mathisen, J. (2004), "Measuring information security awareness – a survey showing the Norwegian way to do it", Master's thesis, NISlab Norwegian Information Security Laboratory, Campus IT University.

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

Ormond, D., Warkentin, M., and Crossler, R. E. (2019). Integrating cognition with an affective lens to better understand information security policy compliance. *Journal of the Association for Information Systems, 20*(12), 4.

Pinder, C. C., and Harlos, K. P. (2001). "Employee silence: Quiescence and acquiescence as responses to perceived injustice," in *Research in personnel and human resources management*, K. M. Rowland, and G. R. Ferris (ed.), Emerald Group Publishing Limited.

Ponemon Institute. (2022). 2022 Ponemon Cost of Insider Threats Global Report. Ponemon Institute.

Posey, C., Roberts, T. L., Lowry, P. B., and Hightower, R. T. (2014). Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. *Information & management, 51*(5), 551-567.

Posey, C., and Shoss, M. (2022). Research: Why employees violate cybersecurity policies. *Harvard Business Review*.

Robinson, G., and McNeill, F. (2008). Exploring the dynamics of compliance with community penalties. *Theoretical Criminology, 12*(4), 431-449.

Rowe, F. (2005). Are decision support systems getting people to conform? The impact of work organization and segmentation on user behavior in a French bank. *Journal of Information Technology, 20*(2), 103-116.

Safa, N. S., Maple, C., Furnell, S., Azad, M. A., Perera, C., Dabbagh, M., and Sookhak, M. (2019). Deterrence and prevention-based model to mitigate information security insider threats in organisations. *Future Generation Computer Systems, 97*, 587-597.

Safa, N. S., Maple, C., Watson, T., and Von Solms, R. (2018). Motivation and opportunity based model to reduce information security insider threats in organisations. *Journal of Information Security and Applications, 40*, 247-257.

Settineri, S., Frisone, F., Merlo, E. M., Geraci, D., and Martino, G. (2019). Compliance, adherence, concordance, empowerment, and self-management: five words to manifest a relational maladjustment in diabetes. *J Multidiscip Healthc, 12*, 299-314.

Sikolia, D., Twitchell, D., and Sagers, G. (2016). Employees' adherence to information security policies: a partial replication. *Proceedings of the Twenty-second Americas Conference on Information Systems*.

Silic, M., and Lowry, P. B. (2020). Using design-science based gamification to improve organizational security training and compliance. *Journal of Management Information Systems, 37*(1), 129-161.

Simons, M. (1992). Interventions related to compliance. *The Nursing Clinics of North America, 27*(2), 477-494.

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

Siponen, M., Pahnila, S., and Mahmood, M. A. (2010). Compliance with information security policies: An empirical investigation. *Computer, 43*(2), 64-71.

Straub, D. W. (1990). Effective IS Security: An Empirical Study. *Information Systems Research*, Vol. 1, No. 3: pp. 255-276.

Trochim, W. M. (1989). An introduction to concept mapping for planning and evaluation. *Evaluation and program planning, 12*(1), 1-16.

Turel, O., Xu, Z., and Guo, K. (2020). Organizational citizenship behavior regarding security: Leadership approach perspective. *Journal of Computer Information Systems, 60*(1), 61-75.

Tyler, T. R., and Blader, S. L. (2005). Can Businesses Effectively Regulate Employee Conduct? The Antecedents of Rule Following in Work Settings. *Academy of Management Journal, 48*(6), 1143-1158.

Van Dyne, L., Ang, S., and Botero, I. C. (2003). Conceptualizing employee silence and employee voice as multidimensional constructs. *Journal of Management Studies, 40*(6), 1359–1392.

Vance, A., Siponen, M., and Pahnila, S. (2012). Motivating IS security compliance: insights from habit and protection motivation theory. *Information & Management, 49*(3-4), 190-198.

Vishwanath, A., Neo, L. S., Goh, P., Lee, S., Khader, M., Ong, G., and Chin, J. (2020). Cyber hygiene: The concept, its measure, and its initial tests. *Decision Support Systems, 128*, 113160.

van Zadelhoff, M. (2016). The biggest cybersecurity threats are inside your company. *Harvard Business Review, 19*.

Warkentin, M., Johnston, A. C., Shropshire, J., and Barnett, W. D. (2016). Continuance of protective security behavior: A longitudinal study. Decision Support Systems, 92, 25-35.

Willison, R., and Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS quarterly*, 1-20.

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

Yazdanmehr, A., Wang, J., and Yang, Z. (2020). Peers matter: The moderating role of social influence on information security policy compliance. *Information Systems Journal, 30*(5), 791-844.

Zimbardo, P. G., and Leippe, M. R. (1991). *The psychology of attitude change and social influence*. New York: McGraw-Hill.