9-2022

Organizational and Team Culture as Antecedents of Protection Motivation Among IT Employees

Shwadhin Sharma
California State University, Monterey Bay, ssharma@csumb.edu

Eduardo Aparicio
California State University, Monterey Bay

Computers & Security 120 (2022) 102774

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

Organizational and team culture as antecedents of protection motivation among IT employees

Shwadhin Sharma*, Eduardo Aparicio

College of Business, California State University Monterey Bay, 100 Campus Center, Seaside, CA 93955, USA

ARTICLE INFO

Article history:
Received 24 December 2021
Revised 17 April 2022
Accepted 22 May 2022
Available online 26 May 2022

Keywords:
Organizational culture
Team culture
Protection motivation theory
Information compliance
IT employees

ABSTRACT

The rapid development of technology and information systems has led to higher information security-related issues in an organization. The age of remote working (i.e., telecommuting) has further increased information security related incidents that need to be adequately addressed. This paper extends the protection motivation theory by drawing insights from organizational and institutional theory literature to examine how organizational culture and subcultures such as team culture impact information security compliance. The primary objective of this study is to understand the impact of the dimensions of organizational culture and team culture on employees' perceived threats and coping motivation associated with information security compliance. The study applied structural equation modeling to analyze survey responses of 341 IT employees in the United States. The result of the study indicates that both organization and team culture impacts employees' perception to appraise threat and coping, which in turn impacts behavioral intention to comply with information security policies. The findings of this study contribute to the information security compliance research by demonstrating the importance of developing an information security culture within an organization and its subgroups.

1. Introduction

The rapid development of technology and information systems has increased information security-related issues in an organization. The recent cyber-attacks on Facebook, Apple, CNA Financial, Microsoft Exchange, Sierra Wireless, and Gyrodata within the last few years show the importance of protecting information technologies. Information security and compliance have become even more critical during the age of remote and hybrid jobs where companies are allowing their employees to work from anywhere around the world. Remote working is presumed to be a factor in causing data breaches (Report, 2021). Understanding and securing information is critical, given that the average total cost of a data breach increased by nearly 10%, from $3.86 million to $4.24 million per incident, the highest average total cost ever recorded (Report, 2021). As such, information security cannot rely solely on technology as people have been found to be a critical link (Tang et al., 2016). Thus, it is important to create a working environment and culture where security behavior is an integral part of the organization (Mahfuth et al., 2017).

An organization's culture and subculture impact the series of beliefs, attitudes, values, customs, and behaviors adopted by its employees (Belias and Koustelios, 2014), which in turn affects the information security of the company (Mahfuth et al., 2017). The way people interact with each other, participate in decision-making, believe in rules, adapt to the changes, develop ethical leadership, and show consistency towards policies, will shape their information security behavior. Culture determines what will be prioritized within an organization (Canning et al., 2020).

Culture refers to the shared values and beliefs of individuals within a unit, such as an organization and team (Sun, 2008). It implies the patterns, arts, customs, values, symbols, and products of an institution and group (Ein-Dor et al., 1993; Dasgupta and Gupta, 2019). Culture is believed to be the single most important factor accounting for the success or failure of an organization (Naqshbandi and Tabche, 2018). It impacts how employees formally and informally act in an organizational context (Briody et al., 2018). It influences the behaviors of employees and the activities of the entire organization, including acceptance of newer technology (Leidner and Kayworth, 2006a) and compliance with security (Uchendu et al., 2021). The culture of an organization and a group or team inspires appropriate or inappropriate security action, which in return creates security norms in the organization (Hu et al., 2012). Organizations recognize that developing culture

* Corresponding author.
E-mail address: ssharma@csumb.edu (S. Sharma).

https://doi.org/10.1016/j.cose.2022.102774

motivates employees toward positive information protection behaviors but for a variety of reasons, creating a positive culture is difficult (Al Hogail, 2015). Thus, exploring the organization and team culture within an organization is appropriate and meaningful (Dasgupta and Gupta, 2019) for predicting information protection motivation behaviors.

Despite the recommendations made in the previous literature that an espoused organizational and team culture would guide and improve information security behavior, there is a lack of studies that take into account their impact (Nasir et al., 2019). While studies have examined the roles of a number of individual factors, such as the national culture of employees (Crossler et al., 2019; Menard et al., 2018) on security compliance, research on the role of espoused organizational culture and team culture has been limited. Similarly, the research that has focused on organizational culture has studied individual behavior in regard to acceptance of technology (Dasgupta and Gupta, 2019).

It is also important to note that organizational culture and team culture are two related but separate artifacts that need to be studied separately. This has been discussed further in the literature review section (under Section 2.3). Organizations nowadays have a flatter hierarchy where employees often belong to a team and are committed to its culture (Chanana, 2021). The distinction between an organization's culture and subculture, such as team culture, is becoming more important as the dynamics and structures of organizations are changing rapidly with remote work trends established by COVID. As organizations are becoming more and more virtual, employees are spending more time with their groups and are more accustomed to the culture of the team rather than that of the overall organization (Adkins and Caldwell, 2004; Asatiani et al., 2021). Thus, studying the impact of organizational culture and team culture separately on information security compliance is important.

Also, the limited studies that have focused on culture in information systems (IS) assume that an organization's culture can be treated as a monolithic culture (Ramachandran et al., 2008). However, this assumption has been questioned in other fields. Researchers in anthropology, sociology, and psychology emphasizes that the organizational culture may vary across different groups within organizations (Jermier et al., 1991; Boisnier and Chatman, 2003). These subcultures are usually formed around existing divisions, departments, and functional or professional groups, which are usually known as teams (Trice and Beyer, 1993). These subcultures can sometimes supplement each other with the organizational culture and sometimes conflict with each other (Sackmann, 2021). Applying the same reasoning, it can be safely stated that the culture within an organization that impacts information security compliance is not monolithic in nature and will vary across teams throughout the organization (Kolkowska, 2011). Indeed, focusing only on organizational culture without exploring the subcultures such as team culture that engages different actors and values across the teams limits the understanding of the employee's behavior towards information security (Ruighaver et al., 2007; Ramachandran et al., 2008).

This study addresses the gap of limited focus on organizational culture in terms of employees' protection motivation behavior. It also addresses limited to no empirical focus on the impact of subcultures on information security compliance. Understanding how organizational and team culture impact the protection motivation theory (PMT) and information security behaviors is important for a variety of reasons discussed earlier. The primary questions this study examines are as follows (1) How does espouse organizational culture impact IT employees' intention to perform secure behaviors? (2) How does team culture affect an IT employee's intention to perform secure behaviors? These questions target the possible link between espoused organizational culture and team culture and the relationships of these two cultures with the commonly used protection motivation constructs.

The remainder of this paper is structured as follows. First, we review the literature on organization and team culture and PMT. Then, we propose the conceptual model along with the supporting hypotheses used to test the model. Next, the research method and data analysis are discussed. We then conclude our paper with a discussion of the results, contributions to research and industry, limitations, and opportunities for future research, followed by conclusions.

2. Theoretical foundation and hypothesis development

In this section, we discuss the theoretical framework for our study, which guides our conceptual model presented later. We start with the description of the PMT, which is a seminal theory used in understanding information security compliance. As this study focuses on culture, we also provide a description and literature review on culture, especially in regard to its impact on information systems. We end this section by proposing our research model and hypotheses.

2.1. Literature review on protection motivation theory (PMT)

PMT was developed by Rogers (1975) to explain the cognitive process people engage in to mediate their behavior when they face health and public safety-related threat and fear. The theory is based primarily on the fact that people perform threat appraisals to appraise existing situations in health and safety and engage in associated coping mechanisms. This appraisal process affects their intention to take precautionary action and can lead to adaptive or maladaptive behaviors. Adaptive behaviors are suggested responses that are believed effective at protecting the individual against the threat. Maladaptive responses are composed of any variety of behaviors in which the individual fails to enact the recommended response. The threat appraisal consists of artifacts such as threat severity and threat vulnerability. The coping appraisal consists of self-efficacy, response-efficacy, and response cost.

Prior research studies have widely used PMT to explain information security behaviors (Johnston and Warkentin, 2010; Liang and Xue, 2009; Menard et al., 2018). Indeed, it has been noted as one of the most powerful explanatory theories for predicting an intention to engage in protective actions such as information security (Anderson and Agarwal, 2010). Some examples of PMT being used in the Information Security (IS) field include identifying the predictors that differentiate between users who secure their home wireless networks and those who do not (Woon et al., 2005); exploring the empirical investigation of factors affecting small and medium-sized business executives' decision to adopt anti-malware software for their organizations (Lee and Larsen, 2009); studying the impact of organizational, environmental, and behavioral factor on the adoption of information security practices and policies (Herath and Rao, 2009); studying the impact of information security awareness on desktop security behavior (Hanus and Wu, 2016); analyzing the impact of individual characteristics such as collectivism and psychological ownership of information within the context of information security-related behaviors (Menard et al., 2018).

2.2. Literature review: culture and information systems

While there is no consensus on what constitutes culture, it's often referred to as the values and beliefs of individuals within a unit or a group, such as a nation, organization, functional area, or team. Culture has been used in understanding several aspects of the IS field over the period of time. Previous literature has supported the

notion that an organizational culture that promotes security awareness increases information security compliance by forming an environment conducive to following policy and rules (Hu et al., 2012; Al Hogail, 2015; Vroom and Solms, 2004). Studies have found that a security-aware organizational culture will reduce the likelihood that employees will engage in misbehavior and harmful interaction with information assets (Da Veiga and Eloff, 2010). Culture will set a precedent on what is acceptable within an organization in terms of information security policy.

Culture has been studied in the context of maximizing usage of existing systems and motivating IT employees for innovativeness, efficiency, and trust. Ein-Dor et al. (1993) and Kappos and Rivard (2008) studied the impact of national cultural environments and factors such as economic, demographic, and sociopsychological into a general framework of information systems. Culture has also been studied to understand the difference in the motivation of the analysts and programmers across different nations (Couger, 1986) and the difference between the different levels of IT professions and executives (Gindley, 1992). Warkentin et al. (2015) reiterated the importance that national culture plays in the design, adoption, and use of information systems and suggested combining and even comparing western and eastern perspectives on these IS topics. Claver et al. (2001) recommended studying the mutual relationships among information technologies, IS, and organizational culture to improve the organizational behavior required to maximize the efficiency of usage of information systems. Thatcher et al. (2003) studied and found relationships between dimensions of culture, qualitative and quantitative work overload, and personal innovativeness with information technology. Lowry et al. (2010) explored the impact of culture, social presence, and group composition on trust in technology-supported groups. The study found that national culture has a significant impact on trust among technology-supported decision-making groups.

Culture has also been studied to understand IT adoption and diffusion. Straub (1994) studied the effect of national culture on IT diffusion and found that the national culture plays an important role in the predisposition toward and selection of electronic communications media. Similarly, Rivard et al. (2011) studied the importance of organizational culture in the implementation of information systems in a hospital setting. Leidner and Kayworth (2006a) examined how the culture at various levels, including national, organizational, and group, can influence the successful implementation and use of information technology. After a literature review, the study developed six themes of IT-culture research, emphasizing culture's impact on IT, IT's impact on culture, and IT culture. Dasgupta and Gupta (2019) explored the impact of espoused organizational culture on the adoption of information systems in India. The study found that espoused cultural traits influence users' acceptance and use of Internet technology in a government agency in India.

There have been a few studies that explore the impact of culture on security compliance, but most of them are focused on individual or national culture or are qualitative in nature. Menard et al. (2018) explored the impact of cross-culture on the security behaviors of the people. Analyzing primarily two cross-cultural variables - collectivism and psychological ownership of information –the study found that individual's personal orientation toward collectivism has an impact on psychological ownership and the intention not to perform secure behaviors. National culture such as espoused individualism-collectivism and uncertainty avoidance has also been studied as antecedents to an individual's threat and coping appraisal toward protecting information (Crossler et al., 2019). Based on the data collected from two separate countries, the study concluded that individualism-collectivism and uncertainty avoidance significantly affect threat and coping appraisals, with uncertainty avoidance demonstrating a slightly stronger effect. In their qualitative study, Tang et al. (2016) agreed that an organizational culture encouraging employees to comply with information policies related to collecting, preserving, disseminating, and managing information would improve information security. The study presented a relationship map showcasing the impact of organizational culture on information security practices based on the interviews conducted.

The study of culture has also often come under scrutiny. Avison and Myers (1995) stated that the concept of culture being used in IS literature to explain the design and use is relatively narrow and suggest using the anthropological view of the relationship between IT and organizational culture. While Myers and Tan (2002) agreed that understanding the cultural differences in the deployment of information technology is important, the analysis of "national culture" in the current IS research literature is too simplistic. The study proposed to view national culture as contested, temporal, and emergent to incorporate a more dynamic and complete view of culture in the IS field. Jackson (2011) stated that the current research simplifies the impact of organizational culture on the adoption of information systems and suggested including Martins and Martins's (2002) three perspectives on culture – namely, integration, differentiation and fragmentation, and grid and group cultural theory. This offers a more penetrating account of how organizational culture influences IS adoption. In a similar line, Karahanna et al. (2005) also suggest researchers to include more than national culture to understand managerial and work behavior. The study suggests that the behaviors of IT employees are affected by professional, organizational, and group-level culture. Recognizing that individuals' workplace behavior is a function of all different cultures simultaneously is the best way to move forward. A few studies have theoretically explored how an organization's security culture in IS field has been treated as a monolithic culture (Ramachandran et al., 2008), and such assumptions need to be questioned (Kolkowska, 2011). Organizations, especially the ones with a flatter hierarchy, have several subcultures around teams and professional groups that may coexist or conflict (Kolkowska, 2009). Thus, it's important to study organizational culture along with subcultures such as team culture to understand the overall behavior of individuals (Da Veiga and Eloff, 2010).

Thus, it can be safely summarized that (a) culture has been used to explore its role in the adoption, use, and diffusion of technology (b) has been studied in regard to how the national culture of employees impacts security compliance, and (c) treating organizational culture as a monolithic culture.

2.3. Organizational culture vs. team culture

The effect of culture is not homogeneous but somewhat dependent on the extent to which the individual subscribes to various cultural values related to their group, organization, profession, nation, and units (Srite and Karahanna, 2006). Also, the effect of culture often differs across the level of units as the characteristics of the culture vary across nations, organizations, groups and teams, and professions. As such, assessing each individual's espoused cultural values across different units such as organizations and teams, is both appropriate and meaningful for predicting individual-level behavior (Dasgupta and Gupta, 2019; Shin et al., 2016). While IS research papers have studied culture as monolithic in nature and thus, focused on organizational culture only, previous literature studies have shown that there are several subcultures around teams and professional groups that may coexist or even conflict (Kolkowska, 2009). Thus, the organizational culture and team culture both need to be studied while exploring the security compliance behavior of the employees (Ramachandran et al., 2008).

Organizational culture is one of the most important factors in organizational effectiveness and employee work outcomes (Deal and Kennedy, 1983; Schein, 1990), including effective usage of information systems and policy compliance (Menard et al., 2018; Crossler et al., 2019; Tang et al., 2016). However, with technological advancement and newer managerial styles, there has been a blurring of organizational boundaries and the proliferation of self-managed teams or autonomous work teams, which has brought team and group cultures to the forefront (Adkins and Caldwell, 2004). Team culture comprises of the distinct clusters of understanding, beliefs, and values of the team an employee is related to in the work setting, and little has been studied about its role and importance (Shin et al., 2016). Team culture may be affected by the organizational culture, but each team and group can have their own distinct beliefs and values that may differ significantly from the organizational culture. The organizational culture reflects an organization-level construct which many accurately reflect macro-level sentiments but may not always measure the micro-level beliefs which the team culture usually covers (Ritchie et al., 2013). Also, the difference between an organization's culture and team culture is becoming more important to be explored as the introduction of remote and hybrid work during COVID has changed the dynamics and structures of organizations in almost all industries. As employees are spending more time with their groups or teams while working virtually and have become more reliant on self-managed teams maintaining an overall organizational culture may become difficult (Adkins and Caldwell, 2004; Asatiani et al., 2021). Thus, it is important to understand that organizational culture and team culture (within that organization) may differ. Different teams within a company can and will manifest their own culture (Brajdic, 2017).

Organizations are composed of several teams, groups, and departments. An employee may be impacted by organizational culture, but the team an employee is working for directly or indirectly plays a bigger role in shaping his/her behavior. While organizational culture is usually what scholars discuss the most, a few researchers have explored the role of subcultures among groups within an organizational culture (Lawrence and Lorsch, 1967; Van de Ven et al., 1980). Kam et al. (2015) state that every organizational culture consists of a team culture that constitutes trust, belonging, values, and beliefs among the members of the teams that they are closely related to. As per the literature review performed by Boisnier and Chatman (2003), organizations can have strong overall culture and at the same time have a distinct subculture such as team culture at the same time. The organizational culture can act as the pivotal one, and the team culture can act as the peripheral one. Pivotal culture, such as the organizational culture, prevails strongly within the organization and is enforced by sanctions, while peripheral culture can strongly prevail within a team but may not be sanctioned by the organization (Adkins and Caldwell, 2004). The team culture may reflect organizational culture but will have its own identity and values, which may change from one team to another. However, despite the numerous amounts of research on the antecedents of team performance, the role of team cultures has only received scant attention (Shin et al., 2016).

The range and variety of subcultures within different teams are as diverse as the range and variety of existing organizational cultures (Bloor and Dawson, 1994; Hofstede, 1998). Subcultures of teams are usually developed by the supervisor and shaped and confirmed by the rest of the teams. Some researchers may argue that an organization with a strong culture does not need or may not even have a team subculture. However, past literature has found that team subcultures can be developed within any organization that has strong integrated cultures, and the team culture does not weaken the overarching culture (Boisnier and Chatman, 2003). The saying "People leave managers, not companies" also shows how an organization can have a subculture developed by managers and supervisors, which impacts lower-level employees.

3. Research model and hypothesis development

Fig. 1 provides an overview of the conceptual model that is proposed and later tested empirically in our study. The conceptual model is primarily based on the seminal theory of protection motivation, which has been used to empirically explain employees' behavior in security compliance. Expanding on this PMT theory, this current study contributes to understanding the role of organizational culture and team culture on the intention of the employees to comply with security policies.

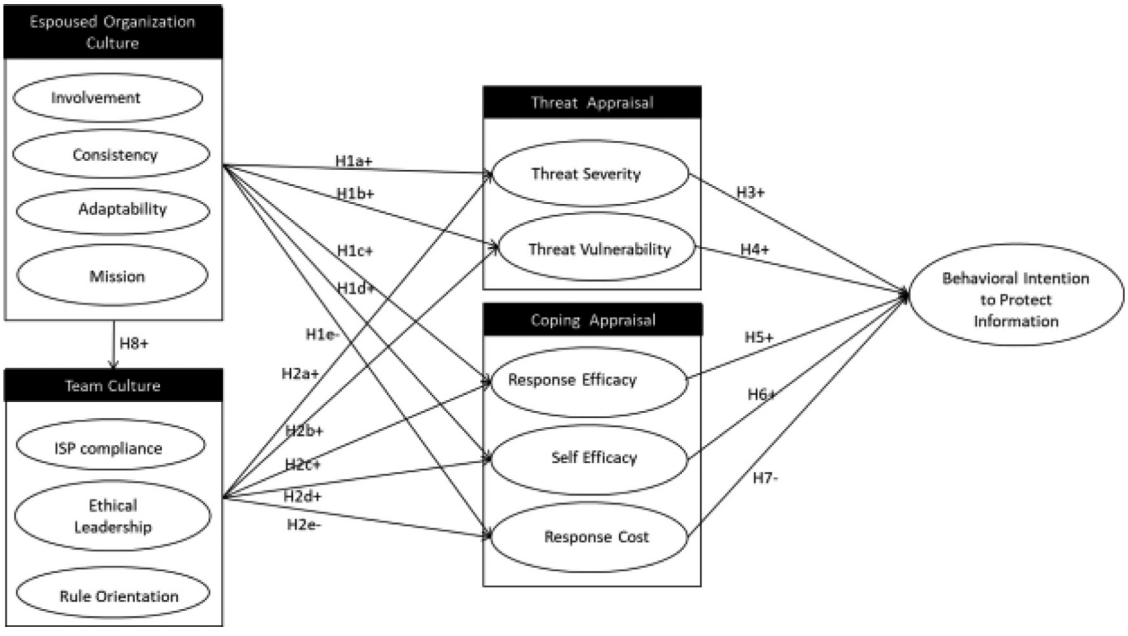

Fig. 1. Conceptual research model.

There has not been a consensus on what constitutes organizational culture. Schein (1985) proposed a three-layered approach to understanding the organizational culture that consisted of organizational structure and processes, espoused cultural beliefs and values, and the underlying assumptions. However, the work focused on the espoused cultural beliefs and values as the primary artifact. Schein (1990) did not present a quantitative way to measure the espoused cultural values. Understanding the limitation, Denison (1990) and Denison and Mishra (1995) created a model of culture and effectiveness that can empirically measure organizational culture at an individual level (as compared to national) using four dimensions: adaptability, involvement, mission, and consistency. Denison's model of culture and effectiveness presents the interrelations of an organization's culture, adaptable management practices, consistency in policies, engagement of employees in decision-making, and proper mission statements. Involvement trait is defined as the degree to which individuals at all levels of the organization are engaged in a collaborative manner to achieve the objectives of the organization. This trait includes building human capability, empowering employees for decision-making, and collaborating across units. Consistency trait is defined as the consistent, agreeable, and established values in the organization for problem-solving, efficiency, and effectiveness. Adaptability trait is the ability to scan the external environment and respond to the ever-changing needs of its stakeholders. It includes traits such as creating changes, responding to the changes, and organizational learning. Mission trait is the degree to which the organization and its members have a vision and strategic direction to where they are going, how they will reach there, and how each employee can contribute to the organization's success.

Several studies have applied Denison and Mishra's model of culture in the IS field for various purposes. The purpose of this paper is to explore the factors that enable end-user adoption of e-government services in Pakistan, where these facilities are at a rudimentary stage. Ahmad et al. (2013) applied Denison and Mishra's model of culture to understand factors that enable factors that enable end-user adoption of e-government services in Pakistan. Chen (2011) applied the same culture model to find the impact of environmental organizational culture and environmental leadership on the organization's green organizational identity and green competitive advantage. Dasgupta and Gupta (2019) used the same four espoused cultural traits to find how the culture influences users' acceptance and use of Internet technology in a government agency in India. In this current paper, we follow Denison (1990) and Denison and Mishra (1995) in creating the four layers of our organizational culture.

While the researchers have explored the overall effects of organizational culture on so many factors, including productivity, satisfaction, and information security compliance, the existence of subcultures within an organization such as team culture has been a widely observed phenomenon (Hofstede, 1998; Jerimer et al., 1991). The importance of understanding and studying subcultures such as team culture has become more pronounced recently in the field such as anthropology, sociology, and psychology. Previous literature has shown how managers' and supervisors' leadership influences employees' deviant activities, including that in IS field (Martinko et al., 2013). The several layers and variables within the team impact the employee's behavior. It is important to conduct an investigation on how ethical leadership, ISP compliance leadership, and perceived rule orientation in the department impact employee's overall perception of information security compliance (Wang and Xu, 2021; Hu et al., 2012). Members of a team or a group often have a certain perception of information security governance by the leaders and colleagues that set their own perception of security compliance . ISP Compliance Leadership is defined as the information security compliance culture set up by the leaders and supervisors of the team, which often impacts the rest of the team members. The managers and the supervisors have the authority and the responsibility to mobilize or allocate funds and resources for information security compliance. The supervisors that grab the opportunity to display leadership often become role model for other employees in the group/team (El-Haddadeh et al., 2012). A team leader's role in complying with information security, disciplining employees who show deviant behavior, and showcasing ethical leadership has been found to impact employees' intention to comply with information security (Wang and Xu, 2021). Ethical leadership is generally defined as "the demonstration of normatively appropriate conduct through personal actions and interpersonal relationships, and the promotion of such conduct to followers through two-way communication, reinforcement, and decision-making" (Brown 2007, p. 141). It often leads to the satisfaction of employees, along with reinforcement of positive outcomes (Neubert et al., 2009). The previous literature has shown that ethical leadership in groups and teams leads to employee satisfaction, productivity, higher retention, and higher information security compliance (Wang and Xu, 2021). Compliance with information security also often depends on the employee's perception of respect for authority, rationality for policies, and understanding of hierarchy and formal communications, known as rule orientation (Van Muijen, 1999). An organization with a strong rule orientation seeks stability and control by developing carefully designed policies and instructions and effectively communicating processes within an organization (Hu et al., 2012). Clearly stated rules and instructions help employees model their behaviors, facilitate their compliance and cooperate with the rules and practices as they feel more in control of their actions and outcomes (Boss et al., 2009). An employee who has a higher level of perceived rule orientation in the team would comply with the information security.

Culture has been operationalized in several ways in the literature, with the majority of the ones, including that in Information Systems literature, treating it as a first-order reflective, second-order formative model (DasGupta and Gupta 2019; Denison and Mishra, 1995). Thus, in this study as well culture will be treated as a first-order reflective, second-order formative model.

PMT was first proposed by Rogers (1975), later drawn based on social cognitive theory (Bandura, 1977), and further expanded by Maddux and Rogers (1983). Pahnila et al. (2007) considered the effect that information quality has on intentions to comply with security policies, using PMT as a foundation. Workman et al. (2008) proposed a threat control model to explain why an individual would choose not to protect himself when faced with a threat, even if he believed in his ability to do so. Lee and Larsen (2009) studied the effects of social influence, specifically vendor support and IT budget, on managers' attitudes toward the adoption of anti-spyware software. Johnston and Warkentin (2010) proposed a Fear Appeal Model in information security where subjects were exposed to the imminent threat of harmful spyware but were given an easy-to-use anti-spyware tool to effectively protect their computers, similar to the threat-response pair described earlier. As shown by the literature, the focus of the theory was on threat appraisal and coping appraisal. Threat appraisal is determined by how detrimental the perceived threat is (threat severity); and the likelihood of personal exposure to the threat (threat susceptibility). Coping Appraisal assesses the individual's perceived ability to manage and avoid the threat described by Threat Appraisal. In this process of coping, the individual is confident in the perceived ability to correctly adapt and perform a protective behavior (self-efficacy), the perceived effectiveness of the recommended response to protect from threat (response efficacy), and the perceived amount of time, money, or effort required to perform the recommended response (response cost).

Threat severity encompasses the employees' assessment or perception of how detrimental the information security threat is for themselves and the organization, while threat vulnerability implies the perception of the likelihood of the employees being vulnerable to the information security threat such as hacking, malware, and phishing (Floyd et al., 2000). As culture impacts people's beliefs and values, it can impact employees' perception of threat severity and threat vulnerability (Menard et al., 2018). Acceptance of organizational cultures by employees facilitates internal control and coordination. A consistent and adaptable culture also informs participants about what is important to perform, how it is supposed to be performed, and to what use it is put (Starbuck et al., 2001). Perceiving a threat as severe and acting upon it by following the security policy is an example of an employee who is influenced by a well-established organization's culture. A strong organizational culture installs a perception of how vulnerable an information system can be and installs a perceived fear of how severe a non-compliance can be (Aurigemma and Mattson, 2018). Understandability of the employees regarding perceived vulnerability and perceived severity of the information security threat to stay prepared when an actual threat such as data phishing, hacking, or malware attacks hits the company is an outcome of an established culture. In an organization where the culture is to adapt to the changes and requirements, where users are involved in developing a consistent information security decision making, and where information security is a part of the mission, the employees understand the perceived severity of the threat and the perceived vulnerability of the systems. Thus, we hypothesize:

H1a. Organizational culture will have a positive effect on perceived threat severity.

H1b. Organizational culture will have a positive effect on perceived threat vulnerability.

Response efficacy is the perceived belief that the adaptive response that an individual take will work (Floyd et al., 2000). In the context of this study, it is the perception of the employees that applying protective action will be effective in protecting the information security of self or other stakeholders within the company. Self-efficacy is the perception of an employee in their ability to actually carry out the adaptive response. Culture has been found to impact people's confidence towards their adaptive response and their overall outlook towards carrying out the response (Medin and Bang 2013). The belief and values of the organization often impact the beliefs employees have about themselves and their actions. The values of the organization and the support systems it provides often help to cultivate confidence in the employees (McAllister and Bigley, 2002). Indeed, culture has been found to impact a person's sense of self-worth (Sasaki et al., 2014). An organizational culture that engages employees in policymaking and is consistent and adaptable to the need of all stakeholders will help in harboring confidence in the employees to take actions to secure information. Previous literature has found that national culture impacts the response efficacy and self-efficacy of employees in complying with information security policy (Zhang and Borden, 2020). Extending the same reasoning, it can be said that the organizational culture can impact the self-efficacy and response efficacy of employees in complying with information security policy. Thus, we hypothesize:

H1c. Organizational culture will have a positive effect on perceived response efficacy.

H1d. Organizational culture will have a positive effect on perceived self-efficacy.

Response costs are any costs such as monetary, personal, time, and effort associated with taking the adaptive coping response to follow information security policy (Floyd et al., 2000). While deciding whether to comply with the organization's ISP, the employees consider the costs or effort of doing so, and this perceived response cost may negatively influence their attitude (Bulgurcu et al., 2010). When the culture of the organization involves developing information security policies by taking inputs from employees, focusing on security policies as a part of the mission, and creating consistent but adaptable values and rules, employees go above and beyond to perform their responsibilities. Employees who find the organization's culture positive are ready to spend more time and effort to show their commitment to the information security policy (Sharma and Warkentin, 2019). A strong organizational culture increases the commitment of the employees toward the existing beliefs. It reduces the perceived response cost of employees towards certain behavior, such as compliance with information security policy. Therefore, we assume:

H1e. Organizational culture will have a negative effect on perceived response cost.

While the organizational culture can impact an individual, the impact, however, may vary across different groups depending on the culture of the groups. Each team within an organization may be separated based on profession or skills, and their behaviors are strongly influenced by the cultural beliefs of the profession that they belong to (Karahanna et al., 2005). It has, for instance, been argued that IT professional teams who are often responsible for security issues in an organization belong to a distinct professional culture (Guzman et al., 2009) than many others who may not have stronger opinions and beliefs towards computers, systems, compliance, and so on. Usually, team culture is heavily influenced by the observed conduct of its leader/s (Puhakainen and Siponen, 2010). Teams with ethical programs that emphasize policy compliance and behavioral monitoring of compliance significantly increase awareness of the severity and vulnerability of security threats (Hina et al., 2019). Following Jarvenpaa and Ives (1991) and Ahmad and Gao (2018), this paper believes that the compliance leadership, constant engagement, ethical leadership, and rule orientation that a supervisor or a team leader showcase impacts the general perception of the team members towards the perceived severity of the security threat and the possible vulnerability through such threats. Thus, we hypothesize:

H2a. Team culture will have a positive effect on perceived threat severity.

H2b. Team culture will have a positive effect on perceived threat vulnerability.

Given that a team with compliance leadership, ethical behavior, and rule orientation requires each member to overcome technical and social barriers and adapt to the practical organizational policies and realities, this will shape the confidence of the individuals along with their control over their responses and behaviors (Hu et al., 2012). Teams that are committed to the culture of information security are developing individuals that have higher perceived self-efficacy and perceived response efficacy regarding new and existing information security initiatives, programs, and policies. Such teams are rule-oriented and provide consistent training and awareness about rules, policies, and ethics (Bulgurcu et al., 2010) which leads to higher self-efficacy and response-efficacy. This also leads to commitment towards the culture of the group and, thus, a sense of lower response cost towards such policy compliance. Thus, it can be assumed that:

H2c. Team culture will have a positive effect on perceived response efficacy.

H2d. Team culture will have a positive effect on perceived self-efficacy.

H2e. Team culture will have a negative effect on perceived response cost.

The next five hypotheses are related to the five independent variables of the PMT model, whose relationship with behavioral intention to comply with information security policies has been empirically tested by previous studies. While the use of these hypotheses is not novel in the IS field, the application and testing of this theory's boundary conditions with newer constructs and contextualization is important for the growth of the field (Gregor and Klein, 2014; Menard et al., 2018). Based on the previous studies, threat susceptibility, threat severity, response efficacy, and self-efficacy decrease the end user's intention to perform maladaptive behaviors. Response cost has been found to negatively impact behavioral intention to comply with information security policies.

A basic premise of the PMT is the assumption that an individual initiates a cognitive threat appraisal process to evaluate a particular threat in information security in terms of its severity as well as the likelihood of such a threat affecting that individual (Rogers, 1975). When the threat is severe and highly damageable, and when the individual believes the company is vulnerable to the threat, research has found empirical evidence of them positively impacting the intention to protect information systems (Pahnila et al., 2007). Thus, we are hypothesizing the following:

H3. Threat severity will have a positive effect on an end user's intention not to comply with information security policy.

H4. Threat vulnerability will have a positive effect on an end user's intention not to comply with information security policy.

The coping appraisal is the additional process that takes place in determining the effectiveness of mitigating the chances of threat by evaluating response efficacy, self-efficacy, and response cost. When the confidence of an individual to perform the response is high, and when the individuals believe that the response will mitigate the threat, the intentions to protect information increase (Rogers, 1975). Performing a response to mitigate the threat comes with certain costs, such as time and resources. The impact of response cost has been extensively studied in PMT and has been found to negatively impact the intention to protect information (Menard et al., 2018). Likewise, we present the following hypotheses:

H5. Response efficacy will have a positive effect on an end user's intention not to comply with information security policy.

H6. Self-efficacy will have a positive effect on an end user's intention not to comply with In.

H7. Response cost will have a negative effect on an end user's intention not to comply with information security policy.

An organization can have a primary organizational culture and subculture that governs and shapes the behavior of the employees. However, the subcultures are usually related to the organizational culture in one or the other way. While a subculture of the team may conflict with the organizational culture, they usually have a "parent" and "child" relationship (Wolfgang and Ferracuti, 1970). The subculture may differ from organizational culture and even be conflicting at times, but they are not entirely different from the "parent" culture. Organizational culture often impacts group culture. Thus, we hypothesize:

H8. Group culture positively impacts team culture.

4. Methodology

4.1. Participants/Sample

In total, approximately 302 IT employees in the United States were recruited via Amazon Mechanical Turk (MTurk). All of these respondents were working in the field of information systems and technology, as the criteria for the survey were designed accordingly to collect responses from only those respondents. 66.8% of the respondents were male, and 32.5% were female. The majority (approximately 59.8%) of the respondents were between the age of 26 to 40 years. 53.3% of the respondents had income between 50 K to 100 K. 86.2% of the respondents were working in Private companies. 60.1% of the respondents held an intermediate job position. The demographic distribution of the respondents is presented below:

4.2. Measures and instrumentation

The following latent perceptual constructs were measured in the instrument with multi-item scales: organizational culture (involvement, consistency, adaptability, mission), team culture (ISP compliance leadership, ethical leadership, perceived rule orientation), threat appraisal (threat severity, threat vulnerability), coping appraisal (response efficacy, self-efficacy, response cost), and behavioral intention. Each item that represented the construct was adapted from existing literature and was modified as per the context of this study. Each item was measured using a five-point Likert scale that ranged from "strongly disagree" to "strongly agree." Appendix 1 provides the measurement instrument along with the source of the items. Several practices recommended by the literature were applied to reduce the common method bias (Podsakoff et al., 2003). The items were randomized within the instrument to minimize the order effect. The attention filters were presented in multiple places to filter inattentive respondents. Also, the anonymity of the respondents was ensured for reducing social desirability biases.

4.3. Panel and pilot testing

The items were collected from the literature review to ensure content validity. The instrument was further analyzed by an expert review panel consisting of subject matter experts as well as instrumentation experts. The results of the expert panel review led to a few minor adjustments. Once the survey was hosted in Qualtrics, the survey was pilot-tested among six individuals to receive their feedback and suggestions. Items were further modified accordingly.

4.4. Survey design

A survey questionnaire hosted in Qualtrics was used to collect data. A survey was administered in the English language. Previous research studies have shown that MTurk can be a valid source for recruiting respondents to participate in statistically rigorous academic research as long as the validity of the data is ensured (Lowry et al., 2016). To ensure the validity of the research, a rigorous posthoc analysis was performed. Out of the 372 responses collected, 70 responses were deleted as they were deemed unfit. These responses either failed the attention checker questions asked in the instrument, or they were completed within unreasonably short completion times (greater than three standard deviations from the mean completion time).

5. Data analysis

The research model for this study has thirteen constructs with behavioral intention to comply with security policies as the depen-

Table 1
Demographic distribution of survey respondents.

Gender	Frequency	Percentage	Job Position held	Frequency	Percentage
Male	228	66.86%	Entry-level	37	10.85%
Female	111	32.55%	Intermediate	205	60.12%
Others	2	0.59%	Senior	99	29.03%
Age	**Frequency**	**Percentage**			
18 to 25 years	31	9.09%	**Income**	**Frequency**	**Percentage**
26 to 40 years	204	59.82%	Less than $50,000	91	26.69%
41 to 60 years	99	29.03%	50k to 100 K	182	53.37%
Above 60 years	7	2.05%	100,001 to 150,000	63	18.48%
			More than 150 K	5	1.47%
Computer Experience	**Frequency**	**Percentage**			
0 to 5 years	68	19.94%	**Organization type**	**Frequency**	**Percentage**
6 to 10 years	194	56.89%	Public	34	9.97%
More than 10 years	79	23.17%	Private	294	86.22%
			Nonprofit/Govt.	10	2.93%
			Other	3	0.88%
Privacy and security Knowledge Level	**Frequency**	**Percentage**			
Novice/beginner	15	4.40%	**Tenure with company**	**Frequency**	**Percentage**
Advanced beginner	103	30.21%	0 to 5 years	111	32.55%
Competent	105	30.79%	6 to 10 years	179	52.49%
Proficient	58	17.01%	More than 10 years	51	14.96%
Expert	60	17.60%			

dent variable. This portion of the paper discusses the data analysis techniques used, such as instrument validity assessment, construct validity tests, and conceptual model analysis (Table 1).

5.1. Instrument validation

We used Partial Least Squares (PLS) through SmartPLS to measure the instrument validation and test the structural model of this study. The instrument was validated by performing convergent validity, discriminant validity, and reliability test. As all of the scales used for our research were reflective in nature, we used multiple items scales to measure our constructs. To measure convergent validity, we conducted statistical analysis to see the items loadings, cross-loadings, and Average Variance Extracted (AVE). Convergent validity is shown when the PLS indicators that are supposed to load on a particular construct load higher on their own loadings than on cross-loadings (Herath and Rao, 2009). Six items that cross-loaded on constructs other than their own were dropped. It is important to mention that construct called perceived rule orientation (i.e., RUL) has only one item as the second item cross-loaded with another construct. All estimated loadings, as shown in Table 2, are well above the acceptable magnitude of 0.7, which suggests good convergent validity (Chin and Marcolin, 1995). Anything below 0.40 was not included in the table below . Also, as shown in Table 2, AVE exceeds the threshold of 0.5 for all the constructs used in the study.

To examine discriminant validity, we further analyze the loadings and cross-loadings. The loadings of the items on their respective constructs were found to be at least an order of magnitude larger than any other loading (Gefen and Straub, 2005). Moreover, Table 3 below confirms convergent validity as the AVE for all constructs in this research model exceeded 0.5 and establishes discriminant validity as correlations of each construct with any other construct are less than the square root of the AVE (Fornell and Larcker, 1981). Reliability for all the constructs is above the threshold of 0.7. This shows that the study meets the reliability and internal consistency test.

We tested our research model and data for signs of common method bias. We applied Harman's single-factor test and found no evidence of common-method bias present in our study. The total variance extracted by one factor is around 30% only, which is less than the recommended threshold of 50% (Podsakoff et al., 2003). We also tested common method bias by using the variance inflation factor (VIF) calculated through the full collinearity test of the research model. Collinearity VIF values for the constructs in our model were below threshold 3.3 (Kock, 2015). Thus, this showed that our data does not have a common method bias problem and is ready for the structural model analysis.

5.2. Testing of the structural model

The structural model and its associated hypotheses were tested using SmartPLS (Ringle, 2005). To approximate the path coefficients and the amount of variance explained in mediating variables, we used bootstrapping resampling technique.

As suggested by Denison and Mishra (1995), we treated culture as a second-order formative construct. In SmartPLS, we set up organizational culture as a formative construct with the four cultural indicators or dimensions and the team culture as a formative construct with the three cultural dimensions. Each dimension of the culture was a reflective construct measured by multiple items. The rest of the model for SmartPLS was set up in line with our research model (see Fig. 1). As espoused organizational culture and team culture are set up as formative constructs, the SmartPLS outcome (Fig. 2) shows arrows from the dimensions to the respective cultural variables. Due to the use of second-order variables in the model and their endogenous nature, our research applied the two-step method (Hair et al., 2017), which is a combination of approximations to both variable evaluation and model evaluation. In the first step, which is the variable evaluation, we used the repeated indicators approach. The items of the first level reflective variables also load in the second level. In the second step, structural model evaluation, we used the single item variables calculated from the first step.

A formative construct refers to an index of a weighted sum of indicators. Thus, the values next to the arrows from the four organizational cultural indicators to espoused organizational culture and three team cultural indicators to team culture (as shown in Fig. 2) are the weights for the respective cultural indicators. Involvement (0.21), consistency (0.32), adaptability (0.34), and mission (0.36) are the indicators of the organizational culture, and these weights determine or cause the higher-order construct, espoused organizational culture. ISP compliance leadership (0.63), ethical leadership (0.45), and perceived rule orientation (0.05) are the indicators of the team culture, and these weights determine or cause the higher-order construct, team culture.

Table 2
Loadings, cross-loadings, and AVEs.

	AD	BI	CO	COM	ETH	IN	MI	RC	RE	RUL	SE	TS	TV	AVE
AD1	0.73													0.52
AD2	0.72													
AD3	0.71													
BI1		0.70												0.55
BI2		0.79												
BI3		0.72												
CO1			0.76											0.53
CO2			0.71											
CO3			0.71											
COM1				0.76										0.53
COM2				0.72										
COM3				0.74										
COM4				0.70										
ETH1					0.76									0.55
ETH3					0.74									
EHT4					0.72									
IN1						0.80								0.58
IN3						0.72								
MI1							0.75							0.58
MI2							0.79							
MI3							0.75							
RC1								0.84						0.67
RC2								0.80						
RE1									0.79					0.69
RE3									0.87					
Rul2										1.00				1.00
SE1											0.76			0.55
SE2											0.72			
SE3											0.75			
TS1												0.73		0.52
TS2												0.72		
TS3												0.71		
TV1													0.84	0.69
TV2													0.82	

AD = adaptability; CO = consistency; ETH: ethical leadership; COM = ISP compliance; IN = involvement; MI = mission; RE = response efficacy; RUL = perceived rule orientation; SE = self-efficacy; TS: threat severity; TV = threat vulnerability; BI = behavioral intention; RC = response cost.

Table 3
Inter-construct correlations.

	AD	CO	ETH	COM	IN	MI	RE	RUL	SE	TS	TV	BI	RC	Composite reliability
AD	0.72													0.76
CO	0.62	0.73												0.77
ETH	0.61	0.58	0.74											0.78
COM	0.62	0.60	0.69	0.73										0.82
IN	0.47	0.48	0.49	0.53	0.76									0.73
MI	0.55	0.58	0.56	0.65	0.45	0.76								0.81
RE	0.54	0.50	0.53	0.55	0.41	0.48	0.83							0.82
RUL	0.07	0.04	0.06	0.10	0.07	0.08	0.09	1.00						1.00
SE	0.54	0.50	0.53	0.60	0.43	0.47	0.44	0.11	0.74					0.79
TS	0.56	0.46	0.52	0.55	0.52	0.53	0.42	0.08	0.42	0.72				0.76
TV	0.41	0.37	0.53	0.56	0.42	0.39	0.42	0.12	0.46	0.50	0.83			0.81
BI	0.55	0.55	0.53	0.59	0.37	0.57	0.51	0.06	0.52	0.51	0.47	0.74		0.78
RC	0.44	0.41	0.51	0.59	0.40	0.45	0.31	0.13	0.37	0.39	0.45	0.36	0.82	0.80

AD = adaptability; CO = consistency; ETH: ethical leadership; COM = ISP compliance; IN = involvement; MI = mission; RE = response efficacy; RUL = perceived rule orientation; SE = self-efficacy; TS: threat severity; TV = threat vulnerability; BI = behavioral intention; RC = response cost; square-root AVEs are shown in shaded area on diagonal axis.

As shown in Fig. 2, results from PLS regression show that most of our hypotheses are supported. We first examine the espoused organizational culture variables and their role as antecedents to the five variables used within the PMT. We found that espoused organizational culture positively influences threat severity ($\beta = 0.46$, R^2=0.42, $p < 0.001$), response efficacy ($\beta = 0.37$, $R^2 = 0.40$, $p < 0.001$), and self-efficacy ($\beta = 0.31$, R^2=0.42, $p < 0.001$). Therefore, we found support for H1a, H1c, and H1d. Espoused organizational culture was not found to have a significant impact on threat vulnerability ($\beta = 0.04$, R^2=0.36, $p >$0.05), and response cost ($\beta = 0.13$, R^2=0.38, $p < 0.001$). Thus, H1b and H1e were not supported. We also examined the role of team culture as an antecedent to the variables of PMT. Team culture was found to have a positive and significant impact on threat severity ($\beta = 0.22$, $R^2 = 0.42$, $p < 0.05$), threat vulnerability ($\beta = 0.56$, R^2=0.36, $p < 0.001$), response efficacy ($\beta = 0.29$, R^2=0.42, $p < 0.001$), and self-efficacy ($\beta = 0.51$, R^2=0.38, $p < 0.001$). This supported our hypotheses H2a, H2b, H2c, and H2d. Team culture was found to have a significant impact on response cost ($\beta = 0.51$, R^2=0.38, $p <$0.001) but towards the opposite direction than hypothesized.

Furthermore, we examined the five variables associated with PMT in relation to the behavioral intention to comply with information security policies. Hypothesis H3, H4, H5, H6, and H7 examine the influence of threat severity, threat vulnerability, response efficacy, self-efficacy, and response cost on behavioral intention to follow information security policies and secure a com-

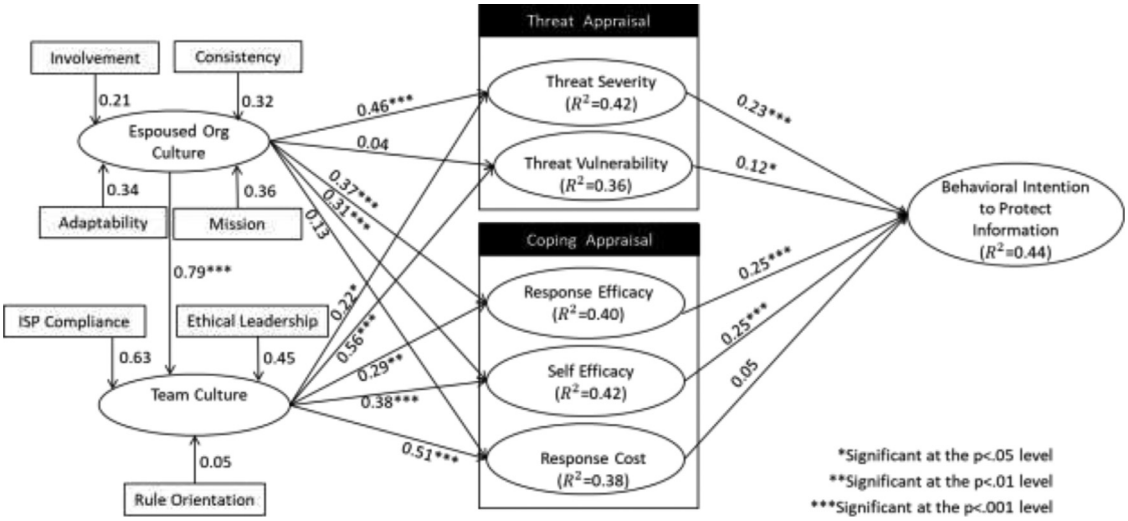

Fig. 2. Structural model.

pany's data. Threat severity ($\beta = 0.23$, $R^2 = 0.44$, $p < 0.001$), threat vulnerability ($\beta = 0.12$, $R^2 = 0.44$, $p < 0.05$), response efficacy ($\beta = 0.25$, $R^2 = 0.44$, $p < 0.001$), and self-efficacy ($\beta = 0.25$, R^2=0.44, $p < 0.001$) were all found to have a positive and significant impact on the behavioral intention to comply with information security policies. Response cost ($\beta = 0.05$, $R^2 = 0.44$, $p > 0.05$) was found to not have any influence on behavioral intention to protect information. Our analysis also found that espoused organizational culture has a positive impact on team culture ($\beta = 0.79$, $p < 0.001$). Thus, we found support for H8.

6. Discussion and conclusion

6.1. Key findings

This study contributes to the knowledge of the role of organizational and team culture in the context of information security behaviors by identifying the importance of protection motivation theory. Specifically, the study expands the existing limited focus on organizational culture and limited to no empirical focus on the impact of subcultures on information security compliance. Our research model drew on understanding the impact of the organizational cultural traits and team cultural traits on different factors associated with the PMT. The structural equation model shows that all the proposed path coefficients were significant towards the proposed direction except for four of them out of sixteen hypotheses. The results of this study are, for a large part, consistent with the previous findings. Espoused organizational culture was found to have a positive and significant relationship with threat severity, response efficacy, and self-efficacy. This implies that when the organization adapts to the recommendations of the employees, involves them in decision-making, has a clear mission, and is consistent with policies, it motivates them to comply with security policies. The team culture was also found to have a positive and significant impact on threat severity, threat vulnerability, response efficacy, and self-efficacy. These findings are consistent with the previous studies that have found a positive impact of culture on some form of protection motivation behavior of employees (Aurigemma and Mattson, 2018; Zhang and Borden, 2020). Also, threat severity, threat vulnerability, response efficacy, and self-efficacy were found to have a positive and significant impact on behavioral intention to comply with security policies. These findings are also consistent with the previous studies (Rogers, 1975; Menard et al., 2018; Pahnila et al., 2007). Espoused organizational culture was found to have no significant impact on threat vulnerability and response cost. Team culture was found to have a significant but positive impact on response cost. Similarly, response cost was found to have no significant impact on behavioral intention to comply with information security policy. While some studies on PMT have shown a significant relationship of response cost with culture as well as behavioral intention, the result has been inconsistent (Pahnila et al., 2007; Menard et al., 2018; Johnston and Warkentin, 2010). Thus, our finding is not surprising. This implies that a strong organizational security culture may not necessarily reduce the perception of the employees in terms of their responses cost associated with the compliance of information security policy. As suggested in previous literature (Wolfgang and Ferracuti, 1970), our analysis also found that espoused organizational culture has a positive impact on team culture.

6.2. Contributions and implications for theory and practice

Prior research has found that an espoused organizational and team culture would guide and improve information security behavior (Nasir et al., 2019). However, the research on the role of espoused organizational culture and team culture has been limited. Similarly, the research that has focused on organizational culture has studied individual behavior in regard to acceptance of technology (Dasgupta and Gupta, 2019). Understanding this research gap, our study has empirically demonstrated that the espoused organizational culture and team culture play an important role in the protection motivation of the employees and in their intention to comply with information security policy.

First, our study is one of the earliest ones to test the espoused organization cultural values from Denison and Mishra (1995) in the context of protection motivation theory in regard to IT employees. This study is also one of the earliest ones to test the espoused team cultural values in the context of protection motivation theory. The culture of an organization and a team inspires appropriate as well as inappropriate security action, which in return creates security norms in the organization (Hu et al., 2012). Our study makes an important contribution to understanding the role of organizational and team cultural values in the protection motivation of employees.

Second, this study also explores the possibility of treating culture with several subdimensions and as subgroups. The limited studies that have studied culture in IS field assume that an organization's culture can be treated as a monolithic culture

(Ramachandran et al., 2008). These subcultures can supplement each other or with the organizational culture and sometimes conflict with each other (Sackmann, 2021). This study addresses the need to study organizational culture and its subculture, such as team culture, separately while examining the protection motivation of the employees.

Third, this study also has implications for the companies. Employers, managers, and supervisors can take help from the findings of this research and focus on both organizational culture as well as team culture to motivate their IT employees toward the protection of information systems. This will help the employers to understand and acknowledge the different values, beliefs, and traits that employees may carry across different groups and within the organization as a whole. Following the output of our study, managers and supervisors should put emphasis on team culture so that employees stay motivated to protect themselves and their data by following follow appropriate information security policy. While these subcultures may sometime complement each other, as shown by our last hypothesis, they may conflict as well. It is important for the managers and supervisors to be aware of the interactions between these cultural dimensions. Making sure that the company involves employees as a part of the culture, keeps the culture consistent, adapt to the changes, focus on the mission, have ethical leadership, and has rules, helps in compliance with the information security policy.

6.3. Limitations and future research

We used a survey design method to empirically test our research model, and the data were collected using a self-administered survey questionnaire. Thus, this research may have limited precision and realism. To address this shortcoming, we suggest utilizing mix research methodology, which may offset the weakness of one method with the strength of another method (McGrath, 1995). The other limitation that this paper faced is the self-selection bias as the respondents self-selected themselves to take the survey that we posted on MTurk for a specific financial benefit. Future research can collect data from different sources at different timelines to make sure that it covers as many generalizable respondents as possible. Also, the data collected for this research are cross-sectional in nature. Future research may perform a longitudinal research study to prove these relationships better. Also, this study focused on different dimensions of organizational and team culture. However, there may be several other types of subcultures within an organization that needs to be studied. Future research can explore them in more detail. One of the limitations of this study is the use of convenience sampling. Our study consists of 66.8% of males, which may impact the generalizability of our study. Future research can use systematic or cluster sampling to make the study more generalizable across different demographics.

6.4. Conclusion

There have been limited studies that have focused on the impact of organizational culture on information security compliance, as the majority of the related studies either focus on national culture or focus on the implementation of newer information systems. Most studies, while examining the organizational culture in regard to information security compliance, have not considered the existence of subcultures and their impact on information security compliance. This is especially true in today's time of remote work, where individuals are spending more time with their team than with other stakeholders and groups (Yang et al., 2022). Our study addresses this research gap and focuses on organizational culture as well as team culture in empirically exploring the protection motivation behavior of the employees. Our study indicates that both organizational culture and team culture impacts employees' cognitive ability to appraise threat and coping, which in turn impacts behavioral intention to comply with information security policies. This study contributes to information security research by demonstrating the importance of developing an information security culture within an organization and its subgroups.

Declaration of Competing Interest

All persons who meet authorship criteria are listed as authors, and all authors certify that they have participated sufficiently in the work to take public responsibility for the content, including participation in the concept, design, analysis, writing, or revision of the manuscript. Furthermore, each author certifies that this material or similar material has not been and will not be submitted to or published in any other publications. Also, there is no funding from external parties to conduct this study that shows a conflict of interest.

CRediT authorship contribution statement

Shwadhin Sharma: Conceptualization, Writing – review & editing, Methodology, Formal analysis. **Eduardo Aparicio:** Conceptualization.

Appendix 1

Scaled variable & Measurement items		Refs.
Involvement		Denison and Mishra (1995)
IN1:	Most people in this company have input into decisions that affect them including practices regarding the protection of information.	
IN2:	Cooperation and collaboration across functional roles, including practices regarding the protection of information, is actively encouraged.	
IN3	This company engages and trains its staff about information security policy.	
Consistency		Denison and Mishra (1995)
CO1:	There is a high level of agreement about the way we do things in this company including practices regarding the protection of information.	
CO2:	Our approach to doing business, including practices regarding the protection of information, is very consistent and predictable.	
CO3	The company takes established information security policy into account when conducting business.	
Adaptability		Denison and Mishra (1995)
AD1:	People's comments and recommendations, including practices regarding the protection of information, often lead to changes in this organization.	
AD2:	This organization is very responsive and changes easily, including practices regarding the protection of information.	
AD3	This organization is prepared to adapt to changes for the sake of protection of information and data.	
Mission		Denison and Mishra (1995)
MI1:	This company has a long-term purpose and direction including practices regarding the protection of information.	
MI2:	There is a shared vision of what this organization will be like in the future including their practices regarding the protection of information.	
MI3	In this institution we have a clear idea of what caring for the information security entails for long-term success.	

(continued on next page)

Scaled variable & Measurement items		Refs.
Threat Vulnerability		Herath and Rao (2009)
TV1	I feel that my organization could become vulnerable to security breaches if I do not adhere to its information security policy.	
TV2	I feel that I could fall victim to a malicious attack if I fail to comply with my organization's information security policy.	
TV3	My organization's data and resources may be compromised if I do not pay adequate attention to information security policies and guidelines.	
Threat Severity		Herath and Rao (2009)
TS1	Having my computer infected by a virus can cause a severe problem for me and my organization.	
TS2	At work, having my confidential information accessed by someone without my consent or knowledge is a severe problem.	
TS3	Loss of data resulting from hacking is a severe problem for me and my organization.	
Response Efficacy		Herath and Rao (2009)
RE1	Every employee can make a difference when it comes to helping to secure the organization's information system.	
RE2	There is not much that any one individual can do to help secure the organization's information security.	
RE3	If I follow the organization information security policies, I can make a difference in helping to secure my organization's information security.	
Response Cost		Menard et al. (2018)
RC1	I would feel that following information security policy would take significant time away from my daily work.	
RC2	I would consider following information security policy to be time consuming.	
RC3	By taking the time to follow information security, I would not have enough time to complete my work.	
Self-Efficacy		Menard et al. (2018)
SE1	I would feel comfortable following most of the information system security policies on my own.	
SE2	If I wanted to, I could easily follow information system security policies on my own.	
SE3	I would be able to follow most of the information system security policies even if there was no one around to help me.	
Behavioral Intention		Johnston and Warkentin (2010)
BI1	I intend to comply with information security policy in the near future.	
BI2	I predict I will comply with information security policy in the near future.	
BI3	I plan to comply with information security policy in the near future.	
ISP Compliance Leadership		Amankwa et al. (2014)
Com1	My supervisor/manager often emphasize the importance of compliance with security policies.	
Com2	Information security policy is given a higher priority by my supervisor/manager.	
Com3	Organizational top management (including my supervisor/manager) have always demonstrated compliance with information security policies.	
Com4	My supervisor/manager emphasize the importance of compliance with security policies that exist in the organization	
Ethical leadership		Wang and Xu (2021)
Eth1	My immediate supervisor discipline employees who violate ethical standards.	
Eth2	My immediate supervisor conducts his/her personal life in an ethical manner.	
Eth3	My immediate supervisor discusses business ethics or values with employees.	
Eth4	My immediate supervisor sets an example of how to do things the right way in terms of ethics.	
Eth5	My immediate supervisor defines success not just by results but also the way they are obtained.	
Perceived rule orientation in the department		Hu et al. (2012)
Rul1	Instructions are written down and followed (in your department).	
Rul2	Jobs are performed according to defined procedures (in your department).	

References

Adkins, B., Caldwell, D., 2004. Firm or subgroup culture: where does fitting in matter most? J. Organ. Behav. Int. J. Ind. Occup. Organ. Psychol. Behav. 25 (8), 969–978.

Ahmad, I., Gao, Y., 2018. Ethical leadership and work engagement: the roles of psychological empowerment and power distance orientation. Manag. Decis. 56 (9), 1991–2005.

Ahmed, Z., Rehman, Z.U., Asad, A., Hussain, N., Bilal, A., 2013. The impact of organizational change on the employee's performance in banking sector of Pakistan. Ethiop. Int. J. Multidiscip. Res. 1 (1), 1–12.

Al Hogail, A., 2015. Cultivating and assessing an organizational information security culture; an empirical study. Int. J. Secur. Appl. 9 (7), 163–178.

Amankwa, E., Loock, M., Kritzinger, E., 2014. A conceptual analysis of information security education, information security training and information security awareness definitions. In: Proceedings of the 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014). IEEE, pp. 248–252.

Anderson, C.L., Agarwal, R., 2010. Practicing safe computing: a multimethod empirical examination of home computer user security behavioral intentions. MIS Q. 34 (3), 613–643.

Asatiani, A., Hämäläinen, J., Penttinen, E., Rossi, M., 2021. Constructing continuity across the organisational culture boundary in a highly virtual work environment. Inf. Syst. J. 31 (1), 62–93.

Aurigemma, S., Mattson, T., 2018. Exploring the effect of uncertainty avoidance on taking voluntary protective security actions. Comput. Secur. 73, 219–234.

Avison, D.E., Myers, M.D., 1995. Information systems and anthropology: and anthropological perspective on IT and organizational culture. Inf. Technol. People 8 (3), 43–46.

Bandura, A., 1977. Self-efficacy: toward a unifying theory of behavioral change. Psychol. Rev. 84 (2), 191.

Belias, D., Koustelios, A., 2014. Organizational culture and job satisfaction: a review. Int. Rev. Manag. Mark. 4 (2), 132–149.

Bloor, G., Dawson, P., 1994. Understanding professional culture in organizational context. Organ. Stud. 15 (2), 275–295.

Boisnier, A., Chatman, J.A., 2003. The role of subcultures in agile organizations. In: Peterson, R.S., Mannix, E.A. (Eds.), Leading and managing people in the dynamic organization. Lawrence Erlbaum Associates Publishers, pp. 87–112.

Boss, S.R., Kirsch, L.J., Angermeier, I., Shingler, R.A., Boss, R.W., 2009. If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. Eur. J. Inf. Syst. 18 (2), 151–164.

Brajdic, A., 2017. What the hell is 'team culture' and why is it so important? Prototypr. https://blog.prototypr.io/what-the-hell-is-team-culture-and-why-is-it-so-important-d923141854e5.

Briody, E.K., Berger, E.J., Wirtz, E., Ramos, A., Guruprasad, G., Morrison, E.F., 2018. Ritual as work strategy: a window into organizational culture. Hum. Organ. 77 (3), 189–201.

Brown, M.E., 2007. Misconceptions of ethical leadership: How to avoid potential pitfalls. Organizational Dynamics 36 (2), 140–155.

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

Canning, E.A., Murphy, M.C., Emerson, K.T., Chatman, J.A., Dweck, C.S., Kray, L.J., 2020. Cultures of genius at work: organizational mindsets predict cultural norms, trust, and commitment. Personal. Soc. Psychol. Bull. 46 (4), 626–642.

Chanana, N., 2021. Employee engagement practices during COVID-19 lockdown. J. Public Aff. 21 (4), e2508.

Chen, Y.S., 2011. Green organizational identity: sources and consequence. Manag. Decis. 49 (3), 384–404.

Chin, W., Marcolin, B., 1995. The holistic approach to construct validation in IS research: examples of the interplay between theory and measurement. In: Proceedings of the Administrative Sciences Association of Canada-Annual Conference, 16. Administrative Sciences Association of Canada, pp. 34–43 Vol.pp..

Claver, E., Llopis, J., González, M.R., Gasco, J.L., 2001. The performance of information systems through organizational culture. Inf. Technol. People 14 (3), 247–260.

Couger, J.D., 1986. Effect of cultural differences on motivation of analysts and programmers: singapore vs. the United States. MIS Q. 10 (2), 189–196.

Crossler, R.E., Andoh-Baidoo, F.K., Menard, P., 2019. Espoused cultural values as antecedents of individuals' threat and coping appraisal toward protective information technologies: study of US and Ghana. Inf. Manag. 56 (5), 754–766.

Da Veiga, A., Eloff, J.H., 2010. A framework and assessment instrument for information security culture. Comput. Secur. 29 (2), 196–207.

Dasgupta, S., Gupta, B., 2019. Espoused organizational culture values as antecedents of internet technology adoption in an emerging economy. Inf. Manag. 56 (6), 103142.

Deal, T.E., Kennedy, A.A., 1983. Culture: a new look through old lenses. J. Appl. Behav. Sci. 19 (4), 498–505.

Denison, D.R., 1990. Corporate Culture and Organizational Effectiveness. John Wiley & Sons.

Denison, D.R., Mishra, A.K., 1995. Toward a theory of organizational culture and effectiveness. Organ. Sci. 6 (2), 204–223.

Ein-Dor, P., Segev, E., Orgad, M., 1993. The effect of national culture on IS: implications for international information systems. J. Glob. Inf. Manag. (JGIM) 1 (1), 33–44.

El-Haddadeh, R., Tsohou, A., Karyda, M., 2012. Implementation challenges for information security awareness initiatives in e-government. In: Proceedings of the ECIS, p. 179 2012 Proceedings.
Floyd, D.L., Prentice-Dunn, S., Rogers, R.W., 2000. A meta-analysis of research on protection motivation theory. J. Appl. Soc. Psychol. 30 (2), 407–429.
Fornell, C., Larcker, D.F., 1981. Evaluating structural equation models with unobservable variables and measurement error. J. Mark. Res. 18 (1), 39–50.
Gefen, D., Straub, D., 2005. A practical guide to factorial validity using PLS-Graph: tutorial and annotated example. Commun. Assoc. Inf. Syst. 16 (1), 5.
Gregor, S., Klein, G., 2014. Eight obstacles to overcome in the theory testing genre. J. Assoc. Inf. Syst. 15 (11), 5.
Grindley, K., 1992. Information systems issues facing senior executives: the culture gap. J. Strateg. Inf. Syst. 1 (2), 57–62.
Guzman, I.R., Stam, K., Hans, S., Angolano, C., 2009. Human factors in security: the role of information security professionals within organizations. In: Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions. IGI Global, pp. 184–200.
Hanus, B., Wu, Y.A., 2016. Impact of users' security awareness on desktop security behavior: a protection motivation theory perspective. Inf. Syst. Manag. 33 (1), 2–16.
Herath, T., Rao, H.R., 2009. Protection motivation and deterrence: a framework for security policy compliance in organisations. Eur. J. Inf. Syst. 18 (2), 106–125.
Hina, S., Selvam, D.D.D.P., Lowry, P.B., 2019. Institutional governance and protection motivation: theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world. Comput. Secur. 87, 101594.
Hofstede, G., 1998. Attitudes, values and organizational culture: disentangling the concepts. Organ. Stud. 19 (3), 477–493.
Hu, Q., Dinev, T., Hart, P., Cooke, D., 2012. Managing employee compliance with information security policies: the critical role of top management and organizational culture. Decis. Sci. 43 (4), 615–660.
Jackson, S., 2011. Organizational culture and information systems adoption: a three--perspective approach. Inf. Organ. 21 (2), 57–83.
Jarvenpaa, S.L., Ives, B., 1991. Executive involvement and participation in the management of information technology. MIS Q. 205–227.
Jermier, J.M., Slocum Jr, J.W., Fry, L.W., Gaines, J, 1991. Organizational subcultures in a soft bureaucracy: resistance behind the myth and facade of an official culture. Organ. Sci. 2 (2), 170–194.
Johnston, A.C., Warkentin, M., 2010. Fear appeals and information security behaviors: an empirical study. MIS Q. 549–566.
IBM Report: cost of a data breach hits record high during pandemic. (2021, July 28). IBM Newsroom. https://newsroom.ibm.com/2021-07-28-IBM-Report-Cost-of-a-Data-Breach-Hits-Record-High-During-Pandemic.
Kam, H.J., Goel, S., Katertannakul, P., & Hong, S.G. (2015). Organizational security norms in the banking industry: the United States vs. South Korea. In Proceedings of Pre-ICIS Workshop on Information Security andPrivacy (SIGSEC), pp. 1-20
Kappos, A., Rivard, S., 2008. A three-perspective model of culture, information systems, and their development and use. MIS Q. 32 (3), 601–634.
Karahanna, E., Evaristo, J.R., Srite, M., 2005. Levels of culture and individual behavior: an investigative perspective. J. Glob. Inf. Manag. (JGIM) 13 (2), 1–20.
Kock, N., 2015. Common method bias in PLS-SEM: a full collinearity assessment approach. Int. J. E Collab. (IJEC) 11 (4), 1–10.
Kolkowska, E., 2009. Lack of compliance with IS security rules: value conflicts in social services in Sweden. In: Proceedings of the 8th Annual Security Conference. Las Vegas, USA 15-16 April 2009(pp. Article-no).
Kolkowska, E. (2011). Security subcultures in an organization-exploring value conflicts. In Proceedings of European Conference on Information Systems, pp. 1-13
Lawrence, P.R., Lorsch, J.W., 1967. Differentiation and integration in complex organizations. Adm. Sci. Q. 12 (1), 1–47.
Lee, Y., Larsen, K.R., 2009. Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. Eur. J. Inf. Syst. 18 (2), 177–187.
Leidner, D.E., Kayworth, T., 2006a. A review of culture in information systems research: toward a theory of information technology culture conflict. MIS Q. 30 (2), 357–399.
Leidner, D.E., Kayworth, T., 2006b. A review of culture in information systems research: toward a theory of information technology culture conflict. MIS Q. 357–399.
Liang, H., Xue, Y., 2009. Avoidance of information technology threats: a theoretical perspective. MIS Q. 33 (1), 71–90.
Lowry, P.B., D'Arcy, J., Hammer, B., Moody, G.D., 2016. Cargo Cult" science in traditional organization and information systems survey research: a case for using nontraditional methods of data collection, including mechanical Turk and online panels. J. Strateg. Inf. Syst. 25 (3), 232–240.
Lowry, P.B., Zhang, D., Zhou, L., Fu, X., 2010. Effects of culture, social presence, and group composition on trust in technology-supported decision-making groups. Inf. Syst. J. 20 (3), 297–315.
Maddux, J.E., Rogers, R.W., 1983. Protection motivation and self-efficacy: a revised theory of fear appeals and attitude change. J. Exp. Soc. Psychol. 19 (5), 469–479.
Mahfuth, A., Yussof, S., Baker, A.A., Ali, N.A., 2017. A systematic literature review: information security culture. In: Proceedings of the International Conference on Research and Innovation in Information Systems (ICRIIS). IEEE, pp. 1–6.
Martinko, M.J., Harvey, P., Brees, J.R., Mackey, J., 2013. A review of abusive supervision research. J. Organ. Behav. 34 (S1), S120–S137.
Martins, E., Martins, N., 2002. An organisational culture model to promote creativity and innovation. SA J. Ind. Psychol. 28 (4), 58–65.
McAllister, D.J., Bigley, G.A., 2002. Work context and the definition of self: how organizational care influences organization-basei self-esteem. Acad. Manag. J. 45 (5), 894–904.
McGrath, J.E., 1995. Methodology matters: doing research in the behavioral and social sciences. In: Readings in Human–Computer Interaction. Morgan Kaufmann, pp. 152–169.
Medin, D.L., Bang, M., 2013. Culture in the classroom. Phi Delta Kappan 95 (4), 64–67.
Menard, P., Warkentin, M., Lowry, P.B., 2018. The impact of collectivism and psychological ownership on protection motivation: a cross-cultural examination. Comput. Secur. 75, 147–166.
Myers, M.D., Tan, F.B., 2002. Beyond models of national culture in information systems research. In: Human Factors in Information Systems. IGI Global, pp. 1–19.
Naqshbandi, M.M., Tabche, I., 2018. The interplay of leadership, absorptive capacity, and organizational learning culture in open innovation: testing a moderated mediation model. Technol. Forecast. Soc. Change 133, 156–167.
Nasir, A., Arshah, R.A., Ab Hamid, M.R., Fahmy, S, 2019. An analysis on the dimensions of information security culture concept: a review. J. Inf. Secur. Appl. 44, 12–22.
Neubert, M.J., Carlson, D.S., Kacmar, K.M., Roberts, J.A., Chonko, L.B., 2009. The virtuous influence of ethical leadership behavior: evidence from the field. J. Bus. Ethics 90 (2), 157–170.
Pahnila, S., Siponen, M., Mahmood, A., 2007. Employees' behavior towards IS security policy compliance. In: Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS'07). IEEE pp. 156b–156b.
Podsakoff, P.M., MacKenzie, S.B., Lee, J.Y., Podsakoff, N.P., 2003. Common method biases in behavioral research: a critical review of the literature and recommended remedies. J. Appl. Psychol. 88 (5), 879.
Puhakainen, P., Siponen, M., 2010. Improving employees' compliance through information systems security training: an action research study. MIS Q. 34 (4), 757–778.
Ramachandran, S., Rao, S.V., Goles, T., 2008. Information security cultures of four professions: a comparative study. In: Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008). IEEE pp. 454–454.
Ringle, C.M.. SmartPLS 2.0 (M3). Hamburg.
Ritchie, W.J., Fornaciari, C.J., Drew, S.A., Marlin, D., 2013. Team culture and business strategy simulation performance. J. Manag. Educ. 37 (5), 601–622.
Rivard, S., Lapointe, L., Kappos, A., 2011. An organizational culture-based theory of clinical information systems implementation in hospitals. J. Assoc. Inf. Syst. 12 (2), 3.
Rogers, R.W., 1975. A protection motivation theory of fear appeals and attitude change1. J. Psychol. 91 (1), 93–114.
Ruighaver, A.B., Maynard, S.B., Chang, S., 2007. Organisational security culture: extending the end-user perspective. Comput. Secur. 26 (1), 56–62.
Sackmann, S.A., 2021. The development of culture and its subcultures. In: Culture in Organizations. Springer, Cham, pp. 57–78.
Sasaki, J.Y., Ko, D., Kim, H.S., 2014. Culture and self-worth: implications for social comparison processes and coping with threats to self-worth. In: Krizan, Z., Gibbons, F.X. (Eds.), Communal functions of social comparison. New York: Cambridge University Press, pp. 230–252.
Schein, E. H. (1985). Organizational culture and leadership. San Francisco, CA: Jossey-Bass.
Schein, E.H., 1990. In: Organizational Culture, 45. American Psychological Association, p. 109 Vol.p..
Sharma, S., Warkentin, M., 2019. Do I really belong?: impact of employment status on information security policy compliance. Comput. Secur. 87, 101397.
Shin, Y., Kim, M., Choi, J.N., Lee, S.H., 2016. Does team culture matter? Roles of team culture and collective regulatory focus in team task and creative performance. Group Organ. Manag. 41 (2), 232–265.
Srite, M., Karahanna, E., 2006. The role of espoused national cultural values in technology acceptance. MIS Q. 30 (3), 679–704.
Straub, D.W., 1994. The effect of culture on IT diffusion: e-mail and fax in Japan and the US. Inf. Syst. Res. 5 (1), 23–47.
Sun, S., 2008. Organizational culture and its themes. Int. J. Bus. Manag. 3 (12), 137–141.
Tang, M., Li, M.G., Zhang, T., 2016. The impacts of organizational culture on information security culture: a case study. Inf. Technol. Manag. 17 (2), 179–186.
Trice, H.M., Beyer, J.M., 1993. The Cultures of Work Organizations. Prentice-Hall, Inc.
Uchendu, B., Nurse, J.R., Bada, M., Furnell, S., 2021. Developing a cyber security culture: current practices and future needs. Comput. Secur. 109, 102387.
Starbuck, William H. and Hedberg, Bo, How Organizations Learn from Success and Failure (2001). Handbook of Organizational Learning and Knowledge; M. Dierkes, A. Berthoin Antal, J. Child, and I. Nonaka (eds.); Oxford University Press, 2001, Available at SSRN: https://ssrn.com/abstract=2708267
Van de Ven, 1980. *Measuring and Assessing Organizations*. John Wiley & Sons, New York.
Van Muijen, J.J., 1999. Organizational culture: the focus questionnaire. Eur. J. Work Organ. Psychol. 8 (4), 551–568.
Vroom, C., Von Solms, R, 2004. Towards information security behavioural compliance. Comput. Secur. 23 (3), 191–198.
Wang, X., Xu, J., 2021. Deterrence and leadership factors: which are important for information security policy compliance in the hotel industry. Tour. Manag. 84, 104282.
Warkentin, M., Charles-Pauvers, B., Chau, P.Y., 2015. Cross-cultural IS research: perspectives from Eastern and Western traditions. Eur. J. Inf. Syst. 24 (3), 229–233.

Wolfgang, M.E., Ferracuti, F., 1970. The subculture of violence. U: bersani, CA (ur.). Crime Delinq. Read. 5, 133–163.
Woon, I., Tan, G.W., & Low, R. (2005). A protection motivation theory approach to home wireless security. In Proceedings of International Conference on Information Systems, pp. 1-15.
Workman, M., Bommer, W.H., Straub, D., 2008. Security lapses and the omission of information security measures: A threat control model and empirical test. Computers in human behavior 24 (6), 2799–2816.
Yang, L., Holtz, D., Jaffe, S., Suri, S., Sinha, S., Weston, J., Teevan, J., 2022. The effects of remote work on collaboration among information workers. Nat. Hum. Behav. 6 (1), 43–54.
Zhang, X.A., Borden, J., 2020. How to communicate cyber-risk? An examination of behavioral recommendations in cybersecurity crises. J. Risk Res. 23 (10), 1336–1352.

Shwadhin Sharma is an Associate Professor in the College of Business at California State University Monterey Bay. His research interests are in the areas of technical and behavioral aspects of consumptions of technology and education. He actively pursues research areas such as privacy and security, electronic commerce and social commerce, big data analytics, the role of dispositional factors in IT, and IT adoption, and discontinuation. He has published his research in journals such as International Journal of Information Management, Journal of Computer Information Systems, Information Technology & People, Government Information Quarterly, and Computers & Security and several academic conferences. He serves on the editorial board of two Journals and has served as a reviewer for several reputed journals and conferences. Dr. Sharma also serves as the Resource/Listserv chair for SIG Decision Support and Analytics (SIGDSA) group which is a reputed chapter with Association of Information Systems. He has co-chaired a mini-track on “Social Network Analytics in Big Data Environment” in AMCIS 2016.

Eduardo Aparicio is a student at College of Business at California State University Monterey Bay. He is interested in research related to privacy and security of information systems.