The Effect of Organizational Information Security Effort on Employee Security Awareness and the Mediating Role of Coping and Threats Appraisal on Shaping Security Protection Motivational Behavior in a Manufacturing Company

Christine Ivy M. Mojares
christineivymojares11@gmail.com
Lipa City, 4217, Philippines

Abstract

In the rapidly evolving manufacturing industry, cybersecurity has become a critical concern as organizations increasingly rely on digital systems and interconnected technologies. However, there is limited empirical evidence explaining how organizational efforts and employee awareness translate into consistent cybersecurity behavior through underlying cognitive processes. Addressing this gap, this study positions Threat Appraisal and Coping Appraisal as key mechanisms linking Organizational Information Security Effort and Employee Security Awareness to Security Protection Motivational Behavior. Specifically, the study investigated the effect of Organizational Information Security Effort on Employee Security Awareness and examined whether Threat Appraisal and Coping Appraisal mediate the relationship between Employee Security Awareness and Security Protection Motivational Behavior. A quantitative research approach employing a descriptive-causal design was utilized, with data collected through survey questionnaires. The respondents consisted of design engineers working in a manufacturing company in Batangas, Philippines, whose roles involve direct interaction with digital systems and sensitive information, enabling them to provide informed insights on cybersecurity practices. The data were analyzed using descriptive and inferential statistical methods, including mean, standard deviation, regression analysis, and mediation analysis. The findings indicate that Organizational Information Security Effort significantly affects Employee Security Awareness, while Threat Appraisal and Coping Appraisal partially mediate the relationship between awareness and Security Protection Motivational Behavior. Based on this, organizations should strengthen their security initiatives, enhance awareness programs, and continuously develop employees' capabilities to promote sustainable cybersecurity behavior

Keywords: Coping Appraisal, Employee Security Awareness, Organizational Information Security Effort, Security Protection Motivational Behavior, Threat Appraisal.

INTRODUCTION

A. Background of the Study

The rapid digital transformation of global industries has significantly reshaped the manufacturing sector. The adoption of automation, Industrial Internet of Things (IIoT), artificial intelligence, enterprise systems, and interconnected operational technologies has enhanced productivity, efficiency, and supply chain integration. However, this increasing digital interconnectivity has also expanded the cyber threat landscape. Since 2022, manufacturing has consistently ranked among the most targeted industries worldwide due to its reliance on continuous operations, integrated supply chains, and the convergence of information technology (IT) and operational technology (OT) systems (IBM Security, 2023; Verizon, 2024). Cyber incidents such as ransomware, phishing attacks, and supply chain compromises frequently result in production downtime, financial losses, and reputational damage.

Despite advancements in technical defenses, evidence suggests that many cybersecurity breaches originate from human-related vulnerabilities rather than purely technological weaknesses. Phishing and social engineering attacks exploit employees' cognitive biases, risk perceptions, and decision-making processes. Employees may unintentionally disclose credentials, fail to recognize malicious communications, bypass protocols due to time pressure, or delay reporting suspicious activity. In manufacturing environments where IT systems are directly integrated with OT infrastructure a single compromised account can disrupt production lines, machinery operations, and supply chain coordination. This reality underscores a critical issue: technological safeguards alone are insufficient if employee cybersecurity behavior remains inconsistent.

In the Philippine context, cybersecurity threats have intensified alongside rapid digital adoption across industries. Reports from national and international cybersecurity organizations indicate a rise in phishing, ransomware, and cloud-related security incidents affecting both public and private sectors. CALABARZON (Region IV-A), one of the country's primary industrial and manufacturing hubs, hosts numerous export-oriented and technology-driven firms that rely heavily on interconnected production networks. The region's economic importance amplifies the consequences of cybersecurity incidents, as disruptions can cascade across supply chains and affect national productivity.

Within this industrial environment, many large manufacturing organizations have implemented formal information security policies, global compliance standards, technical controls, and cybersecurity awareness programs. However, internal organizational assessments in one major manufacturing firm in CALABARZON reveal persistent behavioral concerns. Despite structured training programs and simulated phishing exercises, employees continue to exhibit varying levels of phishing susceptibility, inconsistent password practices, delayed incident reporting, and occasional non-compliance with security procedures. These findings highlight a central organizational problem: the presence of information security efforts does not automatically translate into consistent protective behavior among employees.

Addressing this issue requires examining two key factors: organizational information security effort and employee security awareness. Organizational information security effort refers to the extent to which management implements formal policies, technical safeguards, monitoring systems, enforcement

mechanisms, and structured training programs to promote cybersecurity compliance. Employee security awareness, on the other hand, refers to employees' knowledge, understanding, and recognition of cybersecurity threats, policies, and best practices within the organization. Taken together, these factors establish the foundation upon which secure practices are expected to develop within the organization.

However, the mere presence of these efforts and awareness does not automatically guarantee secure outcomes. While these factors are commonly implemented in manufacturing firms, their effectiveness ultimately depends on whether they influence security protection motivational behavior. Security protection motivational behavior refers to employees' intentional and proactive actions aimed at protecting organizational information assets, including compliance with policies, secure credential management, vigilance against phishing attempts, and timely incident reporting. This behavior reflects not only awareness but also motivational and cognitive processes that drive individuals to act securely even under operational pressures. It encompasses both compliance-oriented behaviors, such as adhering to organizational security policies, and proactive behaviors, including reporting suspicious activities and actively preventing potential threats. As emphasized in recent studies, cybersecurity behavior is a critical human factor in organizational security, as employees serve as both the first line of defense and a potential point of vulnerability (Alshaikh, 2023; Al-Mhiqani et al., 2025).

Building on this, it becomes important to understand how such behavior reflects the success or limitations of organizational initiatives. Moreover, security protection motivational behavior serves as a key indicator of the effectiveness of organizational cybersecurity initiatives, as it demonstrates whether employees are able to translate knowledge, awareness, and policies into consistent real-world practices. In high-risk environments such as manufacturing, where cyber incidents can disrupt both digital and physical operations, employees' consistent engagement in protective behaviors significantly reduces organizational exposure to threats. However, prior research suggests that awareness alone does not guarantee secure behavior; employees must also be motivated and perceive security actions as necessary and manageable (Hussain & Wider, 2022; Rahman et al., 2024). Thus, strengthening security protection motivational behavior requires not only technical and educational interventions but also an understanding of the psychological and motivational factors that influence employees' decision-making processes, ensuring that secure practices are sustained over time and integrated into daily operational routines.

In order to further explain how these behavioral responses are formed, a theoretical lens is necessary. Protection Motivation Theory (PMT) provides a theoretical framework for understanding how organizational efforts and awareness translate into protective behavior. PMT posits that individuals' protective actions are shaped by cognitive appraisal processes involving perceived threat severity, perceived vulnerability, response efficacy, and self-efficacy. In high-pressure manufacturing environments, employees may prioritize productivity over security unless they perceive cyber threats as severe and believe they are capable of effectively mitigating them. Thus, organizational security efforts and awareness initiatives must not only inform employees but also strengthen their motivation to engage in protective behaviors.

Despite these theoretical and practical insights, gaps remain in the existing body of research. Despite the growing body of cybersecurity research globally, there remains a limited number of empirical studies examining how organizational information security efforts and employee security awareness influence security protection motivational behavior within Philippine manufacturing settings, particularly in Tanauan Batangas. Most existing studies focus either on technical controls or general awareness programs without integrating motivational mechanisms that explain why employees choose to comply or fail to comply with security practices under operational constraints.

In light of this gap, further investigation is necessary. This highlights the need to examine how organizational-level security initiatives and employee-level awareness contribute to strengthening security protection motivational behavior in manufacturing firms. By exploring this effect within a key industrial region of the Philippines and grounding the analysis in Protection Motivation Theory, this study aims to provide evidence-based insights that can help organizations enhance cybersecurity resilience not only through technology, but through sustained behavioral motivation.

B. Review of Related Literature

This review examines the mediating role of cognitive and threat appraisals in shaping security protection motivational behavior in manufacturing companies. Drawing on Protection Motivation Theory (PMT), the framework explains how individuals evaluate threats and coping responses to adopt protective behaviors (Rogers, 1975; Rogers, 1983). PMT has been widely applied in recent cybersecurity studies to explain why employees engage in secure practices. Contemporary empirical evidence shows that when individuals perceive a cyber threat as severe and believe they are vulnerable, they are more likely to adopt protective behaviors (Ifinedo, 2022). Likewise, beliefs regarding the efficacy of security measures, self-efficacy, and perceived costs significantly influence motivation to comply with security policies (Hanus & Wu, 2023; AlHogail, 2023; Al-Emran et al., 2023). Recent studies continue to support the use of PMT as a theoretical foundation for understanding cybersecurity behavior. PMT's threat and coping appraisal processes remain strong predictors of protective actions in organizational settings. Hussain and Wider (2022) applied PMT to government employees and found that threat appraisal components such as severity and vulnerability and coping appraisal components such as response efficacy and self-efficacy significantly influenced cybersecurity behavior. Similarly, Tambariki et al. (2024) extended PMT by integrating perceived knowledge and protection habits to explain cybersecurity behavior in mobile banking users, confirming the role of threat and coping appraisals in shaping protection motivation. In the healthcare sector, a 2025 study also demonstrated that PMT effectively predicts information security behaviors among professionals, with perceived severity and response efficacy emerging as key influences on protective motivation. These findings highlight how elements such as perceived severity, perceived vulnerability, response efficacy, self-efficacy, and response cost influence individuals' motivation to adopt protective actions.

Previous studies also emphasize the role of antecedents in influencing cybersecurity behavior. In the study of Li, Xu, and He (2022), antecedents refer to factors that influence or contribute to an individual's cybersecurity behavior before protective action is taken. Organizational cybersecurity efforts such as security training, policy enforcement, and awareness campaigns serve as important antecedents that shape employees' cybersecurity behavior. These efforts influence employees' perceptions of security threats and coping mechanisms, ultimately affecting their motivation to adopt protective cybersecurity practices. Similarly, White et al. (2022) described antecedents as factors that influence an organization's ability to implement cybersecurity measures, including financial and human resource constraints, management characteristics, awareness of cybersecurity risks, and previous experiences with cyber-attacks. Shaikh and Siponen (2024) further explained that antecedents may influence cybersecurity investment decisions, particularly through cybersecurity performance indicators such as breach costs and breach identification sources, which provide feedback that guides organizational decisions to strengthen cybersecurity investments. In the context of financial technology, Alhanatleh et al. (2024) identified social engineering threats, password security practices, and social media engagement as antecedents influencing cybersecurity awareness and the adoption of fintech services.

Organizational support also plays an important role in encouraging secure behavior among employees. Ahmad, Maynard, and Desouza (2022) found that organizations implementing multi-layered security strategies achieve higher employee compliance with information security practices. Similarly, Alshaikh (2023) reported that top management support and a strong security culture promote secure employee behavior. Bada and Nurse (2023) further demonstrated that continuous cybersecurity awareness and education programs improve employees' attitudes toward cybersecurity. Employee security awareness refers to employees' knowledge and understanding of cybersecurity threats, risks, and appropriate protective actions. Rohan et al. (2023) found that employees with higher levels of security awareness consistently demonstrate safer cybersecurity behavior. Likewise, Yılmaz and Ünal (2024) reported that security awareness significantly influences compliance with information security policies among academic library staff. Rahman et al. (2024) also found that cybersecurity awareness directly predicts individuals' motivation to engage in protective behavior. These findings suggest that increasing employee awareness is essential for reducing risky behavior and improving cybersecurity practices.

Perceived cybersecurity severity refers to the extent to which individuals recognize the seriousness of cyber threats and their potential impact. Li, Xu, and He (2022) explained that perceived severity is a key component of Protection Motivation Theory and influences individuals' motivation to take protective cybersecurity actions. Employees who perceive cyber threats as serious are more likely to follow security policies, use strong passwords, and avoid phishing scams. Jones et al. (2022) similarly defined perceived cybersecurity severity as an individual's awareness and evaluation of cybersecurity threats based on personal beliefs, experiences, and risk perception. De Kimpe, Walrave, Verdegem, and Ponnet (2021) further emphasized that individuals who perceive cybercrime as highly serious are more likely to adopt cybersecurity measures. Supporting these findings, Hussain and Wider (2022) and Al-Mhiqani et al. (2025)

reported that perceived severity significantly influences cybersecurity behavior across different organizational contexts.

Perceived vulnerability refers to an individual's subjective assessment of the likelihood of becoming a victim of cybercrime. De Kimpe et al. (2021) explained that this perception influences an individual's willingness to adopt protective cybersecurity measures. Individuals who feel well informed about cybersecurity may recognize the severity of cyber threats but perceive themselves as less vulnerable. Similarly, Li, Xu, and He (2022) described perceived vulnerability as employees' belief about the likelihood of experiencing cyberattacks or security breaches. Their study found that organizational cybersecurity efforts and awareness programs significantly influence employees' perceived vulnerability, which in turn affects their motivation to adopt protective security practices. Studies by Hussain and Wider (2022) and Al-Mhiqani et al. (2025) further confirm that perceived vulnerability significantly predicts cybersecurity behavior.

Response efficacy refers to an individual's belief that recommended cybersecurity measures are effective in preventing or reducing cyber threats. Li, Xu, and He (2022) explained that employees with higher response efficacy are more likely to engage in cybersecurity protective behaviors because they believe these actions will successfully mitigate cyber risks. Organizational cybersecurity efforts such as training programs and security policies also enhance employees' response efficacy. Similarly, De Kimpe et al. (2021) found that individuals who believe in the effectiveness of protective measures are more likely to adopt cybersecurity practices. Studies by Tsohou et al. (2023), Tambariki et al. (2024), and Al-Mhiqani et al. (2025) also reported that response efficacy positively influences cybersecurity behavioral intentions and actual security behavior.

Self-efficacy refers to an individual's belief in their ability to perform cybersecurity protective actions effectively. De Kimpe et al. (2021) explained that individuals with higher self-efficacy feel more confident in implementing security measures such as recognizing phishing attempts, installing antivirus software, and using strong passwords. Similarly, Li, Xu, and He (2022) noted that employees who believe they are capable of performing cybersecurity tasks are more likely to comply with security policies. Studies by Tsohou et al. (2023) and Hussain and Wider (2022) further confirmed that self-efficacy significantly influences employees' intention and actual cybersecurity behavior.

Response cost refers to the perceived burden or inconvenience associated with implementing cybersecurity protective measures. Li, Xu, and He (2022) explained that response cost includes factors such as time, effort, and financial resources required to follow security practices such as updating passwords, enabling multi-factor authentication, or participating in cybersecurity training. De Kimpe et al. (2021) similarly described response cost as the perceived effort, complexity, and inconvenience involved in adopting cybersecurity measures. Studies by Al-Mhiqani et al. (2025) and Tambariki et al. (2024) found that higher response costs reduce individuals' willingness to engage in cybersecurity practices. According to Protection Motivation Theory, high response costs may discourage protective behavior even when individuals recognize the severity and vulnerability of cyber threats.

Security protection motivational behavior refers to individuals' intention and willingness to adopt protective cybersecurity measures in response to perceived threats. De Kimpe et al. (2021) explained that PMT suggests this motivation is influenced by threat appraisal, which includes perceived severity and perceived vulnerability, and coping appraisal, which includes response efficacy, self-efficacy, and response cost. Similarly, Li, Xu, and He (2022) described security protection motivational behavior as the psychological and behavioral processes that drive individuals to engage in cybersecurity protective actions. Hussain and Wider (2022) demonstrated that both threat appraisal and coping appraisal significantly influence employees' cybersecurity behavior, while Rahman et al. (2024) found that cybersecurity awareness further strengthens employees' motivation to practice secure behaviors. Overall, the literature suggests that employees' motivation to adopt cybersecurity practices is shaped by a combination of organizational support, personal awareness, and cognitive appraisal processes. Organizations can therefore strengthen security protection motivational behavior by providing cybersecurity training, increasing awareness, and reducing the perceived cost of security measures, ultimately improving compliance with cybersecurity policies.

C. Research Framework

This outlines the research methods used to examine how antecedent factors and mediating mechanisms influence cybersecurity behavior. This section describes the research design, participants, instruments, and procedures applied in gathering and analyzing data. These methods ensure a systematic approach that supports the accuracy, validity, and reliability of the study's findings.

Theoretical Framework

This study is anchored on the Protection Motivation Theory, developed by Rogers (1975) and later expanded in 1983. Protection Motivation Theory explains how individuals evaluate threats and decide whether to engage in protective behaviors. Rogers proposed that when individuals are exposed to a threat, they undergo two cognitive processes threat appraisal and coping appraisal which shape their protection motivation and behavioral response. This theory suggests that behavior is influenced not only by awareness of risk but also by an individual's evaluation of their ability to respond effectively. Recent studies continue to validate PMT as a strong framework in cybersecurity research, demonstrating its relevance in explaining employees' security behavior in modern organizational environments (Li et al., 2022).

Rogers emphasized that threat appraisal consists of perceived severity and perceived vulnerability. Perceived severity refers to how serious the consequences of a threat are, while perceived vulnerability reflects the likelihood of experiencing the threat. In cybersecurity settings, employees assess the seriousness of cyberattacks and their susceptibility to such risks. According to PMT, higher levels of perceived severity and vulnerability increase the likelihood of developing protection motivation. However, Rogers also highlighted that when individuals perceive high threat but lack the ability to cope, they may

engage in maladaptive responses such as avoidance or denial instead of taking protective action (Rogers, 1983). Recent research supports this, showing that threat perception significantly influences cybersecurity behavior but must be accompanied by strong coping mechanisms to produce positive outcomes (Sulaiman, 2022; Alshaikh, 2022).

To complement threat appraisal, Rogers introduced coping appraisal, which evaluates an individual's ability to manage the threat. This includes response efficacy, self-efficacy, and response cost. Response efficacy refers to the belief that security measures are effective, while self-efficacy reflects confidence in one's ability to perform those measures. Response cost represents perceived barriers such as effort, time, or inconvenience. Rogers explained that individuals are more likely to adopt protective behaviors when they believe that the response is effective, that they are capable of performing it, and that the associated costs are low. Empirical studies have confirmed that coping appraisal plays a critical role in cybersecurity behavior, particularly self-efficacy and response efficacy, which significantly predict employees' compliance with security practices (Li et al., 2022).

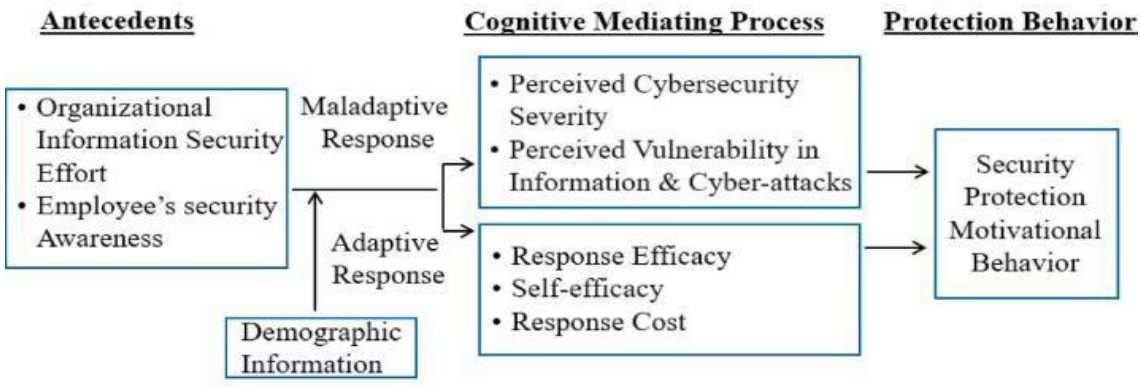

Figure 1. Theoretical Framework

Source: The effects of antecedents and mediating factors on cybersecurity protection behavior (Ling Li *, Li Xu, Wu He 2022)

The application of Rogers' theory in this study is illustrated in Figure 1, which adapts PMT to a cybersecurity context. In this framework, organizational information security effort and employee security awareness function as antecedent variables that influence employees' cognitive appraisal processes. These factors enhance employees' perception of cybersecurity severity and vulnerability (threat appraisal) and strengthen their confidence in performing protective behaviors (coping appraisal). Organizational efforts such as training, policies, and awareness campaigns play a crucial role in improving both appraisal processes by increasing knowledge, building skills, and reducing uncertainty. As supported by recent studies, organizational support and awareness initiatives significantly influence employees' cybersecurity behavior through psychological mechanisms such as threat and coping appraisal (Li et al., 2022).

Overall, the Protection Motivation Theory provides a structured explanation of how employees' cybersecurity behavior is shaped through cognitive evaluation processes. In this study, the theory is extended by incorporating organizational information security effort and employee security awareness as key antecedents that influence both threat appraisal and coping appraisal. These appraisal processes serve as critical mechanisms through which external organizational initiatives are translated into security protection motivational behavior. By positioning threat appraisal and coping appraisal as mediating variables, the framework explains not only the direct influence of organizational and individual factors but also the underlying psychological processes that drive behavioral outcomes. This theoretical integration strengthens the explanatory power of the model and provides a comprehensive basis for examining how organizational strategies and individual perceptions interact to influence cybersecurity behavior in the workplace (Li et al., 2022).

Conceptual Framework

This study adopts the conceptual framework developed by Li, Xu, and He (2022), which is grounded in the Protection Motivation Theory. The framework follows a structured paradigm consisting of independent variables, mediating variables, and a dependent variable. In this study, organizational information security effort is treated as the independent variable, employee security awareness and the cognitive appraisal variables serve as mediating variables, and security protection motivational behavior is the dependent variable. The model explains that employees' cybersecurity behavior is not directly influenced by organizational initiatives alone but is shaped through cognitive evaluation processes, specifically threat appraisal and coping appraisal. The study found that organizational information security effort has a significant positive effect on employee security awareness, highlighting the importance of organizational initiatives in building a foundation for cybersecurity behavior (Li et al., 2022).

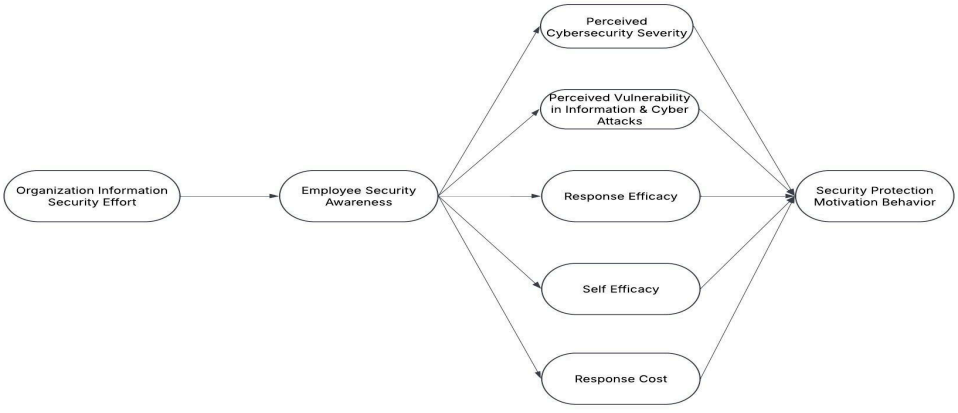

Figure 2. Conceptual Framework

Source: The effects of antecedents and mediating factors on cybersecurity protection behavior

(Ling Li *, Li Xu, Wu He 2022)

Figure 2 illustrates the conceptual framework of the study. It shows that the independent variable, organizational information security effort, directly influences the mediating variable, employee security awareness. This awareness then affects five cognitive variables perceived cybersecurity severity, perceived vulnerability, response efficacy, self-efficacy, and response cost which also function as mediating variables under threat appraisal and coping appraisal. These mediating variables collectively influence the dependent variable, security protection motivational behavior. The study found that employee security awareness significantly influences both threat appraisal and coping appraisal variables, indicating that awareness plays a critical role in shaping how employees perceive risks and evaluate their ability to respond (Li et al., 2022).

In terms of threat appraisal, the mediating variables include perceived cybersecurity severity and perceived vulnerability, which reflect employees' evaluation of the seriousness of cyber threats and their susceptibility to such threats. These variables serve as mediators between awareness and behavior. The study found that both perceived severity and perceived vulnerability have a significant positive effect on the dependent variable, security protection motivational behavior, indicating that higher perceived risk encourages protective actions. However, the study also found that these threat appraisal variables have a weaker influence compared to coping appraisal variables, suggesting that risk perception alone is not sufficient to strongly drive behavior (Li et al., 2022).

With regard to coping appraisal, the mediating variables include response efficacy, self-efficacy, and response cost, which represent employees' evaluation of their ability to manage cybersecurity threats. These variables also act as mediators linking awareness to behavior. The study found that response efficacy and self-efficacy have strong and significant positive effects on the dependent variable, indicating that employees are more likely to engage in protective behavior when they believe in the effectiveness of security measures and their capability to perform them. In contrast, the study found that response cost has a significant negative effect, meaning that higher perceived barriers reduce the likelihood of engaging in protective actions (Li et al., 2022).

The dependent variable, security protection motivational behavior, represents the actual cybersecurity actions performed by employees, such as complying with security policies and practicing safe system use. The study found that both threat appraisal and coping appraisal significantly influence this dependent variable, with coping appraisal exerting a stronger effect, emphasizing that employees' confidence and perceived effectiveness of security measures are more influential than risk perception alone.

Operational Framework.

This section presents the operational framework of the study, which specifies the key variables and their roles in explaining cybersecurity behavior within a manufacturing setting in the Philippines. The framework is adapted from the model of Li, Xu, and He (2022) and is grounded in the Protection Motivation Theory. Consistent with the theoretical and conceptual frameworks, the model explains that employees' cybersecurity behavior is shaped through threat appraisal and coping appraisal, which are affect by both organizational factors and individual awareness. The framework identifies the independent

variable, mediating variables, and the dependent variable, providing a structured basis for analyzing how organizational initiatives translate into employee security behavior through cognitive evaluation processes.

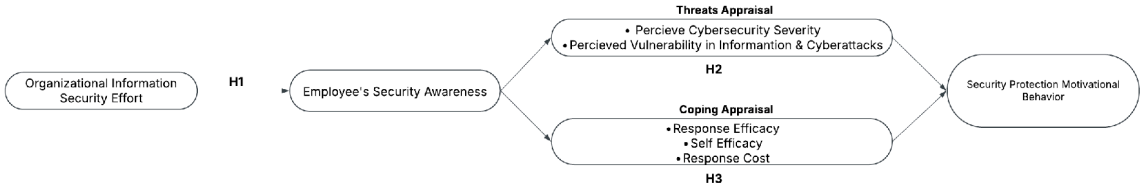

Figure 3. Operational Framework

Figure 3 illustrates the operational framework of the study. It shows that organizational information security effort affects employee security awareness. Threat appraisal (perceived cybersecurity severity and perceived vulnerability) and coping appraisal (response efficacy, self-efficacy, and response cost) mediate employee security awareness and security protection motivational behavior. This sequential structure reflects the core assumption of Protection Motivation Theory, where individuals first become aware of a threat, evaluate its seriousness and their susceptibility, assess their ability to respond, and ultimately decide whether to engage in protective behavior.

The independent variable, organizational information security effort, refers to the organization's overall commitment to cybersecurity through the implementation of formal policies, continuous training programs, awareness initiatives, and managerial support. Within the context of this study, it represents the external environment that promotes secure practices and shapes employees' exposure to cybersecurity information. Aligned with the theoretical framework, this variable serves as the initiating factor that enhances employees' awareness and influences how they cognitively process cybersecurity risks.

Employee security awareness, refers to the degree to which employees possess knowledge and understanding of cybersecurity threats, vulnerabilities, and appropriate protective practices. This includes their ability to recognize potential cyber risks, understand organizational security policies, and apply safe behaviors in handling information systems. In alignment with Protection Motivation Theory, awareness functions as a critical precursor to both threat appraisal and coping appraisal, as it enables employees to accurately evaluate the nature of cybersecurity threats and their ability to respond effectively.

Threat appraisal, includes perceived cybersecurity severity and perceived vulnerability. Perceived cybersecurity severity refers to employees' evaluation of the seriousness of cyber threats and the potential consequences they may cause, such as data breaches, financial loss, or system disruption. Perceived vulnerability refers to employees' belief regarding the likelihood that they or their organization may be affected by such threats. Consistent with the theoretical and conceptual framework, these variables reflect how employees assess risk, which is essential in motivating protective behavior. However, in alignment with PMT, threat perception alone does not guarantee action unless supported by strong coping beliefs.

On the other hand, coping appraisal, includes response efficacy, self-efficacy, and response cost. Response efficacy refers to the belief that recommended cybersecurity measures are effective in preventing or reducing threats. Self-efficacy reflects the individual's confidence in their ability to successfully perform cybersecurity-related actions. Response cost refers to the perceived barriers associated with compliance, such as time, effort, complexity, or inconvenience. These variables explain how employees evaluate their capability to respond to threats, and they play a crucial role in determining whether individuals translate their awareness and risk perception into actual protective behavior.

Security protection motivational behavior, refers to the actual cybersecurity practices performed by employees to safeguard organizational information systems. These behaviors include compliance with security policies, proper handling of sensitive data, use of secure authentication methods, and avoidance of risky online activities. In alignment with both the theoretical and conceptual frameworks, this variable represents the outcome of the cognitive evaluation process, where employees' perceptions of threat and coping ability influence their decision to engage in protective cybersecurity actions.

This means that operational framework demonstrates that cybersecurity behavior is not solely driven by organizational policies or awareness alone but is the result of a structured cognitive process involving threat appraisal and coping appraisal. By aligning with Protection Motivation Theory and the conceptual model of Li et al. (2022), this framework provides a coherent and comprehensive basis for analyzing how organizational and psychological factors interact to influence security protection motivational behavior in the manufacturing sector.

D. Objectives of the Study:

To investigate how organizational information security efforts and employees' security awareness, mediated by cognitive processes influence security protection motivational behavior. Specifically, the study determined if:

1. Organizational Information Security Effort significantly affects on Employee Security Awareness.
2. Threat Appraisal mediates employee security awareness and security protection motivational behavior.
3. Coping Appraisal mediates employee security awareness and security protection motivational behavior.

E. Hypothesis

To address the need of the study, the following hypotheses were tested: This must be aligned with the objectives of the study.

H_{01}: Organization Information Security Effort has no significant effect on Employee Security Awareness.

H_{02}: Threat appraisal has no mediating effect on the relationship between Employee Security Awareness and Security protection motivational behavior.

H_{03}: Coping appraisal has no mediating effect on the relationship between Employee Security Awareness and Security protection motivational behavior

F. Significance of the Study

Cybersecurity threats continue to evolve, posing significant risks to organizations and individuals. Understanding the antecedent factors that influence cybersecurity behavior, as well as the mediation mechanisms that is crucial in strengthening overall security frameworks. This study aims to provide valuable insights into how psychological, organizational, and technological factors drive cybersecurity practices and risk perception among users and institutions.

From an academic perspective, this research contributes to the growing body of knowledge in cybersecurity by integrating behavioral theories. By identifying key drivers of cybersecurity behavior, this study helps bridge gaps in understanding how individuals and organizations respond to cyber threats.

For businesses and industries, particularly in sectors highly vulnerable to cyberattacks, such as manufacturing, finance, and critical infrastructure, the findings can inform the development of targeted cybersecurity policies, employee training programs, and technological interventions to mitigate risks. Organizations can use these insights to cultivate a proactive cybersecurity culture, ensuring resilience against potential cyber threats.

Furthermore, this study aligns with United Nations Sustainable Development Goal (SDG) 9: Industry, Innovation, and Infrastructure, which emphasizes the importance of building resilient infrastructure, promoting inclusive and sustainable industrialization, and fostering innovation. A robust cybersecurity framework is essential for ensuring the security and resilience of digital infrastructures, which play a critical role in economic growth and technological advancement. By improving cybersecurity behaviors strategies, this research contributes to the long-term sustainability of digital ecosystems and industrial progress. Ultimately, this study aims to enhance cybersecurity readiness by providing a holistic understanding of the factors influencing cybersecurity behavior. By addressing these critical areas, the research contributes to building a more secure digital ecosystem for individuals, businesses, and society as a whole.

II. METHODS

This section outlines the research methods and procedures used to achieve the objectives of the study. It includes the research design, data collection techniques, sampling methods, and analytical methods used to examine the mediating role of coping and threats appraisals in shaping security protection motivational behavior in a manufacturing company.

A. Research Design

This study employed a descriptive–causal research design using a quantitative approach to examine the mediating roles of threat appraisal and coping appraisal in shaping security protection motivational behavior within a manufacturing company. The descriptive component of the design was utilized to systematically present the current condition of the key variables included in the study. Specifically, it describes the levels of organizational information security effort, employee security awareness, perceived cybersecurity severity, perceived vulnerability, response efficacy, self-efficacy, response cost, and security protection motivational behavior among employees. By doing so, the study provides a comprehensive empirical profile of employees' cybersecurity-related perceptions and behaviors within the organizational setting.

The study adopted a quantitative approach because it focuses on the numerical measurement of variables and the statistical analysis of relationships among them. This approach allows for objective, systematic, and replicable data collection through structured survey instruments, ensuring consistency and reliability of responses. It enables the researcher to quantify employees' levels of awareness, cognitive appraisal, and protective behavior, and supports the use of statistical techniques necessary for testing the relationships proposed in the conceptual framework.

In addition to describing the variables, the study incorporated a causal design to examine the directional relationships among them. Specifically, it seeks to determine how organizational information security effort influences employee security awareness, and how awareness affects threat appraisal and coping appraisal, which in turn influence security protection motivational behavior. Regression and mediation analysis were employed to assess the strength and significance of both direct and indirect relationships among variables. By integrating descriptive and causal elements within a quantitative framework, the study is able to both describe existing conditions and explain relationships among variables, providing a systematic and theory-aligned approach to understanding cybersecurity behavior in a manufacturing environment.

B. Locale of the Study

This study was conducted in the engineering department of a multinational power management manufacturing firm located in the Tanauan Batangas, within the Region IV-A of the Philippines. Batangas is widely recognized as one of the country's major industrial centers, hosting numerous manufacturing companies engaged in electronics, electrical systems, semiconductors, and industrial equipment production. The selected firm operates in a highly technology-driven environment where engineering and production processes depend on computer-aided design systems, automated machinery, networked platforms, and centralized information systems. Due to the nature of its operations, the organization manages sensitive technical data, proprietary designs, and critical operational information, making cybersecurity a vital concern for maintaining data integrity, system reliability, and organizational continuity.

The manufacturing sector, particularly engineering-intensive firms, is increasingly exposed to cybersecurity risks due to its reliance on interconnected digital systems and industrial technologies. These risks include unauthorized access to confidential data, data breaches, and disruptions to operational processes. Within this context, the engineering (design) department was selected as the focus of the study because employees in this unit are directly involved in the development, modification, and management of technical designs and digital systems. Their roles require continuous interaction with specialized software, databases, and networked platforms, which increases their exposure to cybersecurity threats. As such, this locale provides an appropriate setting for examining how employees' security awareness, threat appraisal, and coping appraisal influence their security protection motivational behavior in a manufacturing environment.

C. Respondents of the Study

The respondents of this study consisted of design engineers working in the engineering department of a multinational power management manufacturing firm located in Batangas. The selection of design engineers was intentional due to the nature of their roles within the organization. These professionals are directly involved in the development, modification, and management of technical designs, systems, and digital files, which often contain sensitive and proprietary information. Their responsibilities require frequent interaction with digital platforms, engineering software, and information systems, making them particularly relevant for examining cybersecurity-related awareness, cognitive appraisal, and protective behavior.

At the time of data collection, the Engineering Department had a total of 672 engineers, consisting of 208 females and 464 males. Focusing on this specific group enabled the study to obtain targeted and context-specific insights into employees' cybersecurity perceptions and behaviors within a manufacturing environment. This approach enhanced the relevance of the data collected and strengthened the validity of the findings, as design engineers represent a critical group whose roles involve both high exposure to cybersecurity risks and significant responsibility in safeguarding organizational information assets.

D. Sampling Design

This study employed a stratified random sampling technique to ensure a proportionate and representative selection of respondents from the Engineering Department. The total population was divided into seven functional teams, with each team treated as a distinct stratum, and respondents were randomly selected from each group based on their proportional size relative to the overall population. The sample size was determined using the G Power statistical tool, with the following parameters: an effect size of 0.15, an error probability (α) of 0.05, a statistical power of 0.95, three tested predictors. Based on this computation, the required sample size was 119 participants.

Table 2. Stratified Distribution of Respondents per Team

Population	No. of Members	Percentage	No. of Respondents
Design Team 1	42	6%	7
Design Team 2	349	52%	62
Design Team 3	46	7%	8
Design Team 4	69	10%	12
Design Team 5	59	9%	10
Design Team 6	62	9%	11
Design Team 7	45	7%	8
Grand Total	**672**	**100%**	**119**

This approach was appropriate as it considered variations in roles and responsibilities among design engineers that may influence cybersecurity awareness, threat appraisal, and coping appraisal. By ensuring representation across all functional teams, the sampling method minimized bias and improved the reliability and validity of the data, providing a comprehensive understanding of cybersecurity-related perceptions and behaviors. It should also be noted that the pre-test data were not included in the final analysis.

E. Data Gathering Procedure

The researcher first sought approval from the ethics and compliance committee of the manufacturing company. Once approval was granted, the questionnaire was shared with participants via Microsoft Forms, accompanied by an informed consent statement explaining the study's purpose, voluntary participation, and data confidentiality. Participants were given a specific timeframe to complete the survey, with follow-ups conducted when necessary to improve response rates.

F. Research Tools and Instruments

The study used a structured survey questionnaire to gather data from the participants. The survey questionnaire was derived from previous studies. The researcher fully adopted and adapted the questionnaire items from these studies to align with the specific objectives of this research. The questionnaire will be adapted from the study of Ling Li, Li Xu, Wu He 2022 which is valid to use on a engineering and manufacturing setup. The survey will be uploaded to Microsoft Forms for ease of distribution and response collection. Anonymity and confidentiality will be ensured to protect the data privacy of respondents. Responses will be measured using a Seven-point Likert scale, with the following options: (5) Strongly Agree, (4) Agree, (3) Neutral, (2) Disagree and (1) Strongly Disagree.

Table 1.0 Mean Score interpretation

Scale	Range of Mean Scores	Verbal Interpretation
5	4.21 - 5.00	Strongly Agree
4	3.41 - 4.20	Agree
3	2.61 - 3.40	Neutral

2	1.81 - 2.60	Disagree
1	1.00 - 1.80	Strongly Disagree

To test the reliability of the survey questionnaire, the researcher distributed the instruments in the 46 participants from the total population of engineering department. Random probability was used to select the respondents and to ensure that all have a chance to be selected on the reliability testing. After the data was collected on the Microsoft form, the researcher run the data using Jamovi software to test the result of the test. The researcher measured the Cronbach's alpha of each of the variable stated on the framework. A value of above or equal to 0.800 is considered acceptable. Table 1 shows the result of the reliability test of the test questionnaire.

Table 2.0 Cronbach's Reliability Results (n=46)

Variable	No. of Items	Cronbach's α
Organizational Information Security Effort	3	0.868
Employee's Security Awareness	3	0.873
Perceived Severity	3	0.886
Perceived Vulnerability	4	0.871
Response Efficacy	3	0.945
Self-Efficacy	3	0.924
Response Cost	3	0.921
Security Protectional Motivational Behavior	3	0.895
OVERALL	**25**	**0.934**

The reliability of the instrument was assessed using Cronbach's alpha. As shown in Table 1, all variables demonstrated acceptable internal consistency, with alpha values ranging from .852 to .939. Specifically, Organization Effort (α = .868), Employee's Security Awareness (α = .871), Perceived Severity (α= .906), Perceived Vulnerability (α = .852), Response Efficacy (α = .939), Self-Efficacy (α = .920), Response Cost (α = .915), and Security protection motivational behavior (α = .890) all exceeded the recommended threshold of .70 (Nunnally & Bernstein, 1994), indicating strong reliability. The overall Cronbach's alpha for the 25-item scale was .934, reflecting excellent internal consistency of the instrument. The instrument was validated using convergent validity and discriminant validity, indicating that all measurement items appropriately captured their intended constructs and were distinct from one another. Convergent validity was confirmed through statistically significant factor loadings and acceptable variance explained, demonstrating that multiple indicators consistently measured the same construct. Discriminant validity was also established, as correlations among constructs remained below the recommended threshold, confirming that each variable represented a unique dimension of cybersecurity behavior. These validation results suggest that the instrument is both reliable and valid for assessing cybersecurity-related constructs. Consequently, the instrument can be considered suitable for application in a design and manufacturing setup, where understanding employee cybersecurity behavior is critical for safeguarding organizational

information systems. These findings are consistent with prior research that utilized Protection Motivation Theory (PMT) and validated similar constructs in organizational cybersecurity contexts (Li et al., 2022).

G. Data Analysis

Once data collection was completed, the responses underwent data cleaning to remove missing or inconsistent values, ensuring accuracy. The cleaned data were then uploaded into statistical software such as SPSS. The study employed appropriate statistical techniques, such as regression and mediation analysis, to test the hypotheses. The findings from this analysis provided valuable insights into the mediating role of coping and threat appraisal, ultimately helping to formulate recommendations for improving security protection motivational behavior within the organization.

H. Ethical Considerations

The researcher carefully followed the ethical guidelines set by the institution's Ethics Review Board and the company's ethics committee throughout the entire study. Before participating, all respondents were informed about the purpose of the research and were asked to sign an informed consent form. The terms stated in the form were strictly followed to protect their rights and well-being. To maintain their privacy, no personal information was revealed, and all responses remained anonymous and confidential. All collected data were stored securely in password-protected digital files accessible only to the researcher. These files were kept for one year after the study was completed, after which they were permanently deleted, and any printed documents were properly shredded. This ensured that participants' information remained private and was handled with the utmost care even after the study ended.

III. RESULTS AND DISCUSSION

This chapter presents the data gathered, discussion, and interpretation of the findings in relation to the study's objectives and hypotheses.

A. Descriptive Statistics

Organizational Information Security Effort, Employee Security Awareness, Threats Appraisal, Coping Appraisal, and Security Protection Motivational Behavior

Table 3 presents the descriptive statistics of the key constructs included in the study, namely Organizational Information Security Effort, Employee Security Awareness, Threats Appraisal, Coping Appraisal, and Security Protection Motivational Behavior. The results indicate that respondents generally reported high to very high levels of agreement across all constructs, as evidenced by mean values ranging

from 3.17 to 4.40 on a five-point Likert scale. Organizational Information Security Effort obtained a mean score of 4.24, interpreted as very high, suggesting that the organization effectively implements cybersecurity policies, training programs, and protective mechanisms to safeguard information assets.

Table 3. Descriptive Statistics of the Study Variables

Variable	Mean	Standard Deviation	Verbal Interpretation
Organizational Information Security Effort	4.24	0.67	Very High
Employee's Security Awareness	4.17	0.82	High
Threats Appraisal	4.36	0.71	Very High
Perceived Severity	4.4	0.72	Very High
Perceived Vulnerability	4.32	0.59	Very High
Coping Appraisal	3.82	0.94	High
Response Efficacy	4.35	1.27	Moderate
Self-Efficacy	3.94	0.68	Very High
Response Cost	3.17	0.66	Very High
Security Protectional Motivational Behavior	4.32	0.67	High

Employee Security Awareness obtained a mean score of M = 4.17, SD = 0.82, interpreted as high, indicating that employees possess a strong understanding of cybersecurity risks and practices. This suggests that awareness initiatives such as training, seminars, and information campaigns are generally effective in improving employees' knowledge and vigilance toward cybersecurity threats.

Threats Appraisal recorded a high overall mean of M = 4.36, SD = 0.71, interpreted as very high, indicating that employees strongly perceive cybersecurity threats. Among its components, Perceived Severity (M = 4.40, SD = 0.72) and Perceived Vulnerability (M = 4.32, SD = 0.59) both fall under the very high category, suggesting that employees recognize both the seriousness of cyber threats and their susceptibility to such risks. These findings imply that employees are highly aware of potential cyberattacks and understand the possible consequences of security breaches.

Coping Appraisal obtained an overall mean score of M = 3.82, SD = 0.94, interpreted as high, indicating that employees generally feel capable of responding to cybersecurity threats. Among its components, Response Efficacy (M = 4.35, SD = 1.27) was interpreted as moderate, suggesting that while employees believe in the effectiveness of security measures, there is some variability in their confidence. Self-Efficacy (M = 3.94, SD = 0.68) was interpreted as very high, indicating strong confidence in their ability to perform protective actions, while Response Cost (M = 3.17, SD = 0.66) was also interpreted as very high, suggesting that employees perceive minimal barriers in adopting security behaviors.

Notably, Security Protection Motivational Behavior obtained a mean score of M = 4.32, SD = 0.67, interpreted as high, indicating that employees are highly motivated to engage in cybersecurity protective behaviors. This suggests that organizational efforts, combined with strong awareness and threat perception, contribute positively to employees' intention to practice secure behaviors in handling information systems.

Overall, these findings suggest that the organization has established a strong foundation in cybersecurity practices, supported by high levels of awareness, threat perception, and motivational behavior among employees. The relatively moderate standard deviation values ranging from 0.59 to 1.27 indicate a reasonable level of consistency in responses, although some variability exists particularly in coping-related factors. Recent literature supports that lower standard deviation reflects greater agreement among respondents, indicating consistency and reliability of survey results (IBM, 2023; Elsevier, 2022). This consistency suggests a shared understanding of cybersecurity practices within the organization, reinforcing the stability and validity of the study findings (Springer, 2022).

B. Inferential Statistics

Effect of Organizational Information Security Effort (OE) on Employee Security Awareness (ESA)

Table 4 presents the regression matrix examining the effect of Organizational Information Security Effort (OE) on ESA. The results indicate that Organizational Information Security Effort has a positive and statistically significant effect on ESA ($\beta = 0.737$, $p = 0.000$). The model is statistically significant ($F = 274.636$, $p = 0.000$), confirming its adequacy.

Table 4

Linear Regression: Effect of Organizational Information Security Effort on ESA

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig. (p-value)	Interpretation
	B	Std. Error	Beta			
(Constant)	-1.108	0.313	—	-3.542	0	Significant
OE	1.216	0.073	0.737	16.57	0	

$R^2 = 0.543$; f – value = 274.636; p – value = 0.000; DV: ESA

This suggests a strong positive relationship between Organizational Information Security Effort and Employee Security Awareness, meaning that as organizations enhance their cybersecurity initiatives—such as implementing policies, conducting training, and promoting awareness ESA significantly improves. Overall, Organizational Information Security Effort explains 54.3% of the variance in ESA ($R^2 = 0.543$, $F = 274.636$, $p = 0.000$), indicating a high explanatory power.

This finding is supported by existing literature indicating that organizational cybersecurity efforts significantly influence employee-related outcomes by strengthening awareness, compliance, and security behavior. Studies have shown that organizational support mechanisms, including clear security policies, continuous training, and management commitment, play a critical role in shaping employees' cybersecurity practices and improving overall behavioral outcomes (Ifinedo, 2022; Sulaiman et al., 2022; AlHogail, 2023). High R^2 values reported in similar research further emphasize the strong explanatory power of organizational initiatives in predicting security-related behaviors. However, employee awareness may still be influenced by other factors such as individual perceptions, prior experience, and organizational culture

(Alshaikh, 2022; Sulaiman et al., 2022). Thus, while organizational effort is a strong predictor, it operates alongside other important variables in enhancing overall cybersecurity effectiveness.

Mediating Effect of Threat Appraisal on the Relationship between Employee Security Awareness and Security Protection Motivational Behavior

Table 5 presents the mediation analysis examining whether Threat Appraisal mediates the relationship between Employee Security Awareness and Security Protection Behavior. The results show that Employee Security Awareness has a significant positive effect on Security Protection Behavior (path c: $\beta = 0.431$, $p = 0.000$), consistent with the earlier findings that awareness enhances employees' cybersecurity behavior.

When Threat Appraisal was included in the model, Employee Security Awareness remained significant (path c': $\beta = 0.482$, $p = 0.000$), while Threat Appraisal showed a significant positive effect on Security Protection Behavior (path b: $\beta = 0.320$, $p = 0.000$). This indicates that employees who perceive higher levels of cybersecurity threats are more likely to engage in protective behaviors. Additionally, the increase in R^2 from 0.186 to 0.468 demonstrates that including Threat Appraisal improves the explanatory power of the model, confirming its mediating role.

Table 5

Mediation Analysis: Threat Appraisal as a Mediator between Employee Security Awareness and Security Protection Behavior

Model	Variable	R^2	Unstandardized Coefficients (β)	Std. Error	Beta	t-value	p-value	Interpretation
1	(Constant)	0.186	4.363	0.315	—	13.873	0.000	Significant
	Employee Security Awareness		0.525	0.074	0.431	7.103	0.000	Significant
2	(Constant)	0.468	1.229	0.236	—	5.196	0.004	Significant
	Employee Security Awareness		0.398	0.045	0.482	8.849	0.000	Significant
	Threat Appraisal		0.217	0.037	0.320	5.878	0.000	Significant

R^2 change = 0.282 Sig. F change = < .001 (Significant)

This suggests that Coping Appraisal partially mediates the relationship between Employee Security Awareness and Security Protection Behavior. In other words, employee awareness not only directly influences security behavior but also indirectly affects it by enhancing individuals' ability to respond effectively to cybersecurity threats, such as their confidence in applying security measures and their belief in the effectiveness of those actions.

This finding is supported by studies emphasizing that coping-related factors play a crucial role in motivating protective behavior. Princely Ifinedo (2022) highlighted that self-efficacy and response efficacy significantly influence employees' compliance with cybersecurity practices. Similarly, A. Sulaiman et al. (2022) found that coping appraisal components, particularly self-efficacy, strongly predict individuals' intention to adopt secure behaviors. Ben Hanus and Yichun Wu (2023) also demonstrated that individuals who believe in their ability to mitigate cyber risks are more likely to engage in proactive security actions.

In addition, Abdullah AlHogail (2023) emphasized that both awareness and coping mechanisms are essential human factors in strengthening organizational cybersecurity behavior. These findings align with recent applications of Protection Motivation Theory, which confirm that individuals are more likely to adopt protective actions when they perceive themselves as capable of performing the behavior and believe that the response will effectively reduce cyber threats.

To further examine the mediating role, the Sobel test was conducted. The results confirmed that Threat Appraisal partially mediates the relationship between Organizational Information Security Effort and Security protection motivational behavior ($Z = 4.520$, $p < .001$), indicating a significant mediation effect. This means that part of the influence of organizational effort on security behavior operates through employees' perception of threats, while the direct effect remains significant, confirming partial mediation.

Mediating Effect of Coping Appraisal on the Relationship between Employee Security Awareness and Security Protection Motivational Behavior

Table 6 presents the mediation analysis examining whether Coping Appraisal mediates the relationship between Employee Security Awareness and Security Protection Behavior. The results show that Employee Security Awareness has a significant positive effect on Security Protection Behavior ($\beta = 0.514$, $p = 0.000$), consistent with the earlier findings that increased awareness enhances employees' engagement in cybersecurity practices. Coping Appraisal, in turn, has a significant positive effect on Security Protection Behavior ($\beta = 0.195$, $p = 0.001$), indicating that individuals who are more confident in their ability to respond to cybersecurity threats are more likely to perform protective behaviors. When Coping Appraisal was included in the model, Employee Security Awareness remained significant ($\beta = 0.520$, $p = 0.000$), suggesting that the mediation is partial. The increase in explanatory power from $R^2 = 0.264$ to $R^2 = 0.413$ further supports the contribution of Coping Appraisal in strengthening the model.

Table 6

Mediation Analysis: Coping Appraisal as a Mediator between Employee Security Awareness and Security Protection Behavior

Model	Variable	R^2	Unstandardized Coefficients (β)	Std. Error	Beta	t-value	p-value	Interpretation
1	(Constant)	0.264	5.675	0.42	—	13.496	0.000	Significant
	Employee Security Awareness		0.88	0.099	0.514	8.902	0.000	Significant
2	(Constant)	0.413	1.644	0.245	—	6.700	0.00	Significant
	Employee Security Awareness		0.430	0.050	0.520	8.638	0.000	Significant
	Coping Appraisal		0.094	0.029	0.195	3.230	0.001	Significant

R^2 change = 0.149 Sig. F change = < .001 (Significant)

To examine whether Coping Appraisal mediates the relationship between Employee Security Awareness and Security protection motivational behavior, a mediation analysis was conducted. Results presented in Table 9 show that Employee Security Awareness has a significant effect on Security protection motivational behavior ($\beta = 0.514$, p-value < .05). When Coping Appraisal was included in the model, the

explanatory power increased from $R^2 = 0.264$ to $R^2 = 0.413$, indicating an improvement in the model. Employee Security Awareness remained a significant predictor of Security protection motivational behavior ($\beta = 0.520$, p-value < .05). In addition, Coping Appraisal was found to be significantly related to Security protection motivational behavior ($\beta = 0.195$, p-value < .05). Since Employee Security Awareness remains significant even after including Coping Appraisal, this indicates that Coping Appraisal partially mediates the relationship between Employee Security Awareness and Security protection motivational behavior. This suggests that employees' awareness not only directly influences their security behavior but also indirectly influences it by improving their coping ability in handling cybersecurity threats.

To further examine the mediating role, the Sobel test was conducted. The results confirmed that Coping partially mediates the relationship between Organizational Information Security Effort and Security protection motivational behavior ($Z = 3.045$, $p < .01$), indicating a significant mediation effect. This means that part of the influence of organizational effort on security behavior operates through employees' coping mechanisms, while the direct effect remains significant, confirming partial mediation.

C. Conclusion

This study investigated the effect of Organizational Information Security Effort on Employee Security Awareness and Security Protection Motivational Behavior, with Threat Appraisal and Coping Appraisal examined as mediating factors in the context of a manufacturing organization. The research aimed to understand how organizational initiatives and individual awareness, together with cognitive appraisal processes including perceived severity, perceived vulnerability, response efficacy, self-efficacy, and response cost affect employees' cybersecurity behavior.

Results show that Organizational Information Security Effort has a significant positive effect on Employee Security Awareness; therefore, the study rejects H_{01}. Furthermore, Employee Security Awareness has a significant positive effect on Security Protection Motivational Behavior, indicating that increased awareness leads to improved cybersecurity practices among employees. The mediation analysis revealed that both Threat Appraisal and Coping Appraisal significantly influence Security Protection Motivational Behavior, confirming their important role in shaping employees' protective actions. Thus, the study rejects H_{02} and H_{03}.

The mediation analysis further revealed that Threat Appraisal and Coping Appraisal partially mediate the relationship between Employee Security Awareness and Security Protection Motivational Behavior, indicating that the influence of awareness on behavior is both direct and indirect through cognitive processes. The R^2 values showed that including these mediators substantially increases the explained variance in Security Protection Motivational Behavior, reinforcing the critical role of cognitive appraisal mechanisms in translating awareness into actual protective behavior.

These findings suggest that organizations seeking to improve cybersecurity behavior should prioritize strengthening both organizational security efforts and employee awareness while also enhancing employees' perception of threats and their ability to respond effectively. While organizational initiatives

and awareness are significant drivers, other organizational and behavioral factors may also influence cybersecurity outcomes, highlighting the need for a comprehensive and integrated approach to information security management.

D. Recommendations

Based on the findings of this study, the following recommendations are proposed to guide the improvement of cybersecurity behavior through Organizational Information Security Effort, Employee Security Awareness, and cognitive appraisal mechanisms:

Strengthen Organizational Information Security Efforts

Organizations are strongly encouraged to continuously enhance their cybersecurity initiatives, including the implementation of clear policies, regular training programs, and strict enforcement mechanisms. These efforts should be consistently updated to address emerging cyber threats and ensure that employees remain well-informed and compliant with security standards.

Enhance Employee Security Awareness Programs

Given the significant effect of awareness on behavior, organizations should invest in more interactive and practical awareness programs. This includes phishing simulations, scenario-based training, and continuous education campaigns that improve employees' ability to recognize and respond to cybersecurity threats in real-world situations.

Improve Threat Appraisal Among Employees

Organizations should focus on strengthening employees' perception of cybersecurity risks by emphasizing the seriousness (severity) and likelihood (vulnerability) of cyber threats. This can be achieved through awareness campaigns, real-life case studies, and incident-sharing sessions that highlight the potential consequences of security breaches.

Strengthen Coping Appraisal Factors

To enhance employees' ability to respond to threats, organizations should improve response efficacy and self-efficacy by providing hands-on training, user-friendly security tools, and clear procedural guidelines. At the same time, efforts should be made to reduce response costs by simplifying security processes and minimizing inconvenience in following security practices.

Promote a Strong Cybersecurity Culture

Organizations should foster a culture that prioritizes cybersecurity by encouraging accountability, open communication, and proactive reporting of security incidents. Management support is essential in reinforcing secure behavior and integrating cybersecurity into daily work practices.

Integrate Behavioral and Technical Security Strategies

Organizations should not rely solely on technical solutions but should integrate behavioral approaches that address human factors. Combining organizational effort, awareness, and cognitive motivation will result in more effective and sustainable cybersecurity practices.

For Future Researchers

Future researchers are encouraged to further explore cybersecurity behavior by examining additional variables such as organizational culture, leadership support, and technological infrastructure. They may also consider using longitudinal research designs or different industry settings to enhance the generalizability and depth of findings.

E. Limitations of the Study

Despite the valuable findings of this study, several limitations should be acknowledged. First, the study was limited to a specific group of respondents within a particular organization, which may restrict the generalizability of the results. The findings may not fully represent employees from other industries or organizations with different cybersecurity practices and work environments.

Second, the study relied on self-reported data, which may be subject to response bias. Participants may have provided socially desirable answers, especially when reporting their security behaviors and awareness. This may have affected the accuracy of the data, as actual behavior may differ from reported behavior.

Third, the study used a cross-sectional research design, meaning that data were collected at a single point in time. Because of this, the study cannot fully establish causal relationships between the variables. While significant relationships were identified, changes over time and long-term effects were not captured.

Additionally, the study focused only on selected variables such as Organizational Information Security Effort, Employee Security Awareness, Threat Appraisal, and Coping Appraisal. Other factors, such as organizational culture, leadership support, peer influence, or technological infrastructure, were not included but may also play an important role in influencing security protection behavior.

Lastly, time and resource constraints may have limited the scope of data collection and analysis.

AI DECLARATION

Research Stages	**AI Use**
Conception	Google Scholar and ChatGPT was used to assist in creating an outline of the Review of Related Literature.
Gathering of Data	The author did not use AI to gather data.
Processing of Data	The author did not use AI to process, code, and categorize the data.

Analysis of Data	The author used Excel in counting the frequency of the demographic profile of respondents and in frequency tables.
Reporting	The author did not used AI to check for grammar, punctuation and spelling errors in the manuscript.

References

Ahmad, A., Maynard, S. B., & Desouza, K. C. (2022). Information security strategies: Towards an organizational multi-strategy perspective. *Journal of Strategic Information Systems, 31*(2), 101705.

Alhanatleh, H., Khaddam, A. A. H., Abudabaseh, F., Alghizzawi, M., & Alzghoul, A. (2024). Factors influencing cybersecurity awareness in mobile financial technology services. *Journal of Financial Technology and Security, 8*(1), 45–62.

AlHogail, A. (2023). Improving cybersecurity behavior in organizations: The role of awareness and human factors. *Computers & Security, 124*, 103025.

Al-Mhiqani, M. N., Ahmad, R., Yassin, A. A., & Abidin, Z. Z. (2025). Information security behavior of healthcare professionals based on protection motivation theory. *Scientific Reports, 15*, 26917.

Alshaikh, M. (2022). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security, 112*, 102515.

Alshaikh, M. (2023). Human factors in cybersecurity: A systematic literature review. *ACM Computing Surveys, 55*(4), 1–36.

Alvarez, M. (2024). Cybersecurity threats in the manufacturing sector. *The Business Research Company*.

Comparitech. (2024). Ransomware attacks on manufacturing companies: Global report.

De Kimpe, L., Walrave, M., Verdegem, P., & Ponnet, K. (2021). What we think we know about cybersecurity: An investigation of perceived knowledge, vulnerability, and protective behavior. *Cyberpsychology, Behavior, and Social Networking, 24*(3), 157–165.

Donalds, C., & Osei-Bryson, K. M. (2025). Causal and descriptive analytics in information systems research. *Journal of Decision Systems, 34*(1), 1–18.

Han, J., Smith, K., & Lee, H. (2025). Protection motivation and cybersecurity intentions: Understanding human factors in organizational security. *Journal of Information Security Research, 14*(2), 45–62.

Hanus, B., & Wu, Y. (2023). Impact of users' security awareness on phishing threat avoidance behavior: A protection motivation theory approach. *Information & Computer Security, 31*(2), 235–252.

Hussain, S., & Wider, W. (2022). Cybersecurity behavior among government employees: The role of protection motivation theory. *Information, 13*(9), 413.

Ifinedo, P. (2022). Understanding information systems security policy compliance: An integration of the theory of planned behavior and protection motivation theory. *Computers & Security, 121*, 102826.

Indino, J. (2024). Cybersecurity threats in Philippine industries. *Kaspersky Security Reports*.

Jones, K., Johnson, D., & Smith, R. (2022). User perceptions of cybersecurity risk and protection behavior. *Information & Computer Security, 30*(2), 210–225.

Khan, N. A., Brohi, S. N., & Zaman, N. (2022). Ten deadly cybersecurity threats amid COVID-19 pandemic. *TechRxiv*.

Kiran, R., Rustandi, A., & Li, W. (2025). Human-centered cybersecurity in manufacturing: Threat appraisal, coping appraisal, and protective behavior. *International Journal of Cybersecurity Studies, 9*(1), 1–20.

Li, L., He, W., & Xu, L. (2023). Influencing factors of employees' information security behavior: An integrated model. *Computers & Security, 124*, 102976.

Li, L., Xu, L., & He, W. (2022). The effects of antecedents and mediating factors on cybersecurity protection behavior. *Journal of Computer Information Systems, 62*(3), 405–417.

Moody, R. (2024). Manufacturing ransomware trends and impacts. *Cybersecurity Review Quarterly, 6*(1), 18–26.

Nunnally, J. C., & Bernstein, I. H. (1994). *Psychometric theory* (3rd ed.). McGraw-Hill.

Pan, G. (2024). Quantitative research methods in information security studies. *International Journal of Research Methodology, 17*(2), 89–104.

Rahman, M. S., Hossain, M. A., & Islam, M. R. (2024). Exploring the interplay of privacy concerns, mobile cybersecurity awareness, and protective motivation behavior. *International Journal of Information Management Data Insights, 4*(1), 100186.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The 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: A sourcebook* (pp. 153–176). Guilford Press.

Rohan, R., Pal, D., Hautamäki, J., Funilkul, S., & Thapliyal, H. (2023). A systematic literature review of cybersecurity scales assessing information security awareness. *Heliyon, 9*(3), e14234.

Rustandi, A. (2025). Cybersecurity in industrial operations: Human factors and organizational resilience. *Journal of Industrial Security, 12*(3), 15–31.

Shaikh, F. A., & Siponen, M. (2024). Cybersecurity investment decisions and performance feedback mechanisms. *Information & Management, 61*(1), 103742.

Sisodia, S. (2024). Human error and cybersecurity breaches: A global analysis. *International Journal of Cybersecurity Studies, 9*(1), 33–47.

Sulaiman, A., Salleh, N., & Ariffin, M. (2022). Determinants of cybersecurity behavior among employees using protection motivation theory. *Journal of Information Security and Applications, 65*, 103092.
Tambariki, C., Sondakh, O. B., Dondokambey, V. A., & Hendriana, E. (2024). Drivers of banking consumers' cybersecurity behavior: Applying extended protection motivation theory. *GATR Journal of Management and Marketing Review, 9*(1), 1–12.
Tsohou, A., Karyda, M., & Kokolakis, S. (2023). Evaluating protection motivation-based cybersecurity awareness training. *Computers & Security, 125*, 103049.
White, G. R. T., Allen, R. A., Samuel, A., Abdullah, A., & Thomas, R. (2022). Cybersecurity readiness and organizational antecedents: Evidence from SMEs. *Journal of Small Business and Enterprise Development, 29*(6), 905–924.
Yılmaz, A., & Ünal, Z. (2024). Impact of information security awareness on information security compliance of academic library staff. *Journal of Academic Librarianship, 50*(5), 102937.