The Effects of Antecedents and Mediating Factors on Cybersecurity Protection Behavior

Ling Li
Old Dominion University, lli@odu.edu

Li Xu
Old Dominion University, lxu@odu.edu

Wu He
Old Dominion University, whe@odu.edu

Original Publication Citation

Li, L., Xu, L., & He, W. (2022). The effects of antecedents and mediating factors on cybersecurity protection behavior. *Computers in Human Behavior Reports, 5*, 1-14, Article 100165. https://doi.org/10.1016/j.chbr.2021.100165

Contents lists available at ScienceDirect

Computers in Human Behavior Reports

journal homepage: www.sciencedirect.com/journal/computers-in-human-behavior-reports

The effects of antecedents and mediating factors on cybersecurity protection behavior

Ling Li [*], Li Xu, Wu He

Old Dominion University, Virginia, USA

ARTICLE INFO

Keywords:
Information security
Protection motivation theory
Employee security behavior
Types of organizations
Digital natives

ABSTRACT

This paper identifies opportunities for potential theoretical and practical improvements in employees' awareness of cybersecurity and their motivational behavior to protect themselves and their organizations from cyberattacks using the protection motivation theory. In addition, it contributes to the literature by examining additional variables and mediators besides the core constructs of the Protection Motivation Model (PMT). This article uses empirical data and structural equation modeling to test the antecedents and mediators of employees' cybersecurity motivational behavior. The study offers theoretical and pragmatic guidance for cybersecurity programs. First, the model developed in this study can partially explain how people may change their cybersecurity protection behavior about security threats and coping actions. Secondly, the result of the study indicates that security coping factors are reliable predictors in projecting individual intention to take protective measures. Third, organizational effort in combatting cyber threats and increasing employee awareness is significantly associated with the use of cyber threat coping processes. Additionally, several practical prescriptions are suggested based on gender, generations, and types of organizations. For example, government organizations have taken well-designed cybersecurity measures and developed detailed protocols to enhance employees' motivational behavior. Finally, future cybersecurity training materials should adapt to the unique traits of different generations, especially the Gen Edge group and digital natives for all cybersecurity subjects.

1. Introduction

In a digital era, technologies, such as computer systems, the Internet, and smart devices, play a fundamental role in everyday life across societies. While we enjoy the convenience and efficiency of the new technologies, we face new risks and threats caused by using technology. In recent years, businesses in all industries and of all sizes have experienced the increased frequency, volume, and sophistication of cyberattacks (Lu & Xu, 2018). For example, on May 7, 2021, an American oil supply system, Colonial Pipeline, suffered a ransomware cyberattack that impacted computerized equipment managing the pipeline. In response, Colonial Pipeline Company halted all of the pipeline's operations and then paid the requested ransom of nearly $5 million to restore its network (McMillan et al., 2021). According to Global Risks Report 2016, cybercrime costed 100 billion dollars in the U.S. in 2014 (Bay Dynamics, 2016). Since information security management is a necessity for all organizations (Haqaf & Koyuncu, 2018; Li et al., 2014, 2019; Liu et al., 2020; Safi et al., 2021), managers of all industries have considered company's cybersecurity a top priority in their risk management agenda (Grauer, 2016; IBM Security, 2020). Gartner Inc. estimated that the worldwide spending on cybersecurity would reach $170 billion by 2020 (Morgan, 2015). Much of this resource will be spent on training employees who are an essential line of defense. Therefore, it is critical to motivate employees to enhance their cybersecurity compliance behavior.

A critical measure in preventing cyber threats is to find effective and feasible ways to encourage employees and end-users of various technologies to effectively protect their individual and organizational information assets. Different research models and theoretical frameworks have been applied to promote security compliance (Xu et al., 2021). For example, Boss et al. (2015) have outlined several models ranging from general deterrence theory (Herath & Rao, 2009b; Hu et al., 2012), the Health Belief Model (Ng et al., 2009), rational choice theory (Bulgurcu et al., 2010; Hu et al., 2011), to the protection motivation theory (Crossler et al., 2014; Sun et al., 2020) that have been applied to analyze cybersecurity behavior. Among them, the Protection Motivation Theory (PMT) has been found to be a very relevant theoretical model in predicting individual intention to take information security actions (Yoo

[*] Corresponding author.
E-mail addresses: lli@odu.edu (L. Li), lxu@odu.edu (L. Xu), whe@odu.edu (W. He).

https://doi.org/10.1016/j.chbr.2021.100165
Received 26 July 2021; Received in revised form 13 October 2021; Accepted 23 December 2021
Available online 28 December 2021

et al., 2021). Previous studies (Wall & Warkentin, 2019; Wu, 2020) have applied some components of PMT to examine how employees' security threat perception may impact an individual's intention to practice safe behavior, but only a few of these studies have presented a comprehensive view on the actual security protection action influenced by the PMT theory (Boss et al., 2015).

In responding to the malicious attacks of the information breach and Internet hacking, information security professionals and researchers are developing measures to help understand the effect of security threats on individual employee's behavior (D'Arcy et al., 2014; Herath and Rao, 2009a; Hu et al., 2012; Posey et al., 2015; Wu, 2020). While the results of these studies have provided useful insights, they (Anderson et al., 2016; Ho et al., 2016; Menard et al., 2017; Wu, 2020) tend to place emphasis on individual's intention and are not sufficient to provide sound advice for organizations to understand the effects of environmental or organizational security awareness on the behavior of their employees. The need for theoretical and pragmatic guidance in the design and implementation of cybersecurity programs is urgent. Organizations must continually seek better direction to develop effective cybersecurity programs to combat the dangerous behaviors associated with employees' motivation toward cybersecurity action. Although much research has been done to test some of the constructs of the PMT model with regards to the threat appraisal and coping appraisal, an overarching integrated model is still lacking. Boss et al. (2015) suggested that researchers should make an effort to examine the variables in the PMT model.

The purpose of this paper is to identify opportunities for potential theoretical and practical improvements in the area of employees' awareness of cybersecurity and motivational behavior using the protection motivation theory. The research objective is (1) to investigate the comprehensive impact of threat and coping assessments as mediating factors of the PMT model on employee's cybersecurity protection action; (2) to explore the role of organizational information security practices as an antecedent on the behavior of their employees; and (3) to study the effects of demographic factors, such as gender and generations, on employee's cybersecurity behavior.

This paper contributes to the growing body of literature on the employee behavior towards IS security in the following ways: (1) it contributes to the literature through developing and testing an overarching protection motivation theoretical model that uses organization cybersecurity effort as antecedent and threat appraisal and coping appraisal as mediators in the information security area; (2) it not only identifies and proposes theoretically and empirically addressable research questions but also provides improved model-fit statistics when compared to models that did not include the complete set of PMT's core constructs; (3) it identifies unique cybersecurity behavior of various generations, such as Baby Boomer, Generation X, Millennial, and Gen Edge. To our knowledge, the previous studies have not looked into the unique cybersecurity behaviors related to generations, though studies on age groups have been conducted; (4) it integrates organizational efforts to the employee's cybersecurity awareness and motivational behavior, not just intentions; (5) it suggests that previous inconclusive findings on the information security behavior between male and female employees are due to the aggregated information; when the data are broken down to detailed analysis, behavioral differences emerge; and (6) the correlation between the awareness of existing cybersecurity policy and employee's cybersecurity protection actions is discussed.

In the next section, research findings related to cybersecurity threats and the PMT model are examined. We then present an extended theoretical framework of the Protection Motivation Model suggested by Rogers (1975, 1983) in a cybersecurity environment. Our extended theoretical framework appears to offer a more relevant explanation of how organizational cybersecurity practices can enhance their employees' cybersecurity actions.

2. Background and literature

2.1. Cybersecurity threats

Cyber threats are getting more sophisticated and intense amid the increasing levels of remote work, virtual conferencing, and dependence on digital devices. Web applications and cloud computing vulnerabilities are ranked at the top of cybersecurity threats. The global market for web applications and cloud computing is estimated to grow 17% to reach the cost of $266 billion in 2020 (Gartner, 2019). As the pandemic lasted, the economy also witnessed a 50% increase in cloud use across all industries. The five leading cybersecurity threats identified are (i) social engineering and phishing attempts, (ii) ransomware, (iii) DDoS attacks, (iv) third-party software, and (v) cloud computing vulnerabilities (Gurinaviciute, 2021).

In a world connected by information highways, no organization is immune from cyberattacks and data breaches. A cybersecurity threat is the threat of a malicious attack by an individual or organization attempting to access a network to corrupt data or steal confidential information. Some cyberattacks can even destroy computer systems or paralyze the supply chain operation, such as a recent incident that happened to Colonial Pipeline, which disrupted gasoline delivery across parts of the southeastern U.S. (McMillan et al., 2021). As cyber threats become increasingly sophisticated, organizations should enhance their employees' awareness of damages caused by cyberattacks and provide training to improve employees' security protection efficacy to safeguard their data and information networks.

The cybersecurity threat posed by vulnerable web applications has been ranked as the most severe by IT professionals. Thus, it is essential for enterprises to develop cybersecurity awareness and training programs, such as cybersecurity-related policy enforcement procedures (Chen & He, 2013; Sen & Borle, 2015; Wu, 2020), mandated training (D'Arcy et al., 2009), and security communication and computer monitoring (D'Arcy et al., 2014) to improve employee's cybersecurity behavior.

Although technology-related factors are essential, behavioral factors are vital contributing factors to cybersecurity protection because humans develop, manage, and use the technology. Siponen and Vance (2010) noted that most users do not fully comply with cybersecurity policies. In recent years, incidents of insider threats such as intentional and unintentional leaking and theft of valuable data have been reported. According to the Cost of Data Breach Report (IBM Security, 2020), about thirty-six percent of substantial cybersecurity breaches are caused by insiders or employees' compliance failures, remote work, and security skill shortages.

2.2. Protection motivation theory

The current version of the Protection Motivation Theory model (PMT) is rooted in the earlier work of Rogers (1975). The PMT model provides a clear prescription for developing messages that can influence adaptive behavior to threats. Our discussion is based on published literature on the PMT model (Floyd et al., 2000; Roger, 1983; Yoo et al., 2021).

The core components of the PMT model are the threat appraisal and coping appraisal processes that shape motivational behavior. The basic idea of the PMT is that a threat triggers the threat-appraisal process (Floyd et al., 2000); in our case, it is a cybersecurity threat. The PMT model suggests five core constructs that influence individuals who intend to protect themselves: (1) The perceived dangerousness of cyber-attack incident (e.g., having one's computer infected by a virus as a result of opening a suspicious email attachment); (2) the perceived likelihood of being vulnerable to malicious assault (e.g., vulnerable to being attacked by a phishing email); (3) the perceived response efficacy (e.g., carry out recommended preventive procedures); (4) The perceived self-efficacy (e.g., an employee's belief in her ability to perform the prescribed procedures successfully), and (5) the response costs (e.g., complying with the information security policies to keep security breaches down).

The threat appraisal and coping appraisal processes mediate the instigation, sustenance, and guidance of protective behavior (Floyd et al., 2000). The appraisal of the threat and different coping responses lead to motivational behavior to perform adaptive responses. Maladaptive responses include behaviors that are considered negative, such as opening up an unknown attachment and ignoring training, which will lead to negative consequences.

The Protection Motivation Theory is a well-accepted theoretical model for examining and analyzing the behaviors or actions recommended to negate the harm related to threats. PMT has been validated in research conducted in healthcare (Milne et al., 2000), psychology (Floyd et al., 2000), information technology (Sun et al., 2020; Wall & Warkentin, 2019), and other disciplines. In the application domain of computer and information security, PMT is naturally suited for information security contexts in which employees and end-users require additional motivation to protect their information assets. Several information security studies that use PMT as the primary theoretical model have been published recently (Anderson & Agarwal, 2010; Boss et al., 2015; Sun et al., 2020; Wu, 2020). For example, by integrating PMT, the Theory of Reasoned Action (TRA), and the Cognitive Evaluation Theory (CET), Siponen et al. (2009) develop a model to explore the factors that impact employees' intentions to comply with information security policies. Based on the PMT concept, Johnston and Warkentin (2010) proposed a Fear Appeals Model (FAM) to estimate the degree that fear appeals can influence an end user's compliance. They concluded that end users' behavioral intentions to adopt prescribed security policies are affected by fear appeals.

Boss et al. (2015) reviewed 28 publications that had applied the PMT model in the area of cybersecurity; they found out that 19 out of 28 studies have missed some of the core constructs of the PMT model (for example, perceived severity, perceived vulnerability, perceived response efficacy, perceived self-efficacy, and response costs). In addition, none of them examined the actual cybersecurity behaviors. However, some recent studies have tried to study actual cybersecurity behavior using experiments. For example, Van Bavel et al. (2019) designed a mock purchasing process to test the level of security of participants' online behavior. Another study was conducted by Jansen and Van Schaik (2019). They examined the impact of fear appeal messages on user cognitions, attitudes, behavioral attentions, and precautionary behavior regarding online information-sharing to protect against the threat of phishing attacks. This development calls for an extension to the PMT model to reflect the unique behavior when applied to the information security setting and provide theoretical justification for using the model. In this study, we will address this issue using empirical data.

2.3. From motivation to action: extending Protection Motivation Model in cybersecurity study

In this study, we extend the PMT model by mediating organizational effort and actual employee cybersecurity behavior with the threat appraisal process and the coping appraisal process. Fig. 1 presents a theoretical model of extended perspective on cybersecurity behavior. We draw insights from Rogers' Protective Motivation Theory (Rogers, 1975; 1983) and the PMT model suggested by Floyd et al. (Floyd et al., 2000 and Boss et al., 2015). Our extended protection motivation conceptual framework includes three parts. First, we consider the organizational effort to fight cybersecurity crime as an antecedent of threat and coping appraisals. The rationale to include organizational effort is that many organizations have increased reliance on information systems for processing and storing information (Wu, 2020) and commutating with their suppliers and customers. Secondly, adopted from Rogers' model (Roger 1983), we consider two cognitive mediating processes: the threat-appraisal process and the coping-appraisal process. And finally, the employee's protective behavior, the construct on the right-hand side of Fig. 1, is the dependent variable of the cognitive mediating process that includes threat and coping appraisal attributes. We included that employees' motivational behavior results from cognitive mediating processes since researchers (Boss et al., 2015) suggested that cybersecurity studies should explore the importance of employees' cybersecurity behavior rather than an intention. This study focuses on employees' self-reported cybersecurity motivational behavior. Table 1 provides a summary of the constructs, the related theoretical concepts, and relevant references.

2.4. Organizational cybersecurity practice and its effect on employee awareness

Johnston and Warkentin (2010) find that social influence such as information from organizations positively affects individuals' intentions to adopt cybersecurity programs. When an organization has cybersecurity procedures or policies in place, its employees are provided with information security training and cybersecurity tips. According to published literature (Herath & Rao, 2009b; Posey et al., 2015), extrinsic motivators, such as social influence, peers, and descriptive norms, enrich employees' experience and positively impact employees' cybersecurity behavior. Previous studies (D'Arcy et al., 2014; Herath & Rao, 2009b; Venkatesh et al., 2003) in the cybersecurity framework indicate that employees are motivated to behave the same way their peers do. It is commonly accepted that "cybersecurity awareness refers to

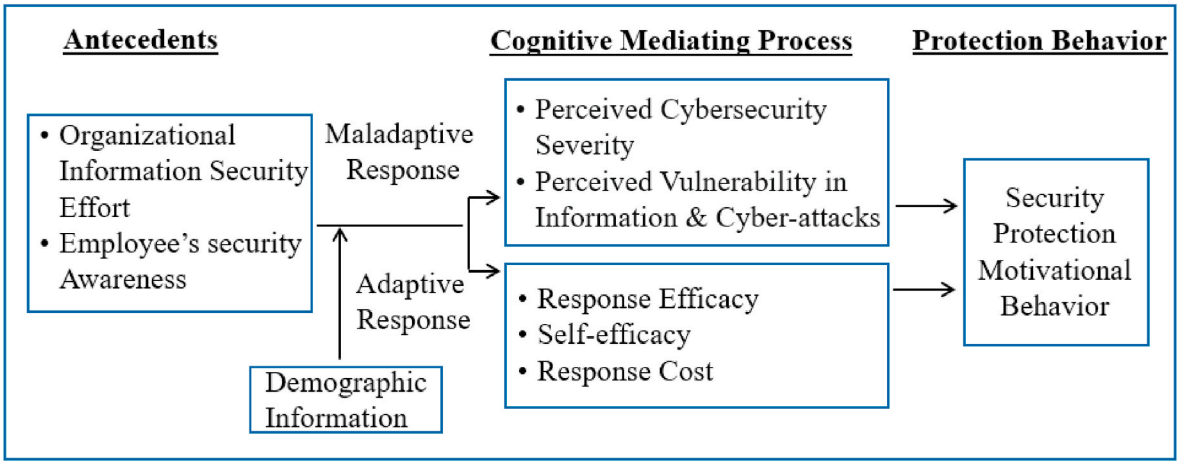

Antecedents
Cognitive Mediating Process
Protection Behavior
• Organizational Information Security Effort
• Employee's security Awareness
Maladaptive Response
Adaptive Response
Demographic Information
• Perceived Cybersecurity Severity
• Perceived Vulnerability in Information & Cyber-attacks
• Response Efficacy
• Self-efficacy
• Response Cost
Security Protection Motivational Behavior

Fig. 1. Extended PMT model for antecedents and mediating factors on cybersecurity actions.

Table 1
Constructs in the model.

Constructs	Theory	References
Organizational information security effort	OE	Herath & Rao, 2009a; Ali et al., 2021
Employee cybersecurity awareness	TPB	Ajzen (2011); Herath & Rao, 2009a; IBM Security, 2020; Ali et al., 2021
Perceived severity	Protection Motivation Theory (PMT)	Boss et al., 2015; Floyd et al., 2000; Herath & Rao, 2009a; Rogers, 1983; Wall & Warkentin, 2019; Wu, 2020; Yoo et al., 2021; Ali et al., 2021
Perceived vulnerability	PMT	Boss et al., 2015; Herath and Rao, 2009b; Lee & Larsen, 2009; Ng et al., 2007; Wall & Warkentin, 2019; Wu, 2020; Yoo et al., 2021; Ali et al., 2021
Response efficacy	PMT	Boss et al., 2015; Crossler & Bélanger, 2014; Lee & Larsen, 2009; Wall & Warkentin, 2019; Wu, 2020; Yoo et al., 2021; Ali et al., 2021
Self-efficacy	PMT	Boss et al., 2015; Crossler & Bélanger, 2014; Herath & Rao, 2009a; Lee & Larsen, 2009; Wall & Warkentin, 2019; Wu, 2020; Yoo et al., 2021; Ali et al., 2021
Response costs	PMT	Boss et al., 2015; Crossler & Bélanger, 2014; Herath & Rao, 2009a; Menard et al., 2017; Ali et al., 2021
Cybersecurity behavior	TPB, PMT	Boss et al., 2015; Floyd et al., 2000; Wall & Warkentin, 2019; IBM Security, 2020

employees' understanding of the nature of cybersecurity threats, how threats can jeopardize organizational security, and what employees should do if they encounter a threat" (Minecast, 2021). The PMT model explicitly suggests that an employee's security awareness is a primary factor for threat appraisal and coping processes (Vance et al., 2013). Therefore, organization effort in enhancing employee's cybersecurity awareness can help employee's subsequent security behavior.

Several authors have explored the effects of security awareness programs conducted by organizations. However, the results are inconclusive. After they tested a theoretical model of the incentive effects of penalties, pressures, and perceived effectiveness of employee actions (Herath & Rao, 2009a), Herath and Rao found that employees' cybersecurity behaviors are influenced by intrinsic and extrinsic motivators. On the contrary, Ng and Xu (2007) found that higher levels of cue to action do not necessarily improve employees' cybersecurity behavior. In recent years, especially after the Snowden incident, specific employee cybersecurity behaviors have been identified. Many organizations are implementing cybersecurity procedures such as providing training, distributing security newsletters, and sending alert messages to employees to fight against cyber hacking and other information leaks. We suspect that the development in cybersecurity practices has enhanced employees' awareness of security protection. We propose the following Hypothesis.

Hypothesis 1. Organizations' cybersecurity efforts are positively related to their employees' cybersecurity awareness.

2.5. The mediating process - cybersecurity threat appraisal and coping appraisal

The PMT model consists of two mediating processes: the threat-appraisal process and the coping-appraisal process. These two processes are mapped to the cognitive processes that people apply to evaluate threats and select coping alternatives. In addition, a threat assessment process evaluates the maladaptive behaviors, which have two constructs – severity and vulnerability (Boss et al., 2015; Roger, 1983). Severity is the degree to which an employee believes that a cybersecurity threat, such as a computer virus, unauthorized access to a computer, or Internet hacking, will cause consequential harm. Perceived severity refers to the extent to which individuals perceive the magnitude of a threat and the potential impact of a threat (Ng & Xu, 2007; Vance et al., 2012). Accordingly, we argue that employees' awareness of cybersecurity helps them better understand the severity of cyber threats than those who do not have a similar experience (Ajzen, 2011; Ali et al., 2021; Herath & Rao, 2009a). Thus, we study the following Hypothesis.

Hypothesis 2a. Employees' cybersecurity awareness is positively related to their perceived severity of cybersecurity incidents.

Vulnerability means the degree to which an employee believes that cyber threat applies to his or her specific circumstances (Boss et al., 2015). Vulnerability is the probability that an unwanted incident will happen in the absence of preventive action (Vance et al., 2012). If employees previously suffered from cybersecurity breaches or data loss due to cyber hacking, they tend to take specific actions to prevent cyber-attack. This discussion leads us to formulate the following Hypothesis:

Hypothesis 2b. Employees' cybersecurity awareness is positively related to their perceived vulnerability caused by cybersecurity incidents.

A coping appraisal process is about how individuals evaluate their abilities to manage the potential loss or damage arising from a threat (Woon et al., 2005). In our case, it is a cybersecurity threat. A coping appraisal is a measure that comprises three constructs: response efficacy, self-efficacy, and response cost of performing the adaptive actions (Rogers, 1983). *Response efficacy* is a belief that the adaptive response will work if one takes a protective measure to protect the company (Anderson et al., 2010). For example, an employee believes that his compliance with the company's information security policies would reduce security breaches.

On the other hand, *self-efficacy* is the degree to which an individual believes that he can cope with threats, such as having confidence in removing spyware from his electronic devices and treating virus-infected files (Ng & Xu, 2007; Sun et al., 2020). We argue that individuals' self-efficacy comes from their motivation and awareness. The more experience and higher motivation they have, the more confident they will carry out coping response tasks. From this argument, we offer these hypotheses:

Hypothesis 2c. Employees' cybersecurity awareness is positively related to their response efficacy when they handle cybersecurity incidents.

Hypothesis 2d. Employees' cybersecurity awareness is positively related to their self-efficacy when they handle cybersecurity incidents.

Finally, *response costs* are any perceived direct personal costs, such as effort, inconvenience, or money incurred when an employee takes protective steps. Response costs usually include individuals' perceived cost and inconvenience of practicing cybersecurity compliance. In our study, the response cost can be backing up a computer regularly or changing the password frequently. An individual's response cost is associated with his cybersecurity awareness. The more security experience an employee has, the less often response costs will occur because he is capable of practicing cybersecurity tasks. Thus, we expect:

Hypothesis 2e. Employees' cybersecurity awareness negatively affects their response costs.

The output of the appraisal-mediating processes is an effective driver for behavioral decisions. Thus, one of the dependent variables of a PMT model is the measure of behavioral intentions or positive behavior. The purpose of PMT applied to information security research is usually to persuade people to develop protective cybersecurity behavior. This leads to our discussion on employee cybersecurity protection behavior in the next section.

2.6. Cybersecurity motivational behavior

Protective Motivation Theory offers adequate explanatory power and is considered by researchers to be one of the valuable guidelines to estimate an individual's commitment to engaging in risk protective actions (Anderson et al., 2016; Floyd, 2000; Yoo, 2021). While most prior cybersecurity studies choose behavioral intention or likelihood of behavior as their dependent variables, we attempt to measure employees' practice in cyber risk management programs to explore the predictive power of employees' perceived severity, perceived vulnerability, response efficacy, self-efficacy, and responsive costs on their cybersecurity protection behaviors. Ajzen (2011) articulated the theory of planned behavior (TPB) that connects beliefs to behavior. He suggested that perceived behavioral control leads to actions. TPB has been applied to a few information security studies regarding behavioral relations among attitudes, motivation, intentions, and behavioral outcomes.

Published research has provided some insights on using compliance behavior as a dependent variable. Herath and Rao (2009b) find that employees' security concerns are significantly impacted by the perceived severity of cyber-attack. D'Arcy et al. (2009, 2014), on the other hand, noted that information system misuse could effectively be reduced by employees' perceived severity of sanctions. Ng and Xu (2007) suggested that individuals with higher levels of perceived severity do not exhibit more significant levels of risk agility. Based on these diverse findings, we intend to test the effects of perceived severity on cybersecurity protection behavior and propose the following Hypothesis:

Hypothesis 3a. Stronger perceived severity toward cybersecurity leads to more assertive motivational behavior to comply with the security policies.

Vance et al. (2012) find that employees' perceived vulnerability does not positively affect their intention to comply with cybersecurity policies. However, Siponen et al. (2014) find that employees' perceived vulnerability significantly and positively impacts their intent to abide by the organization's risk management policies. In order to provide a consistent result to this issue, we intend to test the effects of perceived vulnerability on cybersecurity protection behavior and propose the following Hypothesis:

Hypothesis 3b. Stronger perceived vulnerability toward cybersecurity leads to more assertive motivational behavior to comply with the security policies.

Literature shows that employees' response efficacy significantly affects their attitudes towards cybersecurity policies (Herath & Rao, 2009b). Moreover, Johnston and Warkentin (2010) find that employees' response efficacy positively affects their intentions to adopt cybersecurity actions. However, some authors find that employees' response efficacy does not positively affect their choice to comply with cyber risk management guidelines (Siponen et al., 2014; Vance et al., 2012). Based on the inconsistent findings, we propose:

Hypothesis 3c. Stronger response efficacy toward cybersecurity leads to more assertive motivational behavior to comply with the security policies.

In terms of self-efficacy, the findings from the previous studies report a consistent result. Employees' self-efficacy positively impacts their intention to comply with cybersecurity policies. Therefore, employees' self-efficacy is a strong predictor of cybersecurity protection action (Herath & Rao, 2009b; Johnston & Warkentin, 2010; Ng & Xu, 2007; Siponen et al., 2014; Vance et al., 2012). Thus, we expect:

Hypothesis 3d. Stronger self-efficacy toward cybersecurity leads to more assertive motivational behavior to comply with the security policies.

There is a negative relationship between response cost and security protection behavior. The higher the perceived response costs, the less likely employees exhibit a greater level of cybersecurity protection behavior (Ng & Xu, 2007). To validate this finding, we propose:

Hypothesis 3e. Stronger perceived response costs toward cybersecurity negatively affects motivational behavior to comply with the security policies.

2.7. Effects of demographic factors

Gender Difference. We also intend to explore the moderating effect of gender. Previous research has found that males and females act differently when dealing with technologies, and women represent a distinct voice in business ethics as gendered phenomena (Grosser et al., 2017). Women tend to recognize unethical actions better and behave more ethically when coping with IT-related wrongdoings (Cronan et al., 2005). In addition, women are more likely to report cybersecurity infractions than males (Mesmer-Magnus et al., 2005; Stylianou et al., 2013).

However, the previous findings of the role of gender in cybersecurity management are inconclusive. Some scholars find that gender affects decision-making processes regarding the issues related to information systems (Adam & Ofori-Amanfo, 2000; Kreie & Cronan, 1998; Peslak, 2008); some scholars find that gender does not impact individuals' intentions to violate cybersecurity policies (Barlow et al., 2013; Hovav & D'Arcy, 2012; Siponen & Vance, 2010; Vance et al., 2012); and some scholars find that females had significantly higher security compliance intentions. Because the published literature provides inconclusive results, we take a step further to provide in-depth analysis and expect gender differences exist in our data. The following Hypothesis will be tested.

Hypothesis 4a. Women have a higher level of awareness of cybersecurity severity than men when encountering cybersecurity issues.

Type of Organization. Businesses and government organizations have different organizational goals and business values. The former aims to increase revenue or earn more profit by providing goods and services to satisfy customer needs and stakeholders' expectations, whereas the latter aims to maintain domestic tranquility, achieve sustainable development, and promote general welfare and economic growth (Kim et al., 2014). For example, millions of US federal workers worked from their homes because of the Coronavirus pandemic. This expansive telecommuting activity has increased the potential of sensitive government projects and information being exposed to unauthorized individuals. Therefore, the government agencies require federal employees only use agency-approved video conferencing, collaboration tools and methods to share files, only use laptops and smartphones owned, managed and protected by the government agency that the employee works for, store work-related content on Government Furnished Equipment (GFE) and agency-approved cloud services (Federal Mobility Group, 2020). On the other hand, employees of a business organization, though also need to comply with the company's cybersecurity guideline, can use their own electric devices when they work from home and print documents at home if they needed. Due to the different goals, business firms and government organizations provide fundamentally different environments regarding cybersecurity. Therefore, we expect that differences exist in different types of organizations and will test the following Hypothesis.

Hypothesis 4b. Employees of a government agency have a higher level of awareness of cybersecurity severity than employees in a business firm when encountering cybersecurity issues.

Generation Groups. A few studies on information security tested the difference among age groups (Johnston & Warkentin, 2010; Knight & Pearson, 2005). Knight and Pearson (2005) observed little difference among the various age groups regarding computer behavior in the workplace. In their study on e-commerce, Van Bavel et al. (2019) showed that older adults are more vulnerable than younger adults to certain types of the phishing attack. The younger people, especially Gen Edges born after 1996, are less sensitive to cyber-attacks because they were born in an information era and are more experienced internet users than Baby Boomers, Generation X, and Millennials. Considering the inconclusiveness of the age spectrum on the findings of cybersecurity behavior, we have divided respondents into generation groups instead of age groups. We intend to explore the cybersecurity behavior traits of Baby Boomers, Generation X, Millennials, and Gen Edges. We expect generation difference exists in their response to cybersecurity motivational behavior. Therefore, we will test the following Hypothesis using the ANOVA procedure.

Hypothesis 4c. People in the Gen Edge group have a lower level of sensitivity toward cybersecurity severity than people in the groups of Baby Boomer, Generation X, and Millennials when encountering cybersecurity issues.

3. Research method

3.1. Data

A research instrument that focuses on work-related computer use was sent to 800 employees in various organizations in a major city located on the east coast of the US. The survey was distributed via local business groups through the Internet in 2017. An initial invitation was sent to business and government organizations in a large metropolitan area in the Eastern US. One response was collected from each company. The participants had administrative roles such as manager, director, vice president, or president. Three hundred eighty-seven (387) employees responded to the study, resulting in a 48.37% response rate. The demographic information of the respondents is presented in Table 2. Sixty-one percent of the respondents are female, and 39% are male. About 20% of the respondents are in the group of Gen Edge. The vast majority of the participants (about 83%) have a college education. A little over 46% of the participants work for companies that have more than 500 employees.

The survey consisted of 32 items, including seven demographic questions (See Appendix A). The items for this survey were selected and designed to measure eight different theoretical constructs (see Table 3). Participants responded to each question by choosing a 7-point Likert scale ranging from Strongly Disagree to Strongly Agree. After completing the survey items, participants completed a demographic questionnaire.

3.2. Analysis

3.2.1. Measurement model, construct reliability and validity

The survey was designed to measure eight latent constructs related to the hypotheses proposed above. Therefore, we began our analyses by investigating the construct reliability and validity of the measurement model of the survey items.

Content validity. Generally speaking, content validity refers to whether a research instrument appropriately applies the theoretical constructs to the target domain of the research theme. In this case, content validity was established through discussions with employees from various industries, including retailing, financial services, healthcare, telecommunication, military, information technology, government, etc. to learn the behavioral components related to cybersecurity cues to action, threat appraisal process, coping appraisal process, and employee cybersecurity behavior. In addition, an extensive literature review on each construct specified in the conceptual model (Fig. 1 and Table 1) and recent media reports on cybersecurity (Bay Dynamics, 2016; Infographic, 2016; McMillan et al., 2021) have helped define the scope of the study and objectively test the research instrument.

Table 2
Demographic information.

Gender	Frequency (N = 387)	Percent (%)
Male	149	38.50
Female	238	61.50
Age		
Gen Edge	75	19.38
Millennial	235	60.72
Generation X	47	12.14
Baby Boomer	30	7.75
Education background		
High school	65	16.80
undergraduate	271	70.03
graduate	51	13.18
Job function area		
Accounting	18	4.65
Administration	63	16.28
Information Technology	65	16.80
Instructions/Teaching	62	16.02
R&D	17	4.39
Operations	46	11.89
Marketing and Sales	86	22.22
Others	30	7.75
Organization category		
Government	35	9.04
Education	129	33.33
Finance/Banking/Insurance	11	2.84
Information Technology	30	7.75
Retail/wholesale	58	14.99
Real estate	34	8.79
Telecommunications	6	1.55
Healthcare/Medical	39	10.08
Military	17	4.39
Others	28	7.24
Organization size		
1–50	118	30.49
51–500	93	24.03
>501	176	45.48
Annual revenue		
Less than $1 million	61	15.76
>$1 million-$100 million	64	16.54
>$100 million and more	44	11.37
I don't know	218	56.33

Construct reliability. Cronbach's Alpha was used to assess the internal consistency of the items for each construct (Table 3). The threat appraisal process was measured using two constructs as suggested in Rogers' Protection Motivation Theory (Rogers, 1983): perceived severity and perceived vulnerability with the reliability of 0.83 and 0.84, respectively. The coping process has three constructs: response efficacy, self-efficacy, and response costs. Reliabilities for these three constructs are 0.82, 0.87, and 0.73, respectively. Finally, reliabilities for organizational effort, action experience, and security protection action are 0.81, 0.78, and 0.72, respectively (Table 3). As such, Cronbach alpha values have all exceeded the suggested threshold of 0.60. This result presents evidence of effective measurement of security protection constructs.

Next, we tested the construct reliability of our constructs by conducting a Confirmatory Factor Analysis (CFA). This measurement model was supported by a number of statistical fit indices as shown in Table 3: Chi-square/df = 1.95, RMSEA = 0.05, CFI = 0.95, GFI = 0.90, and IFI = 0.95. The fit indices from our measurement model meet the commonly acceptable statistical fit indices of 0.90. In addition, each of the standardized loadings (indicated under the column of "Loading" in Table 3) for the model paths was highly significant. In summary, each of the proposed constructs that we intended to measure in our survey revealed evidence of good internal consistency and measurement model

Table 3
Confirmatory factor analysis.

Indicator	Loading (Standardized Regression Weights)	S.E.	R^2	Total variance explained (%)	Cronbach α	AVE (Average Variance Extracted)
Organization Effort (OE)				72.88	0.81	0.61
OE1	0.78***	0.09	0.61			
OE2	0.91***	0.08	0.82			
OE3	0.63***	0.09	0.40			
Action Experience(AE)				70.05	0.78	0.57
AE1	0.62***	0.10	0.38			
AE2	0.72***	0.08	0.51			
AE3	0.91***	0.09	0.82			
Perceived Severity(PS)				74.86	0.83	0.64
PS1	0.66***	0.11	0.44			
PS2	0.76***	0.09	0.58			
PS3	0.96***	0.09	0.91			
Perceived Vulnerability(PV)				67.14	0.84	0.56
PV1	0.76***	0.08	0.58			
PV2	0.76***	0.08	0.58			
PV3	0.70***	0.06	0.49			
PV4	0.78***	0.07	0.61			
Response Efficacy(RE)				73.75	0.82	0.61
RE1	0.82***	0.06	0.68			
RE2	0.84***	0.05	0.70			
RE3	0.68***	0.05	0.46			
Self-efficacy(SE)				79.05	0.87	0.70
SE1	0.72***	0.08	0.52			
SE2	0.85***	0.09	0.73			
SE3	0.92***	0.08	0.85			
Response Cost (RC)				64.71	0.73	0.47
RC1	0.66***	0.10	0.43			
RC2	0.74***	0.10	0.55			
RC3	0.66***	0.10	0.44			
Security Protection Action (SPA)				64.59	0.72	0.48
SPA1	0.71***	0.08	0.50			
SPA2	0.59***	0.06	0.35			
SPA3	0.76***	0.08	0.58			

Note: *** significant at 0.001; $\chi2 = 482$, $\chi2/DF = 1.95$, CFI = 0.95, GFI = 0.90, IFI = 0.95, RMESA = 0.05.

fit, suggesting that our data provide acceptable levels of measurement reliability (Hair et al., 2006).

The explained variance for the security protection action is 0.72, meaning that 72% of the variance is captured by the cognitive mediating process that includes perceived cybersecurity severity, perceived vulnerability, response efficacy, self-efficacy, and response cots.

Convergent validity. The convergent validity method applies several items for one scale, and each item in the same scale is viewed as a different approach to assess the same construct. Anderson and Gerbing (1988) suggest that convergent validity can be measured using *t*-tests for the factor loadings. If all factor loadings for the same construct are statistically significant, then this suggests acceptable convergent validity of the items on a scale. The results of CFA in Table 3 confirm that all paths between observed variables and the first-order latent variables are at the significant level of $p < 0.001$. For example, three items loaded to the construct "perceived severity" under the column with the heading "Loading" in Table 3 are statistically significant at $p < 0.001$, indicating all items are effectively assessing perceived severity. Another way to assess the convergent validity of items on a scale is by examining the magnitude of the factor loadings. Table 3 shows the factor loadings of each item on the proposed scale exceed 0.50. The results indicate that the measurements in our model have good convergent validity. Finally, in this eight-factor CFA model, the total variance explained by each construct is in the range of 47%–70% (Table 3). Hence, we claim that the convergent validity of our model is satisfactory.

Discriminant validity. Discriminant validity refers to whether different scales in a model actually measure different constructs. If two scales are both measuring the same or highly similar constructs, then this could be the cause of strong correlations between factors in a model. The discriminant validity of the eight constructs was assessed by computing the correlations between validated constructs (Table 4). Correlations between all pairs of constructs are below the recommended threshold value of 0.90 (Hair et al., 2006). Furthermore, the average variance extracted (AVE) from all the constructs (Table 3) exceeds the threshold of 0.5 except response costs (RC) and cybersecurity protection action (SPA) with AVE values that are very close to 0.5. This result indicates that discriminant validity is acceptable, and correlations between the measures of constructs are not strong enough to suggest that the different scales are multiple measurements of the same construct.

3.3. *Structural equation model testing*

Structural Equation Modeling (SEM) was used to test our proposed theoretical model of the mediating role of PMT cognitive factors in the relationship between organizational efforts and employee protection actions. SEM follows a two-step approach that includes constructing the measurement model and testing the structural model (Anderson & Gerbing, 1988). Specifically, we have tested our proposed Extended Protection Motivation Model and assessed the overall fit using the maximum likelihood method in AMOS. The test of the structural model includes estimating the path coefficients, which indicate the strength of the relationships between the independent and dependent variables, and the R^2 values, which are the amount of variance explained by the independent variables. The final structural equation model that includes all paths is shown in Fig. 2, and the complete set of relationships for the final model is listed in Fig. 2 and Table 5.

Fit statistics SEM. The fit indices chosen for our model represent two characteristics: (i) the global fit measures and (ii) comparative fit measures. The chi-square test (χ^2) with degrees of freedom is commonly used as the global model fit criteria. The chi-square value of our structural equation model is 610, and χ^2/df is 2.31 (Table 5), which is a very good result based on the acceptable ratio of $\chi^2/\text{df} = 2.5$ or smaller. We choose the comparative fit index (CFI), the goodness of fit index (GFI), incremental fit index (IFI), and root mean square error of approximation

Table 4
Correlation matrix of constructs.

	Mean	Std. Deviation	AE	PV	PS	RC	RE	OE	SE	SPB
Action Experience (AE)	4.79	1.55	1.00							
Perceived Vulnerability (PV)	5.03	1.29	.506**	1.00						
Perceived Severity (PS)	4.68	1.82	.145**	.276**	1.00					
Response Cost (RC)	3.60	1.48	-.121*	-.114*	0.08	1.00				
Response Efficacy (RE)	5.52	0.98	.351**	.535**	.199**	-.200**	1.00			
Organization Effort (OE)	4.01	1.61	.630**	.393**	.187**	−0.07	.314**	1.00		
Self-efficacy (SE)	4.26	1.72	.319**	.151**	−0.09	-.132**	0.08	.207**	1.00	
Security Protection Action (SPA)	5.63	1.13	.278**	.268**	0.06	-.273**	.323**	.186**	.474**	1.00

Note: N = 387; **: significant at $p < 0.01$(2-tailed); *: significant at $p < 0.05$ (2-tailed).

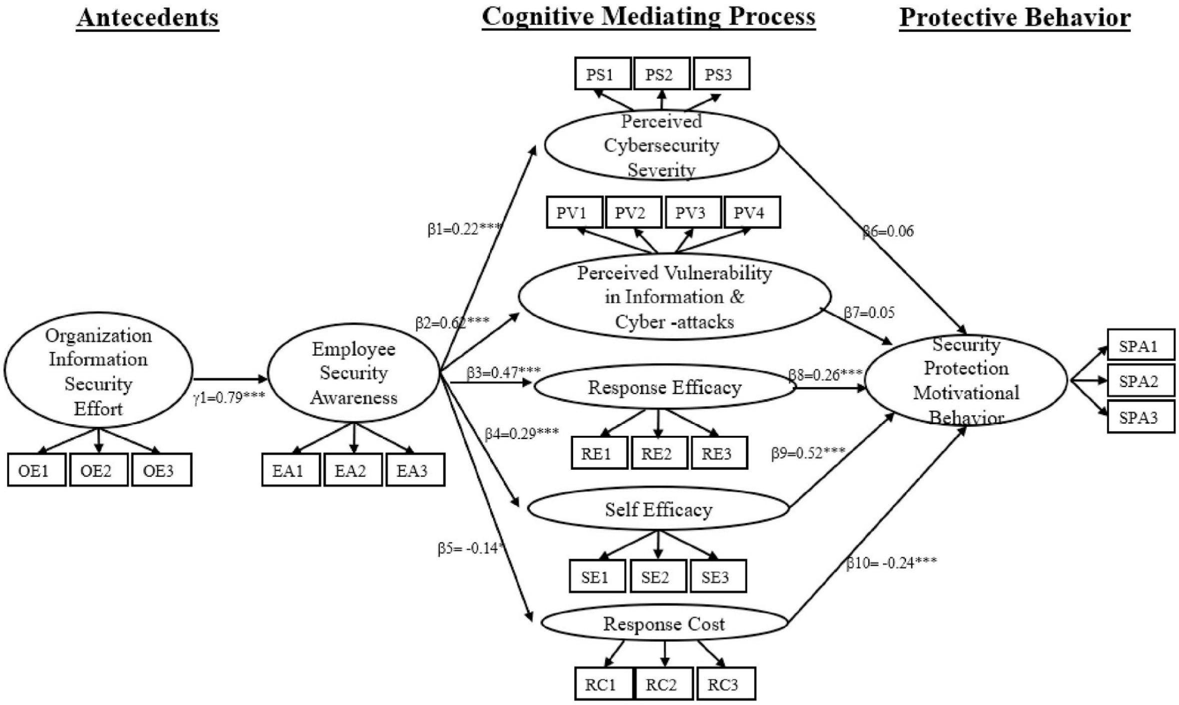


Fig. 2. Structural equation model.

Table 5
Fit statistics for measurement and structural models.

Measurement Model Goodness of Fit Statistics	Model Value
χ^2	482
df	247
χ^2/DF	1.95
Root mean square error of approximation (RMSEA)	0.05
Comparative fit index (CFI)	0.946
Goodness-of-fit index (GFI)	0.904
Incremental fit index (IFI)	0.946
Structural Model Goodness of Fit Statistics	Model Value
χ^2	610
df	264
χ^2/DF	2.31
Root mean square error of approximation (RMSEA)	0.058
Comparative fit index (CFI)	0.92
Goodness-of-fit index (GFI)	0.88
Incremental fit index (IFI)	0.92

(RMSEA) to assess the congruence between the hypothesized model and the data. The comparative fit index for our extended PMT model is CFI = 0.92, GFI = 0.88, IFI = 0.92, and RMSEA = 0.058. All the values have a satisfactory fit of 0.90, except GFI, which has a fit index of 0.88, close to the generally accepted minimum norm of 0.90. These results suggest that overall the proposed Extended Protection Motivation Model (Fig. 1) provides a good overall fit of the data. The variables and constructs represented in the model explain a considerable portion of the variance in the endogenous constructs. In the next section, findings related to hypotheses regarding the individual paths in the model will be discussed.

4. Findings related to hypotheses

The hypotheses in the extended PMT model test the relationships among organization effort, employee's experience of cybersecurity protection, the threat appraisal process (perceived severity and perceived vulnerability), the coping appraisal process (response efficacy, self-efficacy, and response costs), and an employee's cybersecurity protection actions. The results of our study have supported eleven hypotheses proposed in Section 2. Table 6 presents a summary of the hypotheses testing result for the structural model.

The first Hypothesis tests the effects of organizational effort on employees' cybersecurity awareness. We hypothesized (H1) that organizational efforts (i.e., circulating security newsletters, providing security training, and distributing security alert messages/emails) are positively related to employee awareness (i.e., security training experience and understanding their company's information security policy). The result of our study supports this hypothesis. Table 6 shows that the standardized path coefficient between organization efforts and employee action

Table 6
Summary of hypotheses testing result for the structural model.

	Paths	Standard path coefficient	p-value
H1	Organization Effort → Action Experience	$\gamma_1 = 0.79$	<0.001
H2a	Action Experience → Perceived Severity	$\beta_1 = 0.22$	<0.001
H2b	Action Experience → Perceived Vulnerability	$\beta_2 = 0.62$	<0.001
H2c	Action Experience → Response efficacy	$\beta_3 = 0.47$	<0.001
H2d	Action Experience → Self-efficacy	$\beta_4 = 0.29$	<0.001
H2e	Action Experience → Response Cost	$\beta_5 = -0.14$	<0.05
H3a	Perceived Severity → Security Protection Action	$\beta_6 = 0.06$	>0.5
H3b	Perceived Vulnerability → Security Protection Action	$\beta_7 = 0.05$	>0.5
H3c	Response Efficacy → Security Protection Action	$\beta_8 = 0.26$	<0.001
H3d	Self-efficacy → Security Protection Action	$\beta_9 = 0.52$	<0.001
H3e	Response Costs → Security Protection Action	$\beta_{10} = -0.24$	<0.001

experience is $\gamma_1 = 0.79$ with a *p*-value < 0.001.

The next set of two hypotheses (hypotheses H2a and H2b) tested the relationship between employees' cyber security awareness and the threat appraisal process, including perceived severity and perceived vulnerability. We hypothesized (H2a) that Employees' awareness positively related to their perceived severity of cybersecurity incidents. Table 6 shows that the standardized path coefficient for H2a is $\beta_1 = 0.22$ with a *p*-value < 0.001. Therefore, H2a is supported. Hypothesis H2b, "Employee's awareness is positively associated with their perceived vulnerability caused by cybersecurity incidents," is supported by $\beta_2 = 0.62$ and a *p*-value <0.001. The results indicate that cybersecurity awareness training for employees helps address one of the biggest factors in major security breaches: the role humans play in preventing cyber-attack. By training employees to recognize and respond to cyber threats, organizations can improve their security posture and cyber resilience. Furthermore, employees are better aware of the severe consequence of computer viruses, opening a suspicious email attachment, and losing data resulting from hacking.

The three hypotheses (hypotheses H2c, H2d, and H2e) test the relationship between employees' cybersecurity awareness and the coping appraisal process, including response efficacy, self-efficacy, and response cost. The results of structural equation analysis support all three hypotheses. The standardized path coefficient for H2c is $\beta_3 = 0.47$ and for H2d is $\beta_4 = 0.29$, both are with a *p*-value < 0.001. Hypotheses H2e has a negative path coefficient $\beta_5 = -0.14$, with a *p*-value < 0.05. This result is preferred and confirms the previous findings on response costs (Boss et al., 2015). The higher the employees' awareness, the less cost or inconvenience they would incur when performing cybersecurity tasks. The results also indicate that when organizations provide training, distribute security awareness newsletters, and invite experts to give talks on security protection, they provide their employees with a working knowledge of efficacy to cope with cyber intrusion.

Hypothesis 3 (H3a, H3b, H3c, H3d, and H3e) tests the relationship between mediating factors (including threat appraisal process and coping appraisal process) and employee's cybersecurity motivational behavior. The finding of our study supports hypothesis 3. The standardized coefficients of $\beta_8 = 0.26$, $\beta_9 = 0.52$ $\beta_{10} = -0.24$, all are significant at $p < 0.001$ (Fig. 2 and Table 6). The result indicates that response efficacy and self-efficacy increase are positively related to employees' cybersecurity protection behavior. Furthermore, when an employee's awareness improves, the response cost reduces (H2e), and the lower the response cost leads to better employee protection behavior (H3e). This result confirms the previous findings on response costs in the research on information security (Boss et al., 2015) and the research on the PMT model in general.

The mediating power of the cybersecurity threat appraisal process on security protection action (Hypotheses H3a and H3b) is positive but not statistically significant. Detailed discussion is provided in section 6.

5. Testing the effects of demographic factors

5.1. Gender difference - multi-group structural model comparison

While an overall perspective on our extended PMT model shows significant relationships among eight constructs, we would like to explore further the moderating impact of gender by establishing comparison groups. Hypothesis 4a is tested using this procedure.

When analyzing the differences in cybersecurity behavior based on gender, we prefer the structural model parameter comparison procedure to the ANOVA procedure because the structural model parameter comparison builds upon the measurement invariance test and then performs similar types of comparisons to assess the differences in path loadings in the structural model (a feature that ANOVA does not provide). We first test whether the metric invariance exists in the measurement model, and then analyze the differences of paths based on the comparison of the unconstrained model and the constrained model.

We divided our sample into male employees (n = 149) and female employees (n = 238) based on the responses in the survey. The results from the measurement invariance test (Table 7) show that the change in chi-square ($\Delta\chi^2$) is 37 with a change in degrees of freedom (ΔDF) of 25 between the unconstrained group model and constrained group model for males and females. This result indicates that the difference is not significant at $p \leq 0.05$, which supports the full metric invariance comparison between male and female participants. Thus, we select gender as the moderator to conduct the structural model comparison. We further analyze the difference of paths in gender based on the comparison of the unconstrained model and the constrained model to provide a clearer picture of the behavioral difference between the male and female groups when they encounter cybersecurity issues.

The results from the gender analysis show an acceptable fit, $\chi^2/df = 1.8$ (Table 8), RMSEA = 0.046, and CFI = 0.9; therefore, the overall comparison model is acceptable. The χ^2 difference between the unconstrained and constrained structural models is 15, with a change in the degree of freedom of 7, which indicates that the difference between the two models is significant.

This result suggests that gender does moderate cybersecurity behavior to a certain degree. Two path loadings, the relationship between employee awareness and perceived severity (EA→PS), and response cost and security protection action (RC→SPA) are significant at $p < 0.001$ contingent on gender (Table 8).

Further examining the standardized parameter estimates for the unconstrained model, we find that both EA→PS and RC→SPA paths are significant in the female group but not in the male group, which means that the association between employee awareness and perceived severity, and between response cost and security protection action are more substantial for female employees than for male employees. Furthermore, the effect of response efficacy on security protection behavior is stronger in the female group ($p < 0.001$) than in the male group ($p < 0.05$), though both groups show a level of significance in this pair of interactions. Therefore, Hypothesis 4a, *Women have a higher level of awareness of cybersecurity severity than men when encountering cybersecurity issues*," is, at least, partially supported by these results. Our study suggests that previous inconclusive findings on the information security behavior between male and female employees are due to the aggregated information; when the data are broken down to detailed analysis, behavioral differences emerge.

5.2. Generation groups - ANOVA and post hoc analysis

Next, we conduct the Analysis of Variance (ANOVA) procedure to investigate (i) the difference among the four generations regarding security protection actions (H4c). Our sample includes four different

Table 7a
Measurement invariance test.

Group	Unconstrained group Model (Configurable invariance)					Constrained Group Model (Metric invariance)					Model Differences	
	χ^2	Df	χ^2/Df	CFI	RMSEA	χ^2	Df	χ^2/Df	CFI	RMSEA	$\Delta\chi^2$	ΔDf
Gender	811	494	1.6	0.9	0.04	848	519	1.6	0.9	0.04	37	25

Table 7b
Measurement invariance test (partial constrained).

Group	Unconstrained group Model (Configurable invariance)			Partial Constrained Group Model (Metric invariance)			Model Differences	
	χ^2	Df	χ^2/Df	χ^2	Df	χ^2/Df	$\Delta\chi^2$	ΔDf
Gender	811	494	1.6	837	513	1.6	26	19

Table 8
Testing for gender as a moderator in the structural model.

Model Characteristic	Unconstrained Group Model (Configurable invariance)	Constrained Group Model (Metric invariance, AE→PS, AE→PV, AE→RE, AE→RC, PV→SPA, RE→SPA, & RC→ SPA Equal Across Groups)	Model Differences
Model fit			
χ^2	957	972	15
Df	528	535	7
χ^2/Df	1.8	1.8	–
CFI	0.9	0.9	–
RMSEA	0.046	0.046	–
Path estimate ($P_{AE, PS}$)	0.29***(female), 0.18 (male)	0.22***(combined)	
Path estimate ($P_{AE, PV}$)	0.62***(female), 0.64***(male)	0.62***(combined)	
Path estimate ($P_{AE, RE}$)	0.38***(female), 0.70***(male)	0.47***(combined)	
Path estimate ($P_{AE, RC}$)	−0.14 (female), −0.19(male)	−0.14**(combined)	
Path estimate ($P_{PV, SPA}$)	−0.01(female), 0.15 (male)	0.05 (combined)	
Path estimate ($P_{RE, SPA}$)	0.29***(female), 0.27**(male)	0.26***(combined)	
Path estimate ($P_{RC, SPA}$)	−0.29***(female), −0.17 (male)	−0.24***(combined)	

Note: **: significant at $p < 0.05$; ***: significant at $p < 0.001$.

generations: Baby Boomers, Generation X, Millennial, and Gen Edge. People of each generation behave differently when they view the issues related to cybersecurity. Therefore, we split the sample into four subgroups (Table 2): Gen Edge (n = 75), Millennial (n = 235), Generation X (n = 47), and Baby Boomers (n = 30). The sample size reflects the current workforce age distribution. In 2021,[1] baby boomers are 57–75 years old, and many have already retired. Employees in the Generation X group are between 42 andto 56 years old, while millennials are 25–41 years old and are most productive. Gen Edges are 24 years old or younger, and most of them have not entered the workforce yet.

The results from ANOVA (Table 9) show significant differences among the four generations in employee awareness, perceived vulnerability, self-efficacy, and security protection behavior. Tukey's post hoc analysis further indicates that Gen Edge rated the Cyber Security Protection Action construct lower than the other three groups. Additionally, Gen Edge rated employee awareness and self-efficacy lower than that of Millennials, and Gen Edge rated employee awareness and perceived vulnerability lower than that of Generation X (Fig. 3). Thus, Hypothesis 4c, "Different generations behave differently when encountering cybersecurity issues," is supported. This is the first time when generations, rather than age groups, are used as an independent variable to assess employees' cybersecurity actions. Future research should pay more attention to the difference in generations to develop cybersecurity strategies tailored to different generations.

5.3. *The difference in types of organizations*

The sample is divided into two groups based on the survey responses, business (n = 352) and government (n = 35). A paired *t*t-test result shows that the two groups behave differently based on the eight constructs at $p < 0.10$. Fig. 4 indicates a significant difference between the two groups; therefore, Hypothesis 4b, " *Employees of a government agency have a higher level of awareness of cybersecurity severity than employees in a business firm when encountering cybersecurity issues,*" is supported.

Hair et al. (2006, p.174) indicated that researchers use levels ranging from 0.01 (most demanding) to 0.10 (less conservative). Therefore, we would like to remind the readers that $p < 0.10$ is a less conservative significant level.

6. Discussion

Since the efficacy of our proposed extended PMT model has been established, we would like to discuss our contributions to research and theory in the context of the research opportunities. This study evaluates the relationship between employees' cybersecurity awareness and the improvement of their motivational behavior, provides several valuable findings, and suggests a few theoretical implications and practical prescriptions. In the following section, we discuss theoretical contributions, practical applications, and policy implications.

6.1. *Theory-building contribution and predictive power of mediating factors*

This study makes three key theoretical contributions to the literature of cybersecurity research. First, our proposed conceptual model explains how cybersecurity protection action can change in response to security threats and coping behavior. The predictive power of the behavioral mediating factors (i.e., cybersecurity threat appraisal process and threat coping appraisal process) indicates the importance of organization effort on the changes in employee's security protective actions. The results of this study have provided a clear answer to the contradictory findings in the prior research regarding employees' perceived threats and responses when they are facing cybersecurity issues.

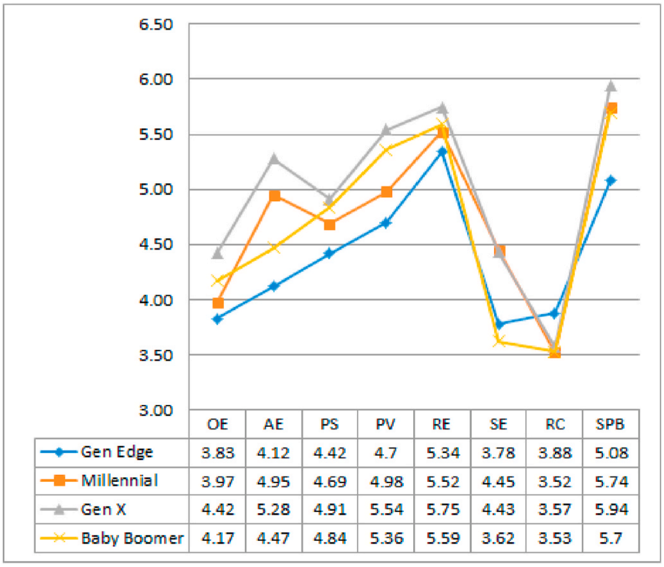
Secondly, the role of mediating factors in predicting cybersecurity protection actions has been confirmed in the information security study. Though employees' prior security action experience is associated with the security threat appraisal process, it does not significantly affect security protection. On the other hand, the coping appraisal process, which indicates the ability to avert the malicious threat, is the most important mediator for employees' cybersecurity protection action. The output of the coping appraisal-mediating process illustrates the predictive power for employee cybersecurity protection action. We believe that this is the first few studies that the role of the appraisal-mediating process in the cybersecurity study has been tested and reported. The

[1] Check this link for age groups https://www.ivyinvestments.com/advisor-resources/genlink/generation-edge.

Table 9
Generations - ANOVA and post hoc test (tukey HSD).

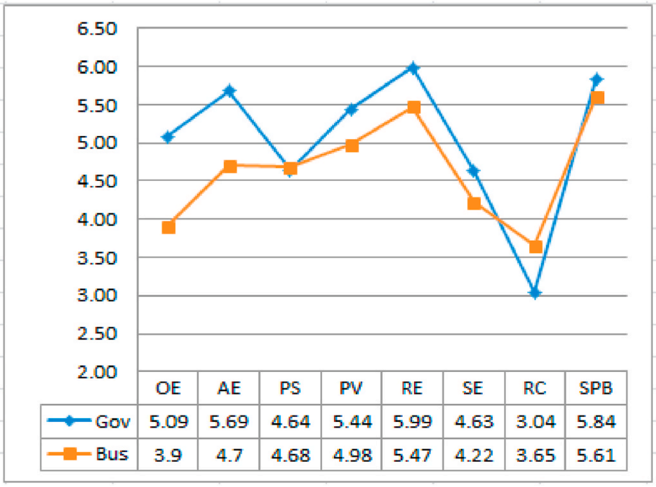
Constructs	ANOVA			Post Hoc Tests (Multiple Comparisons)					
	Between Groups			GenEdge - Millenial		GenEdge - Generation X		GenEdge - BabyBoomer	
	Mean	F	Sig.	Mean Difference	Sig.	Mean Difference	Sig.	Mean Difference	Sig.
OE	4.009	1.492	0.216	−0.139	0.914	−0.591	0.198	−0.340	0.761
EA	4.788	7.917	0.000	-.83,110*	0.000	−1.16161*	0.000	−0.351	0.704
PS	4.677	0.842	0.472	−0.267	0.687	−0.493	0.468	−0.422	0.707
PV	5.025	4.938	0.002	−0.280	0.345	-.83,390*	0.003	−0.655	0.081
RE	5.518	1.750	0.156	−0.175	0.532	−0.409	0.113	−0.247	0.647
SE	4.256	4.562	0.004	-.67,162*	0.016	−0.650	0.169	0.160	0.972
RC	3.596	1.126	0.338	0.357	0.267	0.302	0.692	0.343	0.707
SPA	5.630	8.205	0.000	-.65,604*	0.000	-.85,553*	0.000	-.62,033*	0.047

Note: Age include 4 subgroups.
* The mean difference is significant at the 0.05 level.



	OE	AE	PS	PV	RE	SE	RC	SPB
Gen Edge	3.83	4.12	4.42	4.7	5.34	3.78	3.88	5.08
Millennial	3.97	4.95	4.69	4.98	5.52	4.45	3.52	5.74
Gen X	4.42	5.28	4.91	5.54	5.75	4.43	3.57	5.94
Baby Boomer	4.17	4.47	4.84	5.36	5.59	3.62	3.53	5.7

Fig. 3. Generation groups and mediating factors.



	OE	AE	PS	PV	RE	SE	RC	SPB
Gov	5.09	5.69	4.64	5.44	5.99	4.63	3.04	5.84
Bus	3.9	4.7	4.68	4.98	5.47	4.22	3.65	5.61

Fig. 4. Government vs. Business and Mediating Factors; *t*t-test p < 0.1.

viable dependent variable in research on the extended PMT is the measure of motivational behavior rather than intension, as seen in the previous study. This finding extends and adds a theoretical implication to the PMT model.

Third, the antecedent factors (organization effort in combatting cyber threats and employee awareness in this study) are found to be significantly associated with the appraisal processes. Organization efforts are an essential antecedent for implementing information security policies because these efforts are the source of conviction that employees can reference when they decide to engage in security protection actions. Employee prior experience is an important precondition for information security behavioral change since it determines the initiation of coping behavior.

6.2. *Practical applications and some prescriptions*

Based on demographic information, the outcome of this research highlights three implications for security policy compliance in organizations from a practical view.

First, our result indicates that gender difference exists in the area of cybersecurity protection behavior. Previous research did not offer a conclusive finding. Therefore, this study adopts a multi-group structural model to investigate the moderating effects of gender on the relationship hypothesized in the structural model (Fig. 2). A couple of significant differences between participants who identified as male or female provide insight for future employee cybersecurity training. For example, women view cybersecurity awareness experience as a stronger antecedent to the perceived severity of data loss due to hacking, computer virus, and unauthorized access to information than men do.

Additionally, women view checking email attachments, checking privacy settings on social media, and backing up a dataset regularly (response cost) as less costly than men did. Therefore, we would like to suggest that future security training materials for male employees should emphasize the importance of action experience to alert the awareness of perceived severity. Moreover, it is essential for male employees to understand that response cost is an opportunity cost in cybersecurity protection. When an employee takes on some inconvenient activities, such as backing up computer systems or checking privacy settings, he improves his cybersecurity protection level.

Second, there is a difference between business and government organizations at the cybersecurity protection level. For example, in the US, government organizations have formulated detailed and clear guidelines on things federal employees should do and should not do regarding cybersecurity protective behavior (Federal Mobility Group, 2020), while business firms, though they have security compliance policies, do not have as strict rules as that of the government (i.e., can't print company's materials at home). The US federal government has shared the best cybersecurity practices for teleworking and using video collaboration tools with government employees and business workers (Federal Mobility Group, 2020). These best practices have improved employees' response efficacy and self-efficacy to work safely and securely online. As a result, employees are motivated to take on some inconvenient activities, such as backing up computer systems, updating passwords to protect the integrity of their organization's information system.

Third, the effect of generation difference on perceived threat and security coping strategy has been tested for the first time in this study. Previous studies used age groups as an independent variable to predict employee security protection intention. We suggest that generation groups would be a better predictor because the Gen Edge treats technology as a natural extension of their physical body compared with the other generations. People in the Gen Edge group were born after 1996. The oldest people in the Gen Edge group will be 25 years in 2021. They think and process information differently from those in the Baby Boomer group, Generation X group, and Millennials. Prensky (2001) named them Digital Natives because they are "native speakers" of the digital language of computers, video games, and the Internet. The other generation groups who were not born into the digital world but have learned new technologies later are "digital immigrants."

The results of our study indicate that Gen Edge shows a significant difference from that of other generations in the mediating constructs (Fig. 3). They rated cybersecurity awareness experience, perceived severity, and perceived vulnerability lower than the other three generatons. On the contrary, they view the costs of conducting preventive actions (i.e., response cost) higher than the perceived benefits compared with those of the other three groups. That means that they will back up their computer systems less frequently, pay less attention to unauthorized access of information, etc. As such, their security motivational action is scored lower than that of the other three generations. We suggest that future training should enhance the cybersecurity awareness of the Gen Edge generation, who will be the viable working force contributing to economic development in the near future.

6.3. Policy implications

A valuable policy implication that the results of this study suggest is the process that ensures the implementation of cybersecurity policy in organizations. The awareness of an organization's information security policy is related to employees' cognitive behavior and protective actions. To our knowledge, this finding has not been explicitly tested in previously published research. Developing a cybersecurity policy is not enough; the process that helps educate and maintain employees' awareness to implement the existing security policy is an integral part of a cybersecurity protection plan. Employees who are aware of cybersecurity policy behave significantly differently than employees who are unaware of security policy or employees of a company that does not have a security policy in place. We recommend that organizations develop a process that reminds employees of their essential and personal obligations, just as airline pilots and school bus drivers have to take breath tests before driving to ensure they can safely use their professional equipment.

7. Conclusion

This study tests an extended PMT model through an empirical analysis of the antecedents and mediators of employees engaging in cybersecurity protection actions and makes three key theoretical contributions to the literature of cybersecurity research. First, the proposed conceptual model provides an understanding of how cybersecurity protection action can change in response to security threats and coping behavior. Secondly, the role of mediating factors in predicting cybersecurity motivational actions has been confirmed. Third, the antecedent factors (organization effort in combatting cyber threats and employee awareness in this study) are found to be significantly associated with the cybersecurity threat and coping appraisal processes.

The extended PMT paradigm proposed in this study offers a prescriptive model to improve the effectiveness of cybersecurity fear appeal. Several practical prescriptions are suggested. First, due to the behavioral differences between male and female employees, future security training materials should emphasize the importance of action experience to alert male employees' awareness of the perceived severity of cyber threats. Secondly, government organizations tend to have a higher level of cybersecurity protection actions. Therefore, we suggest that government organizations share their experience in cybersecurity protection with business firms and help businesses develop better information security strategies. Third, future cybersecurity training materials should adapt to the traits of different generations. For example, Gen Edge is versatile with technology, but their awareness of the severity of cybersecurity is lower than other generations. Therefore, future training should focus on security awareness for employees who are in the Gen Edge group.

The main limitations of this study are as follows: the respondents' perceptions about their cybersecurity behaviors and practices were measured based on their self-reported behavior. Therefore, the generalizability of the result is limited. Future research can employ different data collection methods to collect respondents' actual cybersecurity behaniors, such as the experiment design approach that Van Bavel et al. (2019) used to study online purchasing. Other limitations include the sample size difference when we studied government organizations and business firms. Future research may further analyze the moderating effect of organization type on cybersecurity motivational behavior. Additionally, it is the first time generation groups are used as an independent variable to test the impact of generation identity on cybersecurity behavior. Future research should explore the underlying causes of the moderating effect of respective generations found in this study. Research instruments regarding the cybersecuiryt behavior of Digital natives in the Gen Edge group should be developed to understand what they think and how they behave.

Declaration of competing interest

No conflict of interest.

Acknowledgement

This work is supported by the National Science Foundation of the U. S. under Grant Number 1318470 and 1318501.

Appendix A

Constructs (Symbol)	Questions
Organization Effort (OE)	(Key reference and adapted from Herath & Rao, 2009a)
OE1	My organization distributes security newsletters or articles.
OE2	My organization organizes security talks and training.
OE3	My organization's Information Technology helpdesk sends out alert messages/emails concerning security.
Employee's Security Awareness (AE)	(Key reference and adapted from Ajzen, 2011; Herath & Rao, 2009a; IBM Security, 2020)
AE1	I had formal training on standard computer security practices.
AE2	The organization I worked for had an established information security policy.
AE3	The organization I worked for has provided employees with information security training.

(continued on next page)

(*continued*)

Constructs (Symbol)	Questions
Perceived Severity (PS)	(Key reference and adapted from Ali et al., 2021; Boss et al., 2015; Floyd et al., 2000; Herath & Rao, 2009a; Rogers, 1983; Wall & Warkentin, 2019; Wu, 2020; Yoo et al., 2021)
PS1	Having my computer infected by a virus as a result of opening a suspicious email attachment is a severe problem for me.
PS2	At work, having my confidential information accessed by someone without my consent or knowledge is a severe problem for me.
PS3	Loss of data resulting from hacking is a severe problem for me.
Perceived Vulnerability(PV)	(Key reference and adapted from Ali et al., 2021; Boss et al., 2015; Herath and Rao, 2009a; Lee & Larsen, 2009; Ng et al., 2007; Wall & Warkentin, 2019; Wu, 2020; Yoo et al., 2021)
PV1	I feel that my organization could become vulnerable to security breaches if I don't adhere to its information security policy.
PV2	I feel that I could fall victim to a malicious attack if I fail to comply with my organization's information security policy.
PV3	I believe that my effort to protect my organization's information will reduce illegal access to it.
PV4	My organization's data and resources may be compromised if I don't pay adequate attention to information security policies and guidelines.
Response Efficacy (RE)	(Key reference and adapted from Ali et al., 2021; Boss et al., 2015; Crossler & Bélanger, 2014; Wall & Warkentin, 2019; Wu, 2020; Yoo et al., 2021)
RE1	Complying with the information security policies in my organization will keep security breaches down.
RE2	If I comply with information security policies, the chance of information security breaches occurring will be reduced.
RE3	Careful compliance with information security policies helps to avoid security problems.
Self-Efficacy (SE)	(Key reference and adapted from Ali et al., 2021; Boss et al., 2015; Crossler & Bélanger, 2014; Herath & Rao, 2009a; Wall & Warkentin, 2019; Wu, 2020; Yoo et al., 2021)
SE1	I feel confident in setting the Web browser to different security levels.
SE2	I feel confident in handling virus-infected files.
SE3	I feel confident in getting rid of spyware and malware from my computer.
Response Cost (RC)	(Key reference and adapted from Ali et al., 2021; Boss et al., 2015; Crossler & Bélanger, 2014; Herath & Rao, 2009a; Menard et al., 2017)
RC1	It is inconvenient to check the security of an email with attachments.
RC2	Changing the privacy setting on social media sites is inconvenient.
RC3	Backing up a computer regularly is inconvenient.
Security Protection Behavior (SPB)	(Key reference and adapted from Boss et al., 2015; Floyd et al., 2000; Wall & Warkentin, 2019)
SPB1	I keep the anti-virus software on my computer up-to-date.
SPB2	I watch for unusual computer behaviors/responses (e.g., computer slowing down or freezing up, pop-up windows, etc.).
SPB3	I always act on any malware alerts that I receive.

Note: There are eight constructs. Participants responded to the question by choosing a 7-point Likert scale ranging from Strongly Disagree to Strongly Agree.

Demographic Items
1. Gender
2. Age group
3. Education Background
4. Job function area
5. Organization category
6. Organization size
7. Annual revenue

References

Adam, A., & Ofori-Amanfo, J. (2000). Does gender matter in computer ethics? *Ethics and Information Technology, 2*(1), 37–47.

Ajzen, I. (2011). The theory of planned behaviour: Reactions and reflections. *Psychology and Health, 26*(9), 1113–1127.

Ali, R. F., Dominic, P. D. D., Ali, S. E. A., Rehman, M., & Sohail, A. (2021). Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance. *Applied Sciences, 11*(8), 3383.

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimedia empirical examination of home computer user security behavioral intentions. *MIS Quarterly, 34*(3), 613–643.

Anderson, J. C., & Gerbing, D. W. (1988). Structural equation modeling in practice: A review and recommended two-step approach. *Psychological Bulletin, 103*(3), 411.

Anderson, B. B., Vance, A., Kirwan, C. B., Jenkins, J. L., & Eargle, D. (2016). From warning to wallpaper: Why the brain habituates to security warnings and what can be done about it. *Journal of Management Information Systems, 33*(3), 713–743.

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2013). Don't make excuses! Discouraging neutralization to reduce IT policy violation. *Computers & Security, 39*, 145–159.

van Bavel, R., Rodríguez-Priego, N., Vila, J., & Briggs, P. (2019). Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal of Human-Computer Studies, 123*, 29–39.

Bay Dynamics. (2016). How boards of directors really feel about cyber security reports. http://baydynamics.com/resources/how-boards-of-directors-really-feel-about-cyber-security-reports/.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly, 39*(4), 837–864.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 523–548.

Chen, Y., & He, W. (2013). Security risks and protection in online learning: A survey. *International Review of Research in Open and Distance Learning, 14*(5), 108–127.

Cronan, T. P., Leonard, L. N., & Kreie, J. (2005). An empirical validation of perceived importance and behavior intention in IT ethics. *Journal of Business Ethics, 56*(3), 231–238.

Crossler, R., & Bélanger, F. (2014). An extended perspective on individual security behaviors: Protection motivation theory and a unified security practices (USP) instrument. *ACM SIGMIS - Data Base: The DATABASE for Advances in Information Systems, 45*(4), 51–71.

D'Arcy, J., & Greene, G. (2014). Security culture and the employment relationship as drivers of employees' security compliance. *Information Management & Computer Security, 22*(5), 474–489.

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of Management Information Systems, 31*(2), 285–318.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research, 20*(1), 79–98.

Federal Mobility Group. (2020). Cybersecurity experts provide remote work best practices. July 8, 2020. https://www.cio.gov/cybersecurity-experts-provide-remote-work-best-practices/. (Accessed 10 October 2021).

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology, 30*(2), 407–429.

Gartner. (2019). Gartner forecasts worldwide public cloud revenue to grow 17% in 2020. November 13, 2019. https://www.gartner.com/en/newsroom/press-releases/2019-11-13-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-17-percent-in-2020. (Accessed 10 October 2021).

Grauer, Y. (2016). Cyber security executives need to step up their game: Here's why. http://www.forbes.com/sites/ygrauer/2016/06/14/cyber-security-executives-need-to-step-up-their-game-heres-why/#d54abda3be1a. (Accessed 5 January 2021).

Grosser, K., Moon, J., & Nelson, J. A. (2017). Guest editors' introduction: Gender, business ethics, and corporate social responsibility: Assessing and refocusing a conversation. *Business Ethics Quarterly, 27*(4), 541–567.

Gurinaviciute, J. (2021). 5 biggest cybersecurity threats. Security Magazine, February 3, 2021. Sept. 1, 2021 https://www.securitymagazine.com/articles/94506-5-biggest-cybersecurity-threats.

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2006). *Multivariate Data Analysis*. Upper Saddle River, NJ: Pearson Prentice Hall.

Haqaf, H., & Koyuncu, M. (2018). Understanding key skills for information security managers. *International Journal of Information Management, 43*, 165–172.

Herath, T., & Rao, H. R. (2009a). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154–165.

Herath, T., & Rao, H. R. (2009b). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106–125.

Ho, S. M., Hancock, J. T., Booth, C., & Liu, X. (2016). Computer-mediated deception: Strategies revealed by language-action cues in spontaneous communication. *Journal of Management Information Systems, 33*(2), 393–420.

Hovav, A., & D'Arcy, J. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the US and South Korea. *Information & Management, 49*(2), 99–110.

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. *Decision Sciences, 43*(4), 615–660.

Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM, 54*(6), 54–60.

IBM Security. (2020). The cost of a data breach report. Produced jointly between ponemon institute and IBM security. https://www.ibm.com/security/services?utm_content=SRCWW&p1=Search&p4=43700056097600130&p5=b&gclid=Cj0KCQjwnoqLBhD4ARIsAL5JedKMJWWNcGOgdDYtNtHCckJ8EkaFcEA81xIFeDqXu8a9wW1tyW2QNDIaAtuDEALw_wcB&gclsrc=aw.ds. (Accessed 10 October 2021).

Infographic. (2016). The cyber-attack threat in North America. June 16, 2016 https://www.zurichcanada.com/en-ca/knowledge-hub/articles/2016/06/the-cyber-attack-threat-in-north-america. (Accessed 8 May 2021).

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, 549–566.

Kim, G. H., Trimi, S., & Chung, J. H. (2014). Big-data applications in the government sector. *Communications of the ACM, 57*(3), 78–85.

Knight, M. B., & Pearson, J. M. (2005). The changing demographics: The diminishing role of age and gender in computer usage. *Journal of Organizational and End User Computing, 17*(4), 49–65.

Kreie, J., & Cronan, T. P. (1998). How men and women view ethics. *Communications of the ACM, 41*(9), 70–76.

Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: Determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems, 18*(2), 177–187.

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management, 45*, 13–24.

Li, L., He, W., Xu, L., Ivan, A., Anwar, M., & Yuan, X. (2014, August). Does explicit information security policy affect employees' cyber security behavior? A pilot study. In *2014 enterprise systems conference* (pp. 169–173). IEEE.

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

Lu, Y., & Xu, L. (2018). Internet of things (IoT) cybersecurity research: A review of current research topics. *IEEE Internet of Things Journal, 6*(2), 2103–2115.

McMillan, R., & Volz, D. (2021). Colonial pipeline hacker DarkSide says it will shut operations. The Wall street journal. May 14, 2021 https://www.wsj.com/articles/web-site-of-darkside-hacking-group-linked-to-colonial-pipeline-attack-is-down-11621001688?page=1.

Menard, P., Bott, G. J., & Crossler, R. E. (2017). User motivations in protecting information security: Protection motivation theory versus self-determination theory. *Journal of Management Information Systems, 34*(4), 1203–1230.

Mesmer-Magnus, J. R., & Viswesvaran, C. (2005). Whistleblowing in organizations: An examination of correlates of whistleblowing intentions, actions, and retaliation. *Journal of Business Ethics, 62*(3), 277–297.

Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory. *Journal of Applied Social Psychology, 30*(1), 106–143.

Minecast. (2021). https://www.mimecast.com/ Accessed 9/30/2021.

Morgan, S. (2015). Cybersecurity market reaches $75 billion in 2015; expected to reach $170 billion by 2020. http://www.forbes.com/sites/stevemorgan/2015/12/20/cybersecurity%E2%80%8B-%E2%80%8Bmarket-reaches-75-billion-in-2015%E2%80%8B%E2%80%8B-%E2%80%8Bexpected-to-reach-170-billion-by-2020/#14a6c3b12191. (Accessed 8 May 2021).

Ng, B. Y., Kankanhalli, A., & Xu, Y. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems, 46*(4), 815–825.

Ng, B. Y., & Xu, Y. (2007). Studying users' computer security behavior using the Health Belief Model. *PACIS 2007 Proceedings*, 423–437.

Peslak, A. R. (2008). Current information technology issues and moral intensity influences. *Journal of Computer Information Systems, 48*(4), 77–86.

Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems, 32*(4), 179–214.

Prensky, M. (2001). Digital natives, digital immigrants. On the horizon. *MCB University Press, 9*(5). October 2001.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology, 91*(1), 93–114.

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. T. Cacioppo, & R. E. Petty (Eds.), *Social Psychophysiology* (pp. 153–176). New York, NY: Guilford, 1983.

Safi, R., Browne, G. J., & Naini, A. J. (2021). Mis-spending on information security measures: Theory and experimental evidence. *International Journal of Information Management, 57*, 102291.

Sen, R., & Borle, S. (2015). Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information Systems, 32*(2), 314–341.

Siponen, M., Mahmood, M. A., & Pahnila, S. (2009). Technical opinion Are employees putting your company at risk by not following information security policies? *Communications of the ACM, 52*(12), 145–147.

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

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly, 34*(3), 487–502.

Stylianou, A. C., Winter, S., Niu, Y., Giacalone, R. A., & Campbell, M. (2013). Understanding the behavioral intention to report unethical information technology practices: The role of Machiavellianism, gender, and computer expertise. *Journal of Business Ethics, 117*(2), 333–343.

Sun, Y., Wang, N., & Shen, X. L. (2020). Toward a configurational protection motivation theory. HICSS. In *Proceedings of the 53rd Hawaii International conference on system Sciences, 2020*.

Vance, A., Lowry, P. B., & Eggett, D. (2013). Using accountability to reduce access policy violations in information systems. *Journal of Management Information Systems, 29*(4), 263–290.

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

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 425–478.

Wall, J. D., & Warkentin, M. (2019). Perceived argument quality's effect on threat and coping appraisals in fear appeals: An experiment and exploration of realism check heuristics. *Information & Management, 56*(8), 103157.

Woon, I., Tan, G. W., & Low, R. (2005). A protection motivation theory approach to home wireless security. *ICIS 2005 Proceedings*, 31.

Wu, D. (2020). Empirical study of knowledge withholding in cyberspace: Integrating protection motivation theory and theory of reasoned behavior. *Computers in Human Behavior, 105*, 106229.

Xu, L., Lu, Y., & Li, L. (2021). Embedding blockchain technology into IoT for security: A survey. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2021.3060508

Yoo, C. W., Lee, J., Yoo, C., & Xiao, N. (2021). Coping behaviors in short message service (SMS)-based disaster alert systems: From the lens of protection motivation theory as elaboration likelihood. *Information & Management, 58*(4), 103454.