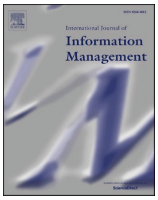
International Journal of Information Management 66 (2022) 102520

Contents lists available at ScienceDirect

International Journal of Information Management

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



Research article

The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities

Lai-Wan Wong[a,b], Voon-Hsien Lee[c], Garry Wei-Han Tan[d,e,h,*], Keng-Boon Ooi[d,e,f,*], Amrik Sohal[g]

[a] *School of Computing and Data Science, Xiamen University Malaysia, Malaysia*
[b] *Center for Advanced Computing and Telecommunications, Malaysia*
[c] *Faculty of Business and Finance, Universiti Tunku Abdul Rahman, Kampar, Malaysia*
[d] *UCSI Graduate Business School, UCSI University, Kuala Lumpur, Malaysia*
[e] *Nanchang Institute of Technology, Jiangxi, China*
[f] *College of Management, Chang Jung Christian University, Tainan City, Guiren District, Taiwan*
[g] *Faculty of Business and Economics, Monash University, Australia*
[h] *School of Graduate Studies, Asia e University, Subang Jaya, Malaysia*

ARTICLE INFO

Keywords:
Cybersecurity awareness
Small medium enterprises
Supply chain attack
Resilience
Cybersecurity policy
COVID-19

ABSTRACT

This paper investigates the role of general cybersecurity and cybersecurity policy awareness in enhancing supply chain cyber resilience reactive capabilities. Theorizing from the Protection Motivation Theory, 200 Small and Medium Enterprises (SMEs) were contacted to understand their perception of cybersecurity and policy awareness in affecting their overall cybersecurity hygiene. Data collection was carried out using a questionnaire survey and analysed via Partial Least Squares-based Structural Equation Modelling to validate the research framework. Results of analysis outlined the importance of general cybersecurity and policy awareness in shifting employees' compliance attitude towards enhancing supply chain reactive capability. Using a mixed-method approach, post-survey interviews were further conducted with practitioners in SMEs to understand the study findings. The implications outlined in this study emphasises the importance of prioritising preventive measures and proper employee cyber hygiene to address the risk and loss following a cyber-attack. Key supply chain operational areas in SMEs are still largely supported by the human workforce serving as its backbone. An unwarranted attack could cause adverse business impacts. Thus, practitioners and SMEs would be alerted to the critical need for a robust security posture and that SMEs' need of the hour lies at the core of its policy and employee cybersecurity hygiene.

1. Introduction

The COVID-19 pandemic represents a profound disruption to global supply chains (SCs) across various industries (Araz et al., 2020; Queiroz et al., 2020; Schleper et al., 2021). According to Ghadge et al. (2019), the backbone of SCs is an "evolving technological ecosystem" (2019, p. 224) in which emerging technologies such as the Internet of Things, blockchain, and artificial intelligence have altered the relationships among SC partners. Unlike traditional SCs, an SC that uses technological systems to satisfy customer requirements—systems which comprise of networks and technologies used to connect and share data—poses new forms of modern security implications to enterprises. This effect has been even more pronounced during the onset of the pandemic, which necessitated a radical change in the way enterprises function (Dwivedi et al., 2020) and caused some 300 million workers globally to work from home. This transition brings new cybersecurity vulnerabilities to many firms (data security risks, hacking attempts, phishing, ransomware, etc.) and remote working adds to the complexity of fielding cybersecurity threats (Chapman, 2020; Coden et al., 2020). Cybercriminals have leveraged this opportunity not only to prey on users via a series of indiscriminate and targeted threats; working from home revealed the unpreparedness of many vendors where their security products are concerned (Lallie et al., 2021). Additionally, work from home *en-masse* meant a surge in the use of digital technologies (Rahul De' et al., 2020).

* Corresponding authors at: UCSI Graduate Business School, UCSI University, Kuala Lumpur, Malaysia.
E-mail addresses: wlaiwan@cact.asia (L.-W. Wong), leevoonhsien@gmail.com (V.-H. Lee), garrytanweihan@gmail.com (G.W.-H. Tan), ooikengboon@gmail.com (K.-B. Ooi), amrik.sohal@monash.edu (A. Sohal).

https://doi.org/10.1016/j.ijinfomgt.2022.102520
Received 6 May 2021; Received in revised form 24 April 2022; Accepted 24 April 2022
Available online 6 May 2022

Researchers such as Hijji and Alam (2021) and Lallie et al. (2021), who have analyzed the pandemic from a cyber-attack perspective, show that the range of cyber-attacks experienced globally heightened during the pandemic. They also reveal that the anxiety caused by the pandemic increased the likelihood of an attack.

Despite this, scholars have shown that employees can be great assets in reducing security-related risks (Esteves et al., 2017; Jalali et al., 2019; Wiley et al., 2020). Employees with the right competencies (coupled with the right organizational design) can better anticipate and respond to potential cybersecurity threats. Unfortunately, this may not be the case for Small and Medium Enterprises (SMEs). Extant literatures have already outlined that SMEs tend to fall short when it comes to cybersecurity concerns and preparedness (Lewis et al., 2014; Nycz et al., 2015). Common reasons given for this include a lack of awareness, expertise, and resources (Bada & Nurse, 2019; Paulsen, 2016); high time pressure when multiple tasks must be juggled; and races to meet tight deadlines (Chowdhury et al., 2019). Further, there are limited studies on this context (Kabanda et al., 2018). According to Wong, Leong et al. (2020), SMEs should not rely on traditional processes—they must instead view technology as an investment for sustainable growth. Many SMEs have difficulty addressing the digitalization gap for productivity and business gains despite achieving a high level of computerization of their processes. It can be inferred from these findings, and from the research of Benz and Chatterjee (2020) and Papadopoulos et al. (2020), that SMEs would not have the technological resources to prepare themselves from external threats. As such, they would be vulnerable in terms of cybersecurity risks and resilience during the pandemic. Without proper risk mitigation, incident response planning, and good cybersecurity awareness, the cost of managing cyber risks in the event of a breach or attack would be high.

The heightened security risks caused by remote work in response to COVID-19 require companies to go beyond protecting their most critical assets (Bates, 2020). Additionally, restrictions on travel have increased demand on digital channels. Systems and services need to be scaled up to deal with these changes in demand. Many questions have arisen: can SMEs function effectively through remote working? Is there a need to relax access controls or provide additional remote login credentials? Is there sufficient help desk capacity for employees unfamiliar with remote logins? In an extended, mass work-from-home scenario, are software vendors prepared and able to provide adequate support? Organized adversarial groups are leveraging public fear of COVID-19 to execute targeted spear-phishing campaigns. Hence, SMEs need to examine and redesign their approach to security operations during the pandemic.

The purpose of this study henceforth is to understand cybersecurity awareness and good practices among employees of SMEs in Malaysia, as well as how their security-related behaviors help to build SC reactive capability in the face of a crisis. The goal of this paper is to understand the attitude of employees in adopting cybersecurity behaviors to improve SC resilience. This paper continues in Section 2 with a review of past literature related to this work. Section 3 then discusses the research model and hypotheses of this study, followed by the research instrument (in Section 4). The methodology and analysis are included in Section 5, while the theoretical and practical implications are presented in Section 6. Finally, Section 7 concludes with a discussion on possible future research that can be developed.

2. Literature review

2.1. The Protection Motivation Theory (PMT) and cybersecurity awareness

According to Connolly et al. (2017), the enforcement of behavioral rules governing incident reporting procedures, adherence to policies, and the dissemination of information extends beyond technical tools. An employee's roles and responsibilities in safeguarding the resources of their organizations are usually highlighted in their firm's policy on security (Bulgurcu et al., 2010). However, adherence to these rules (or compliance) depends on employees' motivation to conform. This study understands *compliance* as the degree to which an individual acts in accordance with prescribed rules or requests made by people in authority.

The Protection Motivation Theory (PMT) (Rogers, 1975) examines threat appraisal together with coping appraisal processes in influencing behaviors of protection and, subsequently, security behaviors (Boss et al., 2015). PMT is the most widely adopted theory in behavioral security studies (Wall & Warkentin, 2019). It can be explained in terms of a process that begins with the receipt of information. This then leads to the use of the information to execute an action, depending on the individual's subjective evaluation (or perception) and interpretation (Jaeger & Eckhardt, 2021). During their threat appraisal, individuals form beliefs regarding the degree of threat existing in the situation. They also generate a perceived threat which includes the following dimensions: the threat's perceived severity (PTS), vulnerability (PTV) and response efficacy (EFF). According to Jaeger and Eckhardt (2021), PTS is the individual's belief about the seriousness of the threat's consequences and PTV is the individual's appraisal of their own likelihood to experience a threat. This appraisal then leads to the formation of a subjective notion on how well the individual can cope with the threat (coping appraisal) and EFF refers to the individual's belief that the recommended behavior will be effective in reducing the threat. Empirical studies in security that have applied PMT include antecedents to threats appraisals (Hanus & Wu, 2016; Martens et al., 2019), the convincing of users to protect themselves (Shillair et al., 2015), and alignment with other theories (Herath & Rao, 2009; Ifinedo, 2011). Despite wide applications of PMT, results have been inconsistent. Menard et al. (2017) attribute this to the fact that, within security, threats are most often against the assets of organizations rather than individual assets. Therefore, there is a lack of perceived personal relevance (Johnston et al., 2015). Another possibility could be studies' omission of the role of attitude (Bélanger et al., 2017). PMT relies on intrinsic motivation to protect, which results from perceived threat. Motivation arouses, sustains, directs, and influences a user's compliant attitude (Menard et al., 2017).

In this study, we integrate employee cybersecurity awareness (CA) as an explicit measure. This allows our research to further investigate employee attitudes toward protection, and understand the gap that exists in PMT-based security research. As per Zwilling et al. (2020) and Jaeger and Eckhardt (2021), the term CA in the context of this study refers to the degree of understanding users have of the importance of cybersecurity and their responsibilities regarding it. It also includes their possession of enough knowledge about existing policies to exercise sufficient levels of cybersecurity control, in order to protect their organization's data and network. Lack of awareness is one of the key reasons for noncompliance (Bulgurcu et al., 2010; Donalds & Osei-Bryson, 2020; Hu et al., 2007).

Hina et al. (2019) show that institutional governance is a significant motivator of employees' protection behavior in policy compliance. Employees are influenced by the firm's security environment in coping with threat appraisal abilities. This also contributes to their compliance behavior (Li et al., 2019). In other words, policies and educational initiatives can increase employee awareness, which in turn can help them to better understand the impact of their actions. This fortifies the "human firewall." Finally, according to Chang and Coppel (2020), security awareness must be professionally prepared. When people are willing to change, training and feedback must be continuously provided in order to successfully sustain the change period. If this consciousness leads to new legislation and inclusion in training programmes, the awareness programme is considered effective and sustainable. The importance of a security culture is further echoed by Wiley et al. (2020) whose study finds that firms can achieve greater security awareness through understanding and strengthening their security culture. Similarly, Balapour et al. (2020) show that awareness moderates the effect of perceived risk on perceived security.

2.2. Supply chains in times of crisis

SCs are not immune to disruptions (Chen et al., 2019). Firms have to be prepared to detect and respond by gathering the experiences of others, identifying successful strategies and practices, and having the right resources (such as employee preparedness and adequate investments in IT tools and analytics capabilities). According to Ivanov and Dolgui (2020), there are three aspects by which SC reaction to disturbances can be analyzed. The first refers to the SC's ability to return to a pre-disruption state to remain functional. *Stability* is a desired property of this network, whereby inventory levels gradually return to pre-established levels following disruptions (Demirel et al., 2019). Next is *resilience*. This refers to the desired state in a performance objective set within a time window (Hosseini et al., 2019). In this paper, the term *resilience* is used in the context of the SC's capability to recover from disruptions. The third aspect is the *robustness* of the SC, which spells out its ability to maintain planned performance via its capability to withstand disruptions with minimal impact in its performance (Zhao et al., 2019). Depending on the context, SCs should be reactive—responding dynamically to changes in the environment—as well as proactive, so as to satisfy customer needs (Chowdhury & Quaddus, 2017).

Although SMEs and their post-disaster policy needs have been a subject of interest for many scholars (Dahles & Susilowati, 2015; Wedawatta & Ingirige, 2012), studies on the impact of epidemics on SMEs are rare (Lu et al., 2020). The COVID-19 crisis offers both upheavals and opportunities (Sarkis, 2020). Demand and supply ripples are observed and widely reported—chaos propagated across global networks. With consumption patterns shifting to digital channels, and resonance occurring in hoarding situations, it is timely to consider what it means for an SC to remain resilient and sustainable. Would stocking more inventory be more expensive and result in greater waste? The answer to this and other questions would allow firms to address situations and adjust in response to the COVID-19 crisis. COVID-19 outcomes related to technological and social innovations can alter how SCs work and redefine the understanding of SC sustainability. Hence, the importance of managing SC risks and impacts could not be underestimated; firms must execute immediate actions to contain impacts and restore operations as soon as possible (Chen et al., 2019; He et al., 2022; Ivanov, 2020a; Kinra et al., 2019).

The success of SME's SC reactive capability (REC) and capacity to rise to both internal and external challenges—in order to ensure uninterrupted operations—is mainly driven by the SC's resilience and reactive capability to mitigate risks (Abeysekara et al., 2019; Hohenstein et al., 2015). Urgent decisions must be made to mitigate the adverse effects of delays and firms must remain vigilant to any escalations and uncertainties in the SC (Dwivedi et al., 2020). This means that firms need to address the needs of their employees, consumers, and suppliers as well as alleviate any reputational effects of SC disruptions (Shaheen et al., 2019). As a result of many unexpected events, SCs' recovery capacity post disruption has garnered extensive attention among scholars (Ivanov & Dolgui, 2020; Ivanov et al., 2019; Ivanov, Dolgui et al., 2017; Kim & Bui, 2019).

2.3. Cybersecurity within supply chains

Extant literature has yet to address the implications of cybersecurity threats at the SC level (Ghadge et al., 2019; Urciuoli & Hintsa, 2017; Xue et al., 2013). Cybersecurity in SCs typically covers a wide spectrum—-from sourcing, vendor management, SC continuity and quality, and transportation security, to further functions that require a coordinated effort. It is a problem that does not solely lie in the technological domain. It also concerns people, processes, and knowledge (Boyens et al., 2020; NIST, 2015). In the case of SMEs, digitalization exposes them to cybersecurity threats from adversaries. Despite having acknowledged the need for SMEs to enhance their cybersecurity understanding (Bada & Nurse, 2019), past research studies have shown that internal factors such as budget, management support, technology complexity, attitudes towards security (Kabanda et al., 2018), and awareness and expertise (Bada & Nurse, 2019) influence SMEs' perception of cybersecurity.

Furthermore, information technology (IT) security systems would not be effective in securing information and intellectual property unless employees adopted cybersecurity best practices (Boyens et al., 2020). They could either willingly or accidentally pose a threat to the company via various means (Urciuoli & Hintsa, 2017). Encouraging good security behavior by employees and developing a security culture can therefore help firms to improve their overall security. However, ways to best encourage good security behavior are less understood (Bada & Nurse, 2019). This has resulted in some SMEs not engaging in security-related training, and not knowing how to avoid security fatigue. In Malaysia, deciding factors on the adoption and use of technology remain "centred between human, and technology" (Wong & Tan, 2020; Wong, Leong et al., 2020, p. 16). Although existing literature is replete with studies that examine different types of risks and mitigation strategies for SC security and disruptions, a significant gap remains (Simon & Omar, 2020).

Security issues must be considered a consequence of human actions (Coles-Kemp & Hansen, 2017). According to Woltjer (2017), the workforce often undermines security compliance through a lack of awareness, leading to new vulnerabilities. This problem goes beyond SMEs. According to Sadok et al. (2020), SME work systems comprise of material procurement, production or services delivery, customer servicing, and many other functions that can be viewed as a sociotechnical or completely automated system. Expectations around management concerns (e.g., task performance, reducing threat vulnerability) and customer interests may not align. In Sadok et al.'s study, 63% of interviewed respondents revealed that they do not consider security a priority while at work. In addition, 53% of respondents who handle sensitive data said that their job does not necessitate meticulous security practices. These findings are coherent with Sadok et al.'s work system framework, implying that work system participants normally prioritize task performance over following security guidelines.

Consequently, the SC becomes a vulnerable attack vector. COVID-19 has caused a large number of people to work from home, and there has been a surge in the use of digital technologies (Rahul De' et al., 2020). Cybercriminals are set to exploit the situation with various scams and attacks such as phishing, ransomware, and increased misinformation surrounding COVID-19 (Dwivedi et al., 2020; Lallie et al., 2021). Hence, SMEs must evolve their cybersecurity reporting practices, policies, and controls to protect themselves and manage information sharing if they wish to prevent the SC from further damage.

3. Theoretical background and hypothesis

Prior research had been carried out from the perspective of resilience in SC at times of crisis (Hosseini et al., 2019; Ivanov et al., 2017, 2019; Ivanov, 2020a) and of cybersecurity practices in SCs/SMEs (Colicchia et al., 2019; Kabanda et al., 2018; Lewis et al., 2014; Paulsen, 2016; Santos-Olmo et al., 2016; Simon & Omar, 2020). General cybersecurity awareness (GCA) and general policy awareness (GPA) have been analyzed in the context of SC operations of SMEs during times of crisis, where they could play a strategic role in firms' understandings of how to invest their efforts in security.

This work aims to support SMEs as they seek to understand the extent to which they should invest their efforts in SC cybersecurity 'good' practices. Our paper does this by exploring the role of cybersecurity awareness (CA) in an employee's compliant or non-compliant behavior regarding cybersecurity policies. We seek to shed light on two key areas: (i) whether employees are cognizant of cybersecurity risks, and (ii) their knowledge of their roles and responsibilities. This motivation shapes their security attitude, which in turn affects the SC reactive capability due to operational vulnerabilities. Against the backdrop of PMT, this study posits that CA influences an employee's attitude toward compliance with cybersecurity policies in accordance with to the severity of the perceived threats and inherent risks. Fig. 1 presents our conceptual model and the sections that follow discuss the formation of hypotheses in this study.

3.1. Cybersecurity awareness

According to Bulgurcu et al. (2010), security awareness plays an important role in understanding the vulnerability of work resources. It is a principal predictor of attitudinal and outcome beliefs for policy compliance. Chen et al. (2015) show that awareness programmes influence security culture in organizations. Similarly, Hanus and Wu (2016) prove that the awareness of threats is a positive indicator of perceived severity, and knowledge of how to counter threats is a positive predictor of response efficacy.

Further, assumptions about user awareness have been challenged by studies on behavioral aspects of phishing and other types of attacks (Jaeger & Eckhardt, 2021; Stacey et al., 2021). Hence, the question of why users fall for such phishing attempts—and whether the action was a result of deliberate thought—remain unanswered. We posit that this gap has not been fully addressed because awareness can be triggered by system warnings, based on an individual's experience level, emotions, or contextual factors such as whether the content of a malware email is aligned to the user's work content. Thus, we hypothesize:

Hypothesis 1. : Cybersecurity Awareness positively influences employees' Perceived Threat Severity (PTS) of cybersecurity incidences.

It is important that employees comprehend their vulnerabilities to breaches, in order to cultivate the motivation to protect institutional assets (Hina et al., 2019). Being aware of a particular threat can lead to a better assessment of one's likelihood of falling for such attacks. Users who are less aware of a security-related situation will underestimate the likelihood of falling prey to an impending attack. If users are aware of the situation, they will evoke an appropriate coping process.

Indeed, one reason individuals exhibit differential concerns about certain phenomena is their varying levels of awareness. According to Balapour et al. (2020), an individual's awareness is increased with more information. This can be obtained by reading, observing, and hearing about security issues. The level of awareness one has influences one's security-related perceptions, which then stimulates protective behavior. Therefore, we posit that awareness increases or decreases the strength of one's perceived vulnerability towards a particular security-related phenomenon. Hence, we hypothesize:

Hypothesis 2. : Cybersecurity Awareness positively influences employees' Perceived Threat Vulnerability (PTV) of cybersecurity incidences.

Some researchers have also considered policy awareness in determining policy compliance and response efficacy. Security policies define the codes of conduct that are implemented to match ongoing problems and counteractions. Elements of threats and fears are integral to policies which seek to motivate employee compliance (Boss et al., 2015; Johnston et al., 2015). Additionally, policies play a pivotal role in cultivating a cultural sense of security (Y. Chen et al., 2015).

Although policy compliance is still considered difficult to achieve (despite frequent awareness attempts) (Hina et al., 2019), motivating employees to adopt protective behavior remains a major organizational challenge (Siponen et al., 2014). In many instances, employees lack compliance with procedures and guidelines designed to counter threats despite policies in place (Ifinedo, 2014). Past studies have shown that lack of awareness is a reason for employee noncompliant behavior (Bélanger et al., 2017; Bulgurcu et al., 2010; Hu et al., 2007). However, forcing individuals into compliance can create undesired effects (Bélanger et al., 2017). Nevertheless, according to Li et al. (2019), employees who are more aware of their company's policy are more competent in managing security tasks. Li et al.'s study indicates that an informed employee positively contributes to their compliance behavior via heightened appraisal and coping abilities. In this study, we hypothesize:

Hypothesis 3. : Cybersecurity Awareness positively influences employees' Response Efficacy (EFF) for cybersecurity incidences.

3.2. Protection Motivation Theory (PMT) and attitude (ATT)

The PMT model consists of threat and coping appraisal processes. Threat appraisal includes PTS and PTV when employees face cyberattacks. It describes how employees assess the level of danger posed by a threat (Li et al., 2019). PMT presumes an individual who, upon evaluating the severity of a particular threat, also considers the likelihood of such a threat affecting himself/herself. For example, during the COVID-19 pandemic, an employee who perceives the threat of phishing attacks to be high would accordingly experience an increase in their belief and in their compliant intention to effectively address the threat. Much empirical evidence lends sustenance to these hypotheses (Ifinedo, 2012; Menard et al., 2018; Siponen et al., 2014).

However, some studies have also highlighted the overlap between severity and vulnerability, arguing that both represent a risk to the employee (Ameen et al., 2021; Ifinedo, 2012). This overlap is attributed to differences in previous studies' conceptualization of severity. For example, Ameen et al. (2021) argue that the severity of adverse consequences in some studies does not play a role in all security, and that

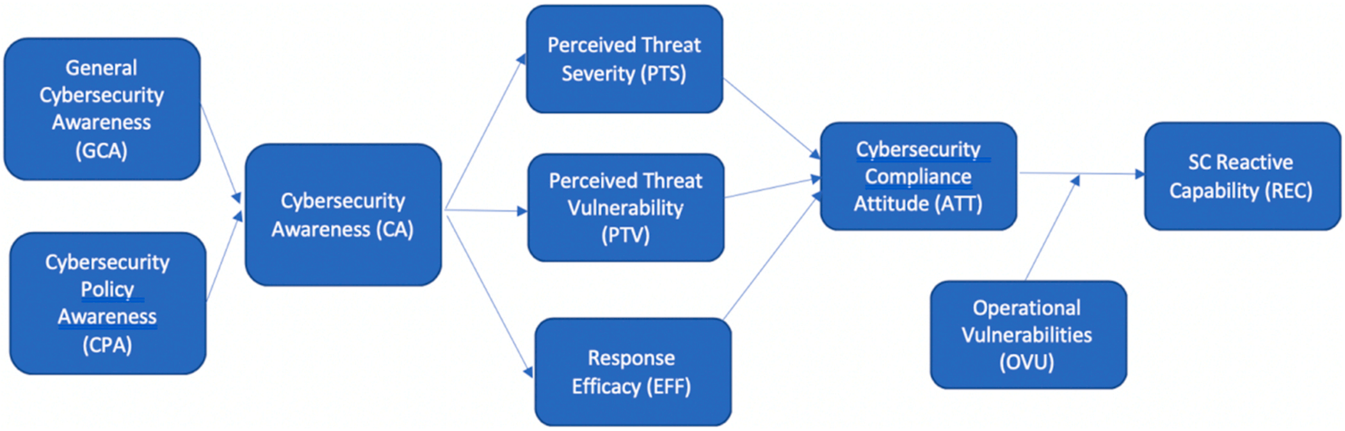

General Cybersecurity Awareness (GCA)
Cybersecurity Policy Awareness (CPA)
Cybersecurity Awareness (CA)
Perceived Threat Severity (PTS)
Perceived Threat Vulnerability (PTV)
Response Efficacy (EFF)
Cybersecurity Compliance Attitude (ATT)
SC Reactive Capability (REC)
Operational Vulnerabilities (OVU)

Fig. 1. Research Framework.

sanctions received in noncompliance are only an implication. As discussed in the preceding sections, perceived adverse threat severity refers to the dire consequences resulting in one's inability to cope with the threat. The existence of a threat renders a subject vulnerable and, conversely, a vulnerable subject is one that is susceptible to threats. In the context of this study, we consider both severity and vulnerability as mutually conditioning factors that affect a person's attitude. Thus, we hypothesize:

Hypothesis 4. : PTSs positively influence an employee's compliance attitude (ATT).

In the context of security, an employee's background knowledge about existing threats and their ability to cope can influence their actions by indirectly forming behavioral, normative, or control beliefs (Bulgurcu et al., 2010). Differences in individual responses following various security interventions have also been shown to be caused by differences in individual profiles and dispositional factors (Johnston et al., 2017). This is because individuals often translate perceptions into intentions based on their personality traits. While meta-personality traits such as emotional stability, openness, and conscientiousness are not factored in this study, it suffices to note that individuals may still exhibit different behaviors based on their perceptions of violations and sanction opportunities. According to Janssen et al. (2017), privacy concerns and security affect users' perceived ability to use, use and trustworthiness. As such, we argue that an individual's view of their own vulnerability still affects their behavior—although perception density is affected by the individual's meta-personality traits.

Additionally, coping appraisal comprises self-efficacy and response efficacy (EFF). This involves an individual deciding whether they can successfully deal with a threat and the cost of their associated adaptive behavior. Individuals who are of the perception that they are not vulnerable to threats are not likely to adhere to preventive measures (Ifinedo, 2012). In other words, employees' positive coping-appraisal response depends on their beliefs that: their response will be effective, they have the ability to perform the action, and there will be an associated response cost (Boss et al., 2015; Sharma et al., 2020). We posit that an employee whose perceived vulnerability is high will be more compliant to policies to increase self-efficacy and will make an extra effort to ensure that the security of tasks remains intact. We therefore hypothesize:

Hypothesis 5. : PTVs positively influence an employee's compliance attitude (ATT).

Anderson and Agarwal (2010) and Menard et al. (2018) show that one's intention to engage in secure behavior is significantly affected by collectivism and psychological ownership. Collectivism considers ownership of a target in a group context, where what belongs to a member of the group belongs to the entire group. Psychological ownership is the mental state or innate feeling of possession over a target. Accordingly, this research postulates that an employee's confidence in their own ability to take safeguard measures depends on their CA, which is aggregately measured in the respective constructs. If an individual perceives a particular threat as relevant, then they see the relevance of performing secure behaviors—otherwise the individual's perception of relevance decreases (Hina et al., 2019; Menard et al., 2017). Further, if the person believes in the effectiveness of a recommended response, they will follow it (ATT).

In security, the protection of resources depends on action rather than intention (Crossler et al., 2013). People will behave more securely if their awareness is enhanced, and they are made conscious of effective actions to protect themselves (van Bavel et al., 2019). Along this line of reasoning, this study measures attitude towards compliance rather than behavioral intention. Self-efficacy is dropped from the model, as we are measuring the employee's belief that organizational policy procedures while working from home are sufficient to avert a threat—we are not measuring how well they conduct the procedure. In line with Martens et al. (2019), response cost is not included in the model because past research has indicated it is difficult and ambiguous (Warkentin et al., 2016). Additionally, according to Hanus and Wu (2016), home users view response cost as insignificant in preventing them from implementing desktop security behavior, because such tools are often bundled in the purchase or readily available. Thus, we hypothesize:

Hypothesis 6. : EFFs positively influence an employee's compliance attitude (ATT).

3.3. Supply-chain-reactive capability (REC) and vulnerabilities (OVU)

Reactive aspects of SCs (RECs) refer to the response and recovery abilities of organizations (Chowdhury & Quaddus, 2017). SC response capabilities refer to a firm's earliest ability to mitigate disruptions with the least impact (Pettit et al. 2013) so that SCs can return to their normal positions, if not stronger positions (Chowdhury & Quaddus, 2017). The recovery capabilities of the SC to recover from a shock are related to resilience (Annarelli & Nonino, 2016). They are usually based on recovery time and recovery cost, disruption absorption, and the ability to ease the impact of loss (Chowdhury & Quaddus, 2016; Wang et al., 2010).

A firm's mitigation capabilities for enhancing SC resilience include both tangible (e.g., technology) and intangible (e.g., knowledge, education, training, and experience) resources that determine how firms react to various threats (Blackhurst et al., 2011). Dabhilkar et al. (2016) show that the resilience capabilities of SCs can be formed from routine practices implemented within firms after a disruptive incident—otherwise known as reactive-internal capabilities. According to Birkie et al. (2017), internal reactive capabilities are stronger in affecting performance, thereby further reinstating practices' role in the formation of resilience. In fact, an employee's attitude towards risk can potentially alter the optimal resilience of supply chain solutions. A highly risk-averse attitude will relate to a lack of resilience with cost components such as vulnerability or loss of control (Christopher & Peck, 2004). The importance of a proactive attitude has been studied by Benzidia and Makaoui (2020) in the context of firms' ability to react quickly to "dynamic environment changes through IT applications adaptability" (p. 3) and by Namdar et al. (2018) in the context of decision-makers' risk attitude to sourcing in reaction to disruptions. Along this line of reasoning, an employee's compliant attitude and its effect on resilience are incorporated into the model. Thus, we hypothesize:

Hypothesis 7. : ATT will positively influence supply-chain-reactive capability (REC).

Furthermore, when considering resilience, the fundamental factors that make the firm susceptible to disruptions—i.e., vulnerabilities (OVU)—must be studied in relation to the firm's capabilities. Firms that are exposed to risks but do not invest in the right capabilities will be "eroding" profits (Pettit et al., 2010, p. 47). The goal is for managers to create a portfolio of balanced resilience. Best practices in SC resilience (Ivanov et al., 2017; Lücker et al., 2019) highlights static capabilities (Ivanov, 2020b) that remain constant and consistent over time. The design of SC reactive policies needs to consider the duration of disruptions, as well as how much the degree of demand varies (the time it takes to begin recovery for the resources is critical depending on the firm's "preparedness" in flexibility and the ability to reallocate resources) (Chen et al., 2017; Ivanov, 2019, 2020b). The COVID-19 pandemic has not only dispersed markets but created unforeseen technology failures that disrupt the SC. It is therefore essential to manage change now. Our final hypothesis is therefore:

H8. : Vulnerabilities (OVU) moderate the relationship between ATT and REC.

4. Methodology

4.1. Research instrument

The instrument developed in this study comprises of two major sections. The first measures employees' GCA and GPA. With it, we sought to understand individuals' motivation for cybersecurity compliance based on the underlying theory of PMT. The second section measures employees' attitudes towards cybersecurity compliance (ATT) and how this affects the SC reactive capability. We adapted the measurement indicators for employee CA (comprising of general cybersecurity awareness and general cybersecurity policy awareness) from Bulgurcu et al. (2010), the PTS indicators from Zhang et al. (2018) and Liang and Xue (2010), the PTV from Bélanger et al. (2017) and Zhang et al. (2018), and the EFF indicators from Zhang et al. (2018). ATT indicators were adapted from Aurigemma and Mattson (2017) and Martens et al. (2019), OVU from Pettit et al. (2013), and REC from Chowdhury and Quaddus (2017). All measurement items were measured on a 7-point Likert scale ranging from "1-Never" to "7-Always."

Following the first round of data collection, we conducted six post-survey interviews. These enabled us to better understand the study findings and to seek further explanations as per Liu et al. (2016). Interviewees were selected based on their industry experience over many years and included a Cyber Security Engineer, Head of Information Security, Software Engineering Manager, IT Manager, Director of IT, and Partner/Chief Architect of an IT Company. Findings relevant to the study from these interviews are discussed below.

4.2. Data collection and analysis

Our study adopted a mixed-methods research design by combining a survey method and semi-structured interviews (qualitative analysis) to further verify and support the results obtained from the questionnaire findings. Questionnaires were first distributed to respondents from SMEs based in the Klang Valley, Malaysia. The SMEs were identified from Suruhanjaya Syarikat Malaysia (also known as Companies Commission of Malaysia), the statutory body that oversees the registration of businesses in Malaysia. According to Wong et al. (2021), Klang Valley is a suitable sampling location because it records the strongest GDP contribution by state and has high population density and economic growth. As with Wong, Leong et al. (2020), random sampling was employed to preserve the anonymity of respondents. 750 survey questionnaires were distributed and a total of 200 responses were collected (a 26.7% response rate) between 1 April 2020 and 20 June 2020. Most of the respondents were executive level and above.

Virtual interviews via Zoom with six practitioners were conducted separately between 1 November 2020 and 25 November 2020 as travel was restricted due to the COVID-19 pandemic. While there is no firm guideline for determining the sample size for interviews, the information gained from the six practitioners had led to a point of data saturation (Warren et al., 2014). Interviewees were sent brief descriptions of the background and rationale of the study together with interview survey questions approximately a week in advance. The semi-structured interviews lasted between 30 and 50 min. These were audio recorded, transcribed and subsequently analysed using NVivo.

5. Results

The demographic profile of respondents is presented in Appendix 1. The overall firm size is between 50 and 200 employees (66.5%). The majority of the respondents are below 40 years of age (77%). Most respondents are senior level executives (e.g., General Manager, Director, CEO) (41.5%) and ISO14001 (Environmental Management System) Person-in-Charge/Management Representative (23.5%). Many have been with their firm for more than 10 years (61.5%).

5.1. Statistical analysis

As our conceptual model includes formatively measured second-order constructs, we adopted Partial Least Squares (PLS) implemented in SmartPLS (version 3.2.9). The program permits the simultaneous testing of both reflective and formative indicators with second-order factors within a model (Kim et al., 2020). PLS is suitable for data that fails the normality requirements (Tan & Ooi, 2018; Ng et al., 2022). Using Web Power online tool, we found that the p-value of Mardia's multivariate skewness ($\beta = 14.823$) and Mardia's multivariate kurtosis ($\beta = 98.896$) were less than 0.001 respectively. This confirms the multivariate non-normality. On the sample size, we employed G*Power 3.1.9.2 with an effect size set as 0.15, the power level at 0.80, the alpha value of 0.05, and 6 predictors as the level of standard parameters. The required sample size is 98, indicating that our sample size is sufficient for testing hypotheses.

5.2. Common method variance

Procedural and statistical designs were taken to mitigate the issue of common method variance (CMV), as we gathered data using a self-reporting questionnaire (Lee V.H, 2020; Wang et al., 2022). Procedurally, the description of the purpose of the study was included in the questionnaire and respondents were guaranteed confidentiality and anonymity (Kim et al., 2020). The survey questions were also separated. For example, questions about demographic characteristics were first presented, followed by questions on the measurement items in the conceptual model (Lee C, 2020). Statistically, the study followed the approach by Liang et al. (2007), using the unmeasured latent construct method. CMV is not an issue in this study, because the majority of method factor loading (Rb) was not significant (as shown in Table 1). Additionally, the average substantive variance (0.615) was greater than the average method variance (0.043).

5.3. Assessing the outer measurement model

As the conceptual model consists of both reflectively and formatively measured constructs, all reflectively first-order constructs were examined in terms of reliability and of both discriminant and convergent validity. Table 2 shows that all first-order constructs have attained internal consistency reliability, because the composite reliability (CR) values are higher than 0.70 (Hew et al., 2017; Wan et al., 2021). In terms of convergent validity, factor loadings (FL) and average variance extracted (AVE) were employed (Wong et al., 2014; Wong et al., 2015). According to Hair et al. (2017), the AVE should exceed 0.50, while FLs should be above the threshold of 0.708. In addition, items with FL below 0.40 should be considered for removal, while FLs between 0.40 and 0.70 should be retained if the AVE can explain about 50% of the construct variance (Tan & Ooi, 2018; Yan et al., 2021). Table 2 shows that all individual FLs are found to be significant at $p < 0.001$ level and range between 0.472 and 0.848—except PTS3, PTS5, REC2, OVU2, OVU4, PTV2, and PTV4, which were dropped, following the suggestions of Hair et al. (2017). The lowest value of AVE, on the other hand, is 0.511, and is above the recommended cut-off value of 0.5. As such, this study has established convergent validity.

The discriminant validity (DV) in the proposed model was confirmed, as all the items in Table 3 are highly loaded on their own constructs rather than other constructs. As such, DV has been established for all constructs.

Hair et al. (2017) suggest that, when assessing the second order formatively measured constructs, collinearity issues among the first order must not be present. In addition, the first-order weights and loadings should be assessed and reported. Table 4 shows that the variance inflation factor (VIF) among the formative indicators of CA is less than 3.3. This indicates that multicollinearity is not an issue (Hew et al., 2017). The outer weights and loadings reported in Table 4 also show

Table 1
Common Method Factor Analysis.

Latent Construct	Indicators	Substantive factor loading (Ra)	Ra^2	Method factor loading (Rb)	Rb^2
ATT	ATT -> ATT1	0.851 ***	0.724	-0.087^{NS}	0.008
	ATT -> ATT2	0.544 ***	0.296	0.169^{NS}	0.029
	ATT -> ATT3	0.729 ***	0.531	-0.039^{NS}	0.002
	ATT -> ATT4	0.735 ***	0.540	-0.040^{NS}	0.002
CPA	CPA -> CPA1	0.895 ***	0.801	-0.051^{NS}	0.003
	CPA -> CPA2	0.642 ***	0.412	0.108^{NS}	0.012
	CPA -> CPA3	0.860 ***	0.740	-0.043^{NS}	0.002
EFF	EFF -> EFF1	0.723 ***	0.523	0.061^{NS}	0.004
	EFF -> EFF2	0.211^{NS}	0.045	0.440**	0.194
	EFF -> EFF3	1.181 ***	1.395	-0.435***	0.189
GCA	GCA -> GCA1	0.801 ***	0.642	0.063^{NS}	0.004
	GCA -> GCA2	0.829 ***	0.687	-0.023^{NS}	0.001
	GCA -> GCA3	0.820 ***	0.672	-0.046^{NS}	0.002
OVU	OVU -> OVU1	0.851 ***	0.724	-0.063^{NS}	0.004
	OVU -> OVU3	0.865 ***	0.748	-0.039^{NS}	0.002
	OVU -> OVU5	0.816 ***	0.666	-0.084^{NS}	0.007
	OVU -> OVU6	0.313^{NS}	0.098	0.285^{NS}	0.081
PTS	PTS -> PTS1	0.582 ***	0.339	0.124^{NS}	0.015
	PTS -> PTS2	0.915 ***	0.837	-0.102^{NS}	0.010
	PTS -> PTS4	0.775 ***	0.601	-0.002^{NS}	0.000
PTV	PTV -> PTV1	1.094 ***	1.197	-0.310***	0.096
	PTV -> PTV3	1.002 ***	1.004	-0.203*	0.041
	PTV -> PTV5	0.681 ***	0.464	0.09^{NS}	0.008
	PTV -> PTV6	-0.041^{NS}	0.002	0.624***	0.389
REC	REC -> REC1	0.846 **	0.716	-0.086^{NS}	0.007
	REC -> REC3	0.768 **	0.590	0.083^{NS}	0.007
	Average	***0.742***	***0.615***	***0.015***	***0.043***

Notes: a. * ** $p < 0.001$; * * $p < 0.01$; * $p < 0.05$, ^{NS} insignificant.

that both formative indicators are relevant and significant and can contribute to forming a CA. Therefore, this study has confirmed that such a formative measurement model is valid.

5.4. *Inspecting the inner structural model*

To assess the inferential statistics, we employed a bias-corrected and accelerated (BCa) bootstrap procedure with 5000 subsamples at a two-tailed 0.05 significance level (Yuan et al., 2021; Loh et al., 2021). Table 5 and Fig. 2 suggest that all hypotheses are supported and have a positive significant relationship, as hypothesized. Hence, H1, H2, H3, H4, H5, H6, and H7 have all been supported. To test H8, we conducted a moderating effect by employing the interaction effect of OVU. However, the bootstrap results in Table 5 show that OVU did not moderate the path between ATT and REC ($\beta = -0.017$, $P > 0.05$). The bias-corrected confidence intervals for 2.5% and 97.5% also indicate that H8 was not supported, as the confidence interval contains the value of zero (2.5% = −0.150% and 97.5% = 0.086).

Table 2
Loadings, composite reliability, Dijkstra Henseler and average variance extracted.

Constructs	Items	Factor Loadings (FL) (p-levels)	Composite Reliability (CR)	Average Variance Extracted (AVE)
ATT	ATT 1	0.772***	0.807	0.511
	ATT 2	0.688***		
	ATT 3	0.704***		
	ATT 4	0.698***		
CPA	CPA1	0.848***	0.846	0.647
	CPA2	0.749***		
	CPA3	0.813***		
EFF	EFF1	0.763***	0.768	0.526
	EFF2	0.637***		
	EFF3	0.771***		
GCA	GCA1	0.845***	0.856	0.665
	GCA2	0.814***		
	GCA3	0.786***		
OVU	OVU1	0.804***	0.821	0.545
	OVU3	0.831***		
	OVU5	0.787***		
	OVU6	0.472***		
PTS	PTS1	0.718***	0.805	0.580
	PTS2	0.815***		
	PTS4	0.753***		
PTV	PTV1	0.788***	0.821	0.538
	PTV3	0.789***		
	PTV5	0.753***		
	PTV6	0.582***		
REC	REC1	0.779***	0.787	0.65
	REC3	0.832***		

5.5. *The predictive relevance and effect size*

This study adopted Cohen's f^2 to assess the effect size of the constructs. According to Cohen (1988), effect size f^2 values that are above 0.02, 0.15, and 0.35 indicate small, medium, and large effects, respectively. Table 6 shows that OVU* has no effect, as the value is below 0.02 (Tan & Ooi, 2018). ATT and OVU demonstrate a large effect size on REC. Similarly, CA shows a large effect size on PTV and EFF respectively. PTS, on the other hand, shows a medium effect on PTS. Lastly, PTV and PTS show a small effect on ATT, while EFF indicates medium effects on ATT. To check on Q^2, we used the blindfolding method with an omission distance of 7 (Tew et al., 2021). Table 6 shows that all values of Q^2 are greater than zero. This indicates that REC, PTV, PTS, EFF, and ATT have predictive relevance. The in-sample predictive power (coefficient of determination, R^2) for REC is 26.5%. Hence, the predictive accuracy of the model is considered to be moderate (Lim et al., 2020). As R^2 did not focus on out-of-sample predictive power, our study engaged PLSpredict by focusing on REC (Loh et al., 2019). Table 7 illustrates that all Q^2 values are positive, implying the predictive ability of the model. Only 1 out of 2 items in PLS has a higher root mean squared errors (RMSE) values in comparison to the linear model (LM) benchmark, according to Shmueli et al. (2016). Therefore, the model has medium predictive power.

5.6. *Qualitative findings*

The interviews with the six practitioners (Angie, HJL, MF, MV, SKS and SR) focused on five main questions relating to issues being examined in this study, with the aim to provide further support for the quantitative findings presented in the previous section. In providing their answers, interviewees were encouraged to highlight relevant examples. The following sub-sections present further insights from these interviews.

Table 3
Loading and cross-loading value.

Latent Construct	ATT	CPA	EFF	GCA	OVU	PTS	PTV	REC
ATT1	0.750	0.406	0.482	0.507	0.505	0.392	0.436	0.383
ATT2	0.720	0.459	0.667	0.401	0.312	0.454	0.520	0.269
ATT3	0.670	0.380	0.409	0.425	0.510	0.309	0.447	0.382
ATT4	0.718	0.387	0.563	0.440	0.232	0.377	0.510	0.254
CPA1	0.450	0.848	0.537	0.593	0.427	0.438	0.523	0.355
CPA2	0.497	0.749	0.511	0.613	0.363	0.361	0.466	0.280
CPA3	0.437	0.813	0.527	0.532	0.463	0.379	0.518	0.364
EFF1	0.530	0.493	0.744	0.527	0.389	0.392	0.634	0.316
EFF2	0.605	0.463	0.658	0.513	0.459	0.309	0.468	0.319
EFF3	0.474	0.452	0.768	0.371	0.221	0.366	0.475	0.212
GCA1	0.571	0.569	0.583	0.845	0.496	0.395	0.553	0.361
GCA2	0.420	0.623	0.520	0.814	0.436	0.385	0.497	0.276
GCA3	0.524	0.571	0.515	0.786	0.357	0.296	0.443	0.307
OVU1	0.489	0.390	0.381	0.329	0.804	0.332	0.437	0.359
OVU3	0.483	0.421	0.399	0.450	0.831	0.332	0.434	0.361
OVU5	0.276	0.398	0.349	0.422	0.787	0.200	0.434	0.399
OVU6	0.406	0.353	0.462	0.418	0.472	0.208	0.467	0.169
PTS1	0.474	0.387	0.343	0.376	0.292	0.734	0.355	0.270
PTS2	0.387	0.358	0.389	0.303	0.301	0.813	0.397	0.116
PTS4	0.359	0.369	0.397	0.318	0.223	0.736	0.501	0.193
PTV1	0.390	0.451	0.504	0.396	0.400	0.377	0.788	0.207
PTV3	0.414	0.508	0.503	0.418	0.461	0.375	0.789	0.275
PTV5	0.541	0.467	0.629	0.465	0.332	0.476	0.753	0.315
PTV6	0.570	0.389	0.473	0.478	0.475	0.340	0.582	0.304
REC1	0.320	0.251	0.285	0.177	0.359	0.219	0.277	0.779
REC3	0.396	0.409	0.353	0.430	0.374	0.201	0.342	0.832

Table 4
Assessing the formative construct.

Formative Indicators	Variance Inflation Factor (VIF)	Outer Weight	Outer Loading
GCA	2.082	0.58[a]	0.916[a]
CPA	2.082	0.497[a]	0.939[a]

[a] Note: $p < 0.001$.

5.6.1. *Cyber security awareness and perceived threat severity*

All interviewees agreed that raising cyber security awareness will influence perceived threat severity. However, one of the interviewees (MF) emphasised that “it depends on employees’ behaviour, the work environment and the [security threat] situation”. HJL also highlighted the fact that many companies have tight budget constraint and resources. Therefore, enforcing minimal cybersecurity measures, including staff training, will be a critical first step. MV also recognised the importance of cyber security awareness, saying that “cyber security incidents can be reduced as users become more aware of the threats and implications of their negligence”. A good example of this was provided by SR where an organisation reselling telco services provided employee training on privacy and Personal Data Protection Act requirements. Subsequently, when store staff were examining forms provided to customers to fill in temporary details, they noticed that these forms contained customers’ National Registration Identity Card information, and quickly alerted their manager on the matter. A thorough investigation was launched immediately and corrective action was implemented. Finally, Angie emphasised on raising awareness through education on cyber threats and also providing sufficient data and supporting information so that employees will be better able to react more effectively accordingly to the severity of perceived threats.

5.6.2. *Cyber security awareness and perceived threat vulnerability*

In discussing cyber security awareness and how this influences perceived threat vulnerability, MF emphasised that “in general, people with cyber security awareness will make much better decisions related to perceived threat vulnerability because they understand the risks and the outcomes when using any system with weak security protection.” He further recognised the importance of the context – “the work environment”, providing the example that if employees are only given one option with risks associated, they do not have a choice! In this respect, SKS said that it is necessary to regularly brief staff on the potential threats

Table 5
Hypotheses testing.

Hypothesis	PLS Path	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics (|O/STDEV|)	P Values	Bias Corrected Confidence Interval		Remarks
H7	ATT -> REC**	0.27	0.249	0.097	2.795	0.005	0.106	0.477	Yes
H3	CA -> EFF***	0.708	0.708	0.049	14.579	0	0.594	0.786	Yes
H1	CA -> PTS***	0.504	0.509	0.06	8.441	0	0.384	0.616	Yes
H2	CA -> PTV***	0.667	0.664	0.06	11.158	0	0.537	0.763	Yes
H6	EFF -> ATT***	0.522	0.522	0.077	6.776	0	0.366	0.67	Yes
H8	OVU* -> REC^{NS}	-0.017	-0.028	0.064	0.263	0.792	-0.15	0.086	No
H4	PTS -> ATT**	0.18	0.18	0.065	2.776	0.006	0.06	0.313	Yes
H5	PTV -> ATT*	0.191	0.189	0.087	2.193	0.029	0.015	0.354	Yes

Notes a.* Significant at $p < 0.05$ level.
b.* * Significant at $p < 0.01$ level.
c.* ** Significant at $p < 0.001$ level.
d.^{NS} Not supported

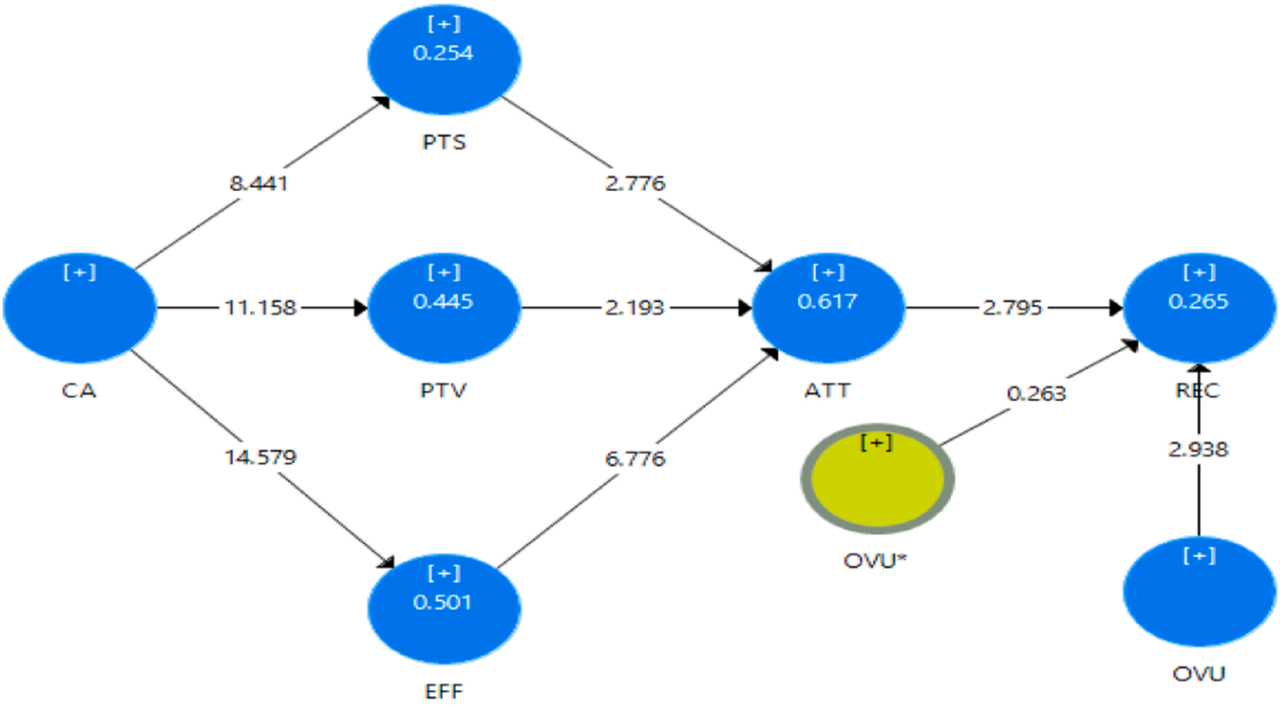


Fig. 2. Result of Hypotheses Testing.

Table 6
Quality of the structural model.

Endogenous variables	R^2	Q^2	Exogenous variables	Effect size f^2
REC	0.265	0.233	ATT	0.060
			OVU	0.085
			OVU*	0.001
PTV	0.445	0.434	CA	0.801
PTS	0.254	0.247	PTS	0.340
EFF	0.501	0.487	CA	1.004
ATT	0.617	0.587	PTV	0.040
			PTS	0.058
			EFF	0.322

Table 7
PLSpredict results.

REC	PLS			LM	
	Q^2_predict	RMSE	MAE	RMSE	MAE
REC1	0.100	1.064	0.852	**1.072**	0.836
REC3	0.161	**1.092**	0.888	1.125	0.897

whilst HJL stated that organisations should be encouraged to use state-of-the-art cyber securities tools such as LastLine, Fireeye, Kaspersky etc.

SR provided a good example of the benefit of raising employees' awareness as follows: "The IT Security team had sent awareness material that had explained about potential phishing scam based on COVID-19 pandemic. A staff at the Finance Department was constantly getting an email related to the COVID-19 which they did not request for. The matter was escalated to the IT Security team, who discovered that the email had a malware in the attachment and had evaded the anti-spam mechanism. Subsequently the anti-spam rules were tightened, a threat hunt was done to ensure that the malware in question did not execute in the environment." This and other examples provided by the interviewees illustrate the importance of raising employee awareness to address cyber security incidents.

5.6.3. Cyber security awareness and respond efficacy

In response to the question relating to response efficacy, MV stated that "Cyber security awareness can improve response efficacy when users are shown how their security negligence can impact the security posture of an organization. Users should be made aware of how they can help organizations protect themselves against adversaries who are often targeting them as victims." In this respect, "exercises and phishing simulations where users are forced to respond to real-world scenarios in a simulated environment" are essential. HJL emphasised the need for General Data Protection Regulation across the region to enforce cyber security across many organisations as well as the use of Security Information and Event Management system. SKS emphasised the need to raise awareness of Standard Operating Procedures and introducing added verifications for suppliers and customers. Angie and MF provided good examples of respond efficacy through raising awareness, both emphasising on education, and on upgrading software with "good antivirus protection and firewall".

5.6.4. Policy compliance and compliance attitude

Concerns relating to employees' compliance to policies and Data Protection Act was raised by all interviewees. HJL emphasised on the need for a "Data Leakage Protection tool…. to monitor employee activity and behaviour, where actions are reported and handled accordingly." The need for including policy compliance in employees' KPI was raised by MV: "I feel policy compliance has to be included in key performance indicators of employees in order to get commitment from them. If employees do not want to voluntarily adopt protective behaviour, then it has to be made a goal in their yearly targets, to ensure that they are forced to ensure that they adopt protective behaviour." SR stated that "motivation for compliance is either driven by a carrot or a stick approach. Compliance needs to be a culture that is driven from both directions, top and bottom, through series of activities which motivates and rewards staff as it is "another additional" item that needs to be done." In this respect, MF again highlighted the need for education and Angie noted the need to "conduct a thorough vulnerability assessment and penetration testing for the whole company system and network to improve the current security policy."

5.6.5. Policy attitude and supply chain reactive capability

Interviewees emphasised on compliance attitude being essential for building supply chain reactive capability. They talked about creating a secure "inter-org" trust bubble [SR]; 'defense-in-depth' strategy always being the best control [MV]; having a well formulated framework to mitigate disruptions, should a threat incident occurred [HJL]; following all procedures correctly and in a prudent manner [MF]; and putting in place safeguards in the form of firewalls, Active Directory Group Policies, whitelisting, 2-Factor Authentication and aggressive Spam/Phishing filters [SKS]. Angie also emphasised on the importance of companies using advanced tools such as host checking (a tool to check the security posture of an endpoint before authorizing access to corporate information systems) to reinforce the security of remote working.

6. Discussion

This study employed the Protection Motivation Study (PMT) framework to propose that employees' general cybersecurity awareness (comprising of cybersecurity and policy awareness) affects their compliance attitude. It does this via appraisal beliefs and the effectiveness of coping mechanisms on cybersecurity threats to protect and fortify the supply-chain-reactive capability (refer to Fig. 1). Our hypotheses expected all eight key determinants to be positively associated. This would result in a shift in employees' compliance attitude regarding cybersecurity.

First, the empirical results of our findings show that the conceptual framework presented in Fig. 1 is supported and that is a robust framework to investigate the role of CA on employees' beliefs and behaviors on cybersecurity. CA is found to influence employees' PTS and PTV when exposed to cyber threats. This means that cybersecurity awareness education and explicit security policies do enhance employees' competency in managing cybersecurity tasks in coping with perceived threats. This is consistent with findings from past studies on the role of CA. For example, Donalds and Osei-Bryson (2020) have found that general CA yields a significant impact on general security and password security compliance behavior. Bulgurcu et al. (2010) have also shown that awareness significantly impacts employees' compliance attitude. According to Bada and Nurse (2019), in the context of CA, the challenges of SMEs are not new, and practitioner insights are important, given their practical nature. Insufficient cybersecurity and awareness can undermine SME security (Cheung et al., 2021). While academic literature has provided informative insights, it rarely reaches real-world programs (Bada & Nurse, 2019). The reality is that SMEs are often too focused on daily operations. They are thus unlikely to proactively bolster their security postures. Our interviewees iterated and emphasized the importance of having the right cybersecurity knowledge—knowledge that will influence employees' threat appraisal and responses in a more effective manner. Taking minimal cybersecurity measures, including staff training, will be one of the required steps for SMEs to move ahead.

Second, the results of this study suggest that all three constructs (PTV, PTS, and EFF) are significant determinants of ATT. An effective, personal, and practical training program that educates users to efficiently use a system can enhance their coping abilities (Alalwan et al., 2016). Users who are conscious of a threat will be wary of falling prey to it (Johnston & Warkentin, 2010). Thus, their attitudes will be positively influenced (Anderson & Agarwal, 2010). This reinforces the importance of creating user awareness around the risks and ways to mitigate them. This finding is also consistent with that of Li et al. (2019), who indicated that positive influences on employees' threat appraisal and coping appraisal abilities can yield a positive impact the employee's motivation to comply. Interviewees echoed this, placing much emphasis on the value of equipping employees with proper CA. They reasoned that this is important because employees are then more likely to know how to deal with specific issues, such as sensitive data, as most COVID-19 related security issues emerge from the network, internet, and IoT (remote pc, uploading and downloading files from an unknown source, unsecure cloud storage, etc.).

Next, we propose that a compliant attitude helps to build SC post-disruption reactive capabilities in the form of a *proactive* mediation. This is moderated by vulnerabilities. However, empirical results revealed that, while the hypothesis between compliant attitude and reactive capabilities holds, the moderating effect was not supported. There are a few plausible explanations. Reactive security strategies require that firms be ready with a vast arsenal of defense mechanisms before exploitation. Many SMEs do not have a solid foundation of effective cybersecurity risk management, and securing SC resilience typically requires both proactive and reactive capabilities (Chowdhury & Quaddus, 2017). Supply chain managers need to design SCs that reduce vulnerabilities to respond effectively. Selecting suitable security supply chain measures is complex (Cheung et al., 2021). Managing vulnerabilities is a continuous process that requires keeping up with new systems being added into networks, changes made to systems and the discovery of new vulnerabilities over time. SMEs will need to run multiple assessments to gather vulnerability data. According to one of our interviewees: *"Motivation for compliance is usually driven by the carrot and stick approach, and compliance needs to be a culture that should be driven from both directions - top and bottom, through series of activities which motivates and rewards employees as it is another additional item that needs to be done."*

In summary, cybersecurity awareness and policy compliance are difficult to achieve and most organizations are still resorting to "*driving adoption through mandate,"* while "*structuring policies that encourage and reward compliance will help drive adoption.*" Perhaps a stark statement by another interviewee is that: *"An attitude that is vigilant towards uncovering potential attack [that] surfaces in an organization can [allow organizations to] respond to threats has not happened yet by implementing security safeguards."*

A final comment by another interviewee was: *"There's no silver bullet when it comes to mitigating attacks that can disrupt the supply chain of an organization. Taking security measures at different layers is always the best strategy as attacks cannot be entirely prevented, therefore mitigation capabilities should be instilled into the organization at every layer possible. With effective control in place, an active attack can be controlled before an actual breach happens. Therefore, it is important that these controls should not only be in place within the organization but also with its third parties."*

We can speculate that there have been tendencies to mandate compliance rather than investing in security-related services like education and training programmes. However, this work provides empirical evidence focusing on end-users instead of security teams at an aggregated level, where changes in awareness contribute to SMEs' capability to reduce incidents. This is meaningful, as often members of firms are categorized diversely according to their job roles and responsibilities. Therefore, we hypothesized that CA would make a difference in reducing firm security incidents, and evidenced the importance of both quantitatively and qualitatively.

6.1. Theoretical contributions and implications

This research advances the existing body of work in explaining the results of applying PMT in cybersecurity contexts. Prior studies have evidenced the effect of motivation on both behavioral intention and behavior in various contexts. However, in the context of cybersecurity, an individual's motivation for protection may not necessarily yield personal benefits and may depend on other factors (Menard et al., 2017). We observed that CA reinforces an individual's competence in relation to responding to a particular threat—action cues are more effective in improving security behavior. The COVID-19 pandemic disrupted many SME SCs in an unforeseen manner. We argue that, despite the good intentions of employees to comply, intent does not necessarily make an SC more resilient. Cybersecurity threats vary from inadvertent events to deliberate attacks. Furthermore, the implementation of standard compliance procedures generally requires a larger commitment of resources than SMEs would otherwise channel into business activities (Manso et al., 2015). Furthermore, this is in line with our earlier discussion, where we contended that employees are measured on their ability to follow and carry out a specific action, rather than to deal with an entire cyber incident. More importantly, there are lessons that can be drawn from the COVID-19 pandemic from SC, policymaker, and individual perspectives when topics such as risk management become relevant again (Barbieri et al., 2020).

6.2. Implications for practice

This study has significant implications. The findings highlight the importance of educating employees as we found that cybersecurity awareness affects employees' threat appraisal (i.e. perceived threat severity and perceived threat vulnerability). Hence, SMEs need to actively promote cybersecurity rules to staff and stakeholders by encouraging a cyber-secure mindset. Training and educating staff to understand the forms of a potential attack can help them avoid falling for cybersecurity threats, improve their abilities to assess the severity of the threat (PTS) and understand their own vulnerabilities (PTV). Some possible activities such as organizing regular campaigns to engage and inform employees on how to minimize their online footprint, promote personnel safety, and recognize insider threats are essential and should be advocated. One of the interviewees stressed that, when an employee receives a suspected COVID-19 themed phishing email, they should be able to notify their respective department to tighten anti-spam rules and execute an anti-threat-hunt, ensuring the malware was not executed in the SC.

Further, the findings also indicate that CA affects employees' coping appraisal (i.e. response efficacy). As an employee's perception of response efficacy (EFF) increases, their tendency to adopt appropriate coping strategy increases. Hence, organizations must provide both training and support to help their employees properly use the technology and increase their response efficacy. Implementation guidelines must be made known to employees during the adoption phase. SMEs must ensure these are clear, structured, and easy to follow, to further encourage awareness and attitudinal compliance. This would enable employees to have an ongoing pursuit to manage and minimize risks by prioritising actions that maximize protection. Further, managers should place greater emphasis on supply chain disruption with a commitment to learning from SC disruptions can help firms to be more responsive. They should not wait for pandemic-related disruptions to understand the vulnerabilities inherent in their SCs.

In this study, both threat and coping appraisals significantly affects cybersecurity compliance attitude (ATT). These finding stresses that security breaches are both serious and important to businesses. Hence, building positive attitudes that can lead to enhanced supply chain reactive capabilities (REC) is critical. This is also supported in our study. Given that most SMEs are still in the early stages of digitalising their SCs, risk management teams and employees themselves would become the key players and guardians of SC cyber resilience. Therefore, employees should realize that safeguarding against cybersecurity attacks is not the responsibility of the IT/Security team exclusively. It applies to everyone who is connected to cyberspace. SMEs should promote the importance and benefits of cybersecurity awareness and undertake a planned approach to strengthen their cybersecurity postures. At the same time, the risks of poor cybersecurity hygiene must be demonstrated through scenario planning and or simulations that can uncover weak points or issues in defending the supply chain. As emphasized by one of the interviewees, without established communication channels and baseline requirements, it will be difficult to create a secure "trust bubble" that ensures operations are kept intact amidst a cyberattack. Here, engagements of professionals like Chief Information Security Officers could help SMEs devise appropriate control and mitigation measures strategically to strengthen the security posture of SMEs while streamlining cybersecurity strategies.

The results of this study did not support the mediating role of vulnerabilities (OVU) in enhancing SC reactive capabilities. As explained earlier, protecting a system goes beyond human resources. The very nature of technology is such that it becomes obsolete quickly due to the fast pace of technological advancements. The moment technology is deployed is the very moment debt is accrued. For example, a breach event causes overheads in any organizations, ranging from manpower to engagement of third-party for recovery services and forensics. All these incur additional costs. The inability to backup and restore systems will only cause further expenses and, in most cases, additional expenditure becomes the only option to restore, instead of expanding.

6.3. Limitations and future research directions

Although this study has identified CA as a significant factor that affects an employee's motivation to protect, this work does not take into consideration gender and representation in job and roles (Anwar et al., 2017; Li et al., 2019). Female self-efficacy is found to be lower than men's and maybe a target for intervention (Anwar et al., 2017). Second, we measured the data we collected from Malaysian SMEs at a single point in time. Future work may benefit from a comparative study of various regions to add diversity into the work and to confirm findings using different samples and longitudinal analysis. Third, the source of threats is not considered in this study, and neither are safeguarding measures. Further research may be carried out to examine the variance in findings—if any—relating to this (Liang & Xue, 2010). Fourth, to fully understand the non-significant relationship between operational vulnerabilities and reactive capabilities, it would be interesting to expand the study on different contexts of vulnerabilities to SC proactive and reactive capabilities and their relation to the security behavior of employees. Finally, SMEs produce and consume enormous amounts of data, but they often lack adequate resources both to safeguard this data and comply with regulatory standards. Future work may consider awareness programmes tailored for SMEs to understand the challenges of CA programmes faced by them. Finally, our work echoes Dwivedi et al. (2017) in calling for research to investigate the relationship between human and non-human actors to advance insights on the role that technology can play in facilitating human processes, and to identify and define the conditions for SMEs to innovate and level up their competitiveness.

7. Conclusion

The present study advances our understandings of how cybersecurity awareness influences employee compliant attitudes, through the lens of the protection motivation theory. Analysis of survey data from 200 SME respondents and six expert interviews with SME practitioners informed the proposed research framework, which explains how an employee's compliant attitude impacts supply-chain-reactive capability. Conceptualized as comprising of general cybersecurity awareness and cybersecurity policy, we found that cybersecurity awareness positively impacts an employee's motivation to engage in protective behavior. This is expressed in terms of positive effects for perceived threat severity, perceived threat vulnerability, and coping efficacy. In this manner, the employee's attitude to comply is positively affected, which bolsters supply-chain-reactive capabilities. However, vulnerabilities did not moderate the relationship between employees' compliant attitudes in enhancing supply chain reactivity. The above findings combine quantitative and qualitative insights, that balance the preponderance evidence on cybersecurity in logistics and supply chain management and narrow the gap between empirical insights and practical applicability.

CRediT authorship contribution statement

Lai-Wan Wong: Conceptualization, Methodology, Formal Analysis, Writing – original draft, Writing – review & editing. **Voon-Hsien Lee**: Conceptualization, Methodology, Formal analysis, Writing – original

draft, Writing – review & editing. **Garry Wei-Han Tan**: Conceptualization, Methodology, Formal analysis, Writing – original draft, Writing – review & editing. **Keng-Boon Ooi**: Conceptualization, Methodology, Formal analysis, Writing – original draft, Writing – review & editing. **Amrik Sohal**: Conceptualization, Methodology, Formal analysis, Writing – original draft, Writing – review & editing.

Appendix 1. : Respondents' Profile

Demographic Items	Options	Frequency	Percentage
Gender	Female	94	47%
	Male	106	53%
Age	30 and below	86	43%
	Between 31 and 40	68	34%
	Between 41 and 50	40	20%
	51 and above	6	3%
Education	High school and below	17	8.5%
	Diploma/Advanced Diploma	32	16%
	Bachelor's degree/Professional Qualification	93	46.5%
	Postgraduate Degree	58	29%
Job Position	Executive (e.g., Officer, Accountant, Senior Accountant, Engineer, Senior Engineer, Staff Engineer, System Analyst, Assistant Manager etc)	18	9%
	Senior Staff Engineer/Principal Engineer/Manager/Senior Manager/ Head of Department	30	15%
	General Manager/Director/Senior Director/Executive Director/Managing Director/Chief Executive Officer/Vice President/ President/Chairman	83	41.5%
	ISO14001 Management Representative/ Person-in-charge (PIC)	47	23.5%
	ISO9001 Management Representative/ Person-in-charge (PIC)	16	8%
	Others	6	3%
Age of the firm	Less than 5 Years Old	26	13%
	Between 5 and 10 Years Old	51	25.5%
	More than 10 Years	123	61.5%
Company Size	Below 50 Employees	8	4%
	50 – 200 Employees	133	66.5%
	More than 200 Employees	59	29.5%

References

Abeysekara, N., Wang, H., & Kuruppuarachchi, D. (2019). Effect of supply-chain resilience on firm performance and competitive advantage: A study of the Sri Lankan apparel industry. *Business Process Management Journal, 25*(7), 1673–1695. https://doi.org/10.1108/BPMJ-09-2018-0241

Alalwan, A. A., Dwivedi, Y. K., Rana, N. P., & Simintiras, A. C. (2016). Jordanian consumers' adoption of telebanking: Influence of perceived usefulness, trust and self-efficacy. *International Journal of Bank Marketing, 34*(5), 690–709. https://doi.org/10.1108/IJBM-06-2015-0093/FULL/XML

Ameen, N., Tarhini, A., Shah, M. H., Madichie, N., Paul, J., & Choudrie, J. (2021). Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce. *Computers in Human Behavior, 114*, Article 106531. https://doi.org/10.1016/J.CHB.2020.106531

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly: Management Information Systems, 34*(SPEC. ISSUE 3), 613–643. https://doi.org/10.2307/25750694

Annarelli, A., & Nonino, F. (2016). Strategic and operational management of organizational resilience: Current state of research and future directions. In *Omega, 62* pp. 1–18). Elsevier Ltd. https://doi.org/10.1016/j.omega.2015.08.004

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior, 69*, 437–443. https://doi.org/10.1016/j.chb.2016.12.040

Araz, O. M., Choi, T. M., Olson, D. L., & Salman, F. S. (2020). Data analytics for operational risk management. *Decision Sciences, 51*(6), 1316–1319. https://doi.org/10.1111/deci.12443

Aurigemma, S., & Mattson, T. (2017). Privilege or procedure: Evaluating the effect of employee status on intent to comply with socially interactive information security threats and controls. *Computers & Security, 66*, 218–234. https://doi.org/10.1016/j.cose.2017.02.006

Bada, M., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). *Information and Computer Security, 27*(3), 393–410. https://doi.org/10.1108/ICS-07-2018-0080

Balapour, A., Nikkhah, H. R., & Sabherwal, R. (2020). Mobile application security: Role of perceived privacy as the predictor of security perceptions. *International Journal of Information Management, 52*, Article 102063. https://doi.org/10.1016/J.IJINFOMGT.2019.102063

Barbieri, P., Boffelli, A., Elia, S., Fratocchi, L., Kalchschmidt, M., & Samson, D. (2020). What can we learn about reshoring after Covid-19? *Operations Management Research.* https://doi.org/10.1007/s12063-020-00160-1

Bates, S. (2020). Managing the information security impact of COVID-19. *KPMG.* ⟨https://home.kpmg/xx/en/home/insights/2020/04/managing-the-information-security-impact-of-covid-19.html⟩.

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. https://doi.org/10.1016/j.ijhcs.2018.11.003

Bélanger, F., Collignon, S., Enget, K., & Negangard, E. (2017). Determinants of early conformance with information security policies. *Information and Management, 54*(7), 887–901. https://doi.org/10.1016/j.im.2017.01.003

Benz, M., & Chatterjee, D. (2020). Calculated risk? A cybersecurity evaluation tool for SMEs. *Business Horizons*. https://doi.org/10.1016/j.bushor.2020.03.010

Benzidia, S., & Makaoui, N. (2020). Improving SMEs performance through supply chain flexibility and market agility: IT orchestration perspective. *Supply Chain Forum.* https://doi.org/10.1080/16258312.2020.1801108

Birkie, S. E., Trucco, P., & Fernandez Campos, P. (2017). Effectiveness of resilience capabilities in mitigating disruptions: leveraging on supply chain structural complexity. *Supply Chain Management, 22*(6), 506–521. https://doi.org/10.1108/SCM-01-2017-0009

Blackhurst, J., Dunn, K. S., & Craighead, C. W. (2011). An empirically derived framework of global supply resiliency. *Journal of Business Logistics, 32*(4), 374–391. https://doi.org/10.1111/j.0000-0000.2011.01032.x

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: Management Information Systems, 39*(4), 837–864. https://doi.org/10.25300/MISQ/2015/39.4.5

Boyens, J., Paulsen, C., Bartol, N., Winkler, K., & Gimbi, J. (2020). Case studies in cyber supply chain risk management: anonymous consumer electronics company. *National Institute of Standards and Technology*. https://doi.org/10.6028/NIST.CSWP.02042020-2

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly: Management Information Systems, 34*(SPEC. ISSUE 3), 523–548. https://doi.org/10.2307/25750690

Chang, L. Y. C., & Coppel, N. (2020). Building cyber security awareness in a developing country: Lessons from Myanmar. *Computers and Security, 97*, Article 101959. https://doi.org/10.1016/j.cose.2020.101959

Chapman, P. (2020). Are your IT staff ready for the pandemic-driven insider threat? *Network Security, 2020*(4), 8–11. https://doi.org/10.1016/S1353-4858(20)30042-8

Chen, H. Y., Das, A., & Ivanov, D. (2019). Building resilience and managing post-disruption supply chain recovery: Lessons from the information and communication technology industry. *International Journal of Information Management, 49*, 330–342. https://doi.org/10.1016/J.IJINFOMGT.2019.06.002

Chen, Y., Ramamurthy, K., & Wen, K. W. (2015). Impacts of comprehensive information security programs on information security culture. *Journal of Computer Information Systems, 55*(3), 11–19. https://doi.org/10.1080/08874417.2015.11645767

Chen, Y., Ponsignon, T., Weixlgartner, R., & Ehm, H. (2017). Simulating recovery strategies to enhance the resilience of a semiconductor supply network. Proceedings - Winter Simulation Conference, 4477–4478. https://doi.org/10.1109/WSC.2017.8248170.

Cheung, K. F., Bell, M. G. H., & Bhattacharjya, J. (2021). Cybersecurity in logistics and supply chain management: An overview and future research directions. *Transportation Research Part E Logistics and Transportation Review, 146*, Article 102217. https://doi.org/10.1016/J.TRE.2020.102217

Chowdhury, M. M. H., & Quaddus, M. (2016). Supply chain readiness, response and recovery for resilience. *Supply Chain Management, 21*(6), 709–731. https://doi.org/10.1108/SCM-12-2015-0463

Chowdhury, M. M. H., & Quaddus, M. (2017). Supply chain resilience: Conceptualization and scale development using dynamic capability theory. *International Journal of Production Economics, 188*, 185–204. https://doi.org/10.1016/j.ijpe.2017.03.020

Chowdhury, N. H., Adam, M. T. P., & Skinner, G. (2019). The impact of time pressure on cybersecurity behaviour: A systematic literature review. *Behaviour and Information Technology, 38*(12), 1290–1308. https://doi.org/10.1080/0144929X.2019.1583769

Christopher, M., & Peck, H. (2004). Building the resilient supply chain. *The International Journal of Logistics Management, 15*(2), 1–14. https://doi.org/10.1108/09574090410700275

Coden, M., Close, K., Bohmayr, W., Winkler, K., & Thorson, B. (2020). Managing the cyber risks of remote work. *Boston Consulting Group*. 〈https://www.bcg.com/en-us/publications/2020/covid-remote-work-cyber-security.aspx〉.

Cohen, J. (1988). Statistical Power Analysis for the Behavioral Sciences. *Statistical Power Analysis for the Behavioral Sciences*. New York: Routledge.

Coles-Kemp, L., & Hansen, R.R. (2017). Walking the line: The everyday security ties that bind. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 10292 LNCS, 464–480. https://doi.org/10.1007/978–3-319–58460-7_32.

Colicchia, C., Creazza, A., & Menachof, D. A. (2019). Managing cyber and information risks in supply chains: insights from an exploratory analysis. *Supply Chain Management, 24*(2), 215–240. https://doi.org/10.1108/SCM-09-2017-0289

Connolly, L. Y., Lang, M., Gathegi, J., & Tygar, D. J. (2017). Organisational culture, procedural countermeasures, and employee security behaviour A qualitative study. *Information and Computer Security, 25*(2), 118–136. https://doi.org/10.1108/ICS-03-2017-0013

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers and Security, 32*, 90–101. https://doi.org/10.1016/j.cose.2012.09.010

Dabhilkar, M., Birkie, S. E., & Kaulio, M. (2016). Supply-side resilience as practice bundles: a critical incident study. *International Journal of Operations and Production Management, 36*(8), 948–970. https://doi.org/10.1108/IJOPM-12-2014-0614

Dahles, H., & Susilowati, T. P. (2015). Business resilience in times of growth and crisis. *Annals of Tourism Research, 51*, 34–50. https://doi.org/10.1016/j.annals.2015.01.002

Demirel, G., Maccarthy, B. L., Ritterskamp, D., Champneys, A. R., & Gross, T. (2019). Identifying dynamical instabilities in supply networks using generalized modeling. *Journal of Operations Management, 65*(2), 136–159. https://doi.org/10.1002/joom.1005

Donalds, C., & Osei-Bryson, K. M. (2020). Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents. *International Journal of Information Management, 51*, Article 102056. https://doi.org/10.1016/j.ijinfomgt.2019.102056

Dwivedi, Y. K., Janssen, M., Slade, E. L., Rana, N. P., Weerakkody, V., Millard, J., … Snijders, D. (2017). Driving innovation through big open linked data (BOLD): Exploring antecedents using interpretive structural modelling. *Information Systems Frontiers, 19*(2), 197–212. https://doi.org/10.1007/S10796-016-9675-5/FIGURES/2

Dwivedi, Y. K., Hughes, D. L., Coombs, C., Constantiou, I., Duan, Y., Edwards, J. S., … Upadhyay, N. (2020). Impact of COVID-19 pandemic on information management research and practice: Transforming education, work and life. *International Journal of Information Management, 55*, Article 102211. https://doi.org/10.1016/j.ijinfomgt.2020.102211

Esteves, J., Ramalho, E., & De Haro, G. (2017). *To improve cybersecurity, think like a hacker*. MIT Sloan Management Review. 〈https://sloanreview.mit.edu/article/to-improve-cybersecurity-think-like-a-hacker/〉.

Ghadge, A., Weiß, M., Caldwell, N. D., & Wilding, R. (2019). Managing cyber risk in supply chains: a review and research agenda. In *Supply Chain Management, 25* pp. 223–240). Emerald Group Publishing Ltd. https://doi.org/10.1108/SCM-10-2018-0357

Hair, J. F., Jr., Sarstedt, M., Ringle, C. M., & S. P. G. (2017). *Advanced Issues in Partial Least Squares Structural Equation Modeling*. Sage Publications.

Hanus, B., & Wu, Y., "Andy." (2016). Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. *Information Systems Management, 33*(1), 2–16. https://doi.org/10.1080/10580530.2015.1117842

He, Y., Zamani, E. D., Lloyd, S., & Luo, C. (2022). Agile incident response (AIR): Improving the incident response process in healthcare. *International Journal of Information Management, 62*, Article 102435. https://doi.org/10.1016/J.IJINFOMGT.2021.102435

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106–125. https://doi.org/10.1057/ejis.2009.6

Hew, J. J., Tan, G. W. H., Lin, B., & Ooi, K. B. (2017). Generating travel-related contents through mobile social tourism: Does privacy paradox persist? *Telematics and Informatics, 34*(7), 914–935. https://doi.org/10.1016/j.tele.2017.04.001

Hijji, M., & Alam, G. (2021). A multivocal literature review on growing social engineering based cyber-attacks/threats during the COVID-19 pandemic: Challenges and prospective solutions. *IEEE ACCESS, 9*, 7152–7169. https://doi.org/10.1109/ACCESS.2020.3048839

Hina, S., Panneer Selvam, D. D. D., & Lowry, P. B. (2019). Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world. *Computers and Security, 87*, Article 101594. https://doi.org/10.1016/j.cose.2019.101594

Hohenstein, N. O., Feise, E., Hartmann, E., & Giunipero, L. (2015). Research on the phenomenon of supply chain resilience: A systematic review and paths for further investigation. *International Journal of Physical Distribution and Logistics Management, 45*, 90–117. https://doi.org/10.1108/IJPDLM-05-2013-0128

Hosseini, S., Ivanov, D., & Dolgui, A. (2019). Review of quantitative methods for supply chain resilience analysis. *Transportation Research Part E Logistics and Transportation Review, 125*, 285–307. https://doi.org/10.1016/j.tre.2019.03.001

Hu, Q., Hart, P., & Cooke, D. (2007). The role of external and internal influences on information systems security - a neo-institutional perspective. *Journal of Strategic Information Systems, 16*(2), 153–172. https://doi.org/10.1016/j.jsis.2007.05.004

Ifinedo, P. (2011). An empirical analysis of factors influencing internet/e-business technologies adoption by smes in Canada. *International Journal of Information Technology and Decision Making, 10*(4), 731–766. https://doi.org/10.1142/S0219622011004543

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers and Security, 31*(1), 83–95. https://doi.org/10.1016/j.cose.2011.10.007

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information and Management, 51*(1), 69–79. https://doi.org/10.1016/j.im.2013.10.001

Ivanov, D. (2019). Disruption tails and revival policies: A simulation analysis of supply chain design and production-ordering systems in the recovery and post-disruption periods. *Computers and Industrial Engineering, 127*, 558–570. https://doi.org/10.1016/j.cie.2018.10.043

Ivanov, D. (2020aaa). Predicting the impacts of epidemic outbreaks on global supply chains: A simulation-based analysis on the coronavirus outbreak (COVID-19/SARS-CoV-2) case. *Transportation Research Part E Logistics and Transportation Review, 136*, Article 101922. https://doi.org/10.1016/j.tre.2020.101922

Ivanov, D. (2020bbb). 'A blessing in disguise' or 'as if it wasn't hard enough already': Reciprocal and aggravate vulnerabilities in the supply chain. *International Journal of Production Research, 58*(11), 3252–3262. https://doi.org/10.1080/00207543.2019.1634850

Ivanov, D., & Dolgui, A. (2020). Viability of intertwined supply networks: extending the supply chain resilience angles towards survivability. A position paper motivated by COVID-19 outbreak. *International Journal of Production Research, 58*(10), 2904–2915. https://doi.org/10.1080/00207543.2020.1750727

Ivanov, D., Dolgui, A., & Sokolov, B. (2019). The impact of digital technology and Industry 4.0 on the ripple effect and supply chain risk analytics. *International Journal of Production Research, 57*(3), 829–846. https://doi.org/10.1080/00207543.2018.1488086

Ivanov, D., Dolgui, A., Sokolov, B., & Ivanova, M. (2017). Literature review on disruption recovery in the supply chain*. *International Journal of Production Research, 55*(20), 6158–6174. https://doi.org/10.1080/00207543.2017.1330572

Jaeger, L., & Eckhardt, A. (2021). Eyes wide open: The role of situational information security awareness for security-related behaviour. *Information Systems Journal, 31*(3), 429–472. https://doi.org/10.1111/ISJ.12317

Jalali, M. S., Siegel, M., & Madnick, S. (2019). Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment. *Journal of Strategic Information Systems, 28*(1), 66–82. https://doi.org/10.1016/j.jsis.2018.09.003

Janssen, M., Rana, N.P., Slade, E.L., & Dwivedi, Y.K. (2017). Trustworthiness of digital government services: deriving a comprehensive theory through interpretive structural modelling. Https://Doi.Org/10.1080/14719037.2017.1305689, 20(5), 647–671. https://doi.org/10.1080/14719037.2017.1305689.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information s ecurity behaviors: An empirical study. *MIS Quarterly Management Information Systems, 34*, 549–566. https://doi.org/10.2307/25750691 (SPEC. ISSUE 3).

Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly Management Information Systems, 39*(1), 113–134. https://doi.org/10.25300/MISQ/2015/39.1.06

Johnston, A.C., Warkentin, M., McBride, M., & Carter, L. (2017). Dispositional and situational factors: influences on information security policy violations. Https://Doi.Org/10.1057/Ejis.2015.15, 25(3), 231–251. https://doi.org/10.1057/EJIS.2015.15.

Kabanda, S., Tanner, M., & Kent, C. (2018). Exploring SME cybersecurity practices in developing countries. *Journal of Organizational Computing and Electronic Commerce, 28*(3), 269–282. https://doi.org/10.1080/10919392.2018.1484598

Kim, K., & Bui, L. (2019). Learning from Hurricane Maria: Island ports and supply chain resilience. *International Journal of Disaster Risk Reduction, 39*, Article 101244. https://doi.org/10.1016/j.ijdrr.2019.101244

Kim, M. J., Lee, C. K., & Jung, T. (2020). Exploring consumer behavior in virtual reality tourism using an extended stimulus-organism-response model. *Journal of Travel Research, 59*(1), 69–89. https://doi.org/10.1177/0047287518818915

Kinra, A., Ivanov, D., Das, A., & Dolgui, A. (2019). Ripple effect quantification by supplier risk exposure assessment. *International Journal of Production Research*. https://doi.org/10.1080/00207543.2019.1675919

Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers and Security*, *105*. https://doi.org/10.1016/j.cose.2021.102248

Lee, C., & Hallak, R. (2020). Investigating the effects of offline and online social capital on tourism SME performance: A mixed-methods study of New Zealand entrepreneurs. *Tourism Management, 80*, Article 104128. https://doi.org/10.1016/j.tourman.2020.104128

Lee, V. H., Hew, J. J., Leong, L. Y., Tan, G. W. H., & Ooi, K. B. (2020). Wearable payment: A deep learning-based dual-stage SEM-ANN analysis. *Expert Systems with Applications, 157*, Article 113477. https://doi.org/10.1016/j.eswa.2020.113477

Lewis, R., Louvieris, P., Abbott, P., Clewley, N., & Jones, K. (2014). Cybersecurity information sharing: A framework for information security management in UK SME supply chains. ECIS 2014 Proceedings - 22nd European Conference on Information Systems.

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. https://doi.org/10.1016/J.IJINFOMGT.2018.10.017

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems, 11*(7), 394–413. https://doi.org/10.17705/1jais.00232

Liang, H., Saraf, N., Hu, Q., & Xue, Y. (2007). Assimilation of enterprise systems: The effect of institutional pressures and the mediating role of top management. *MIS Quarterly: Management Information Systems, 31*(1), 59–87. https://doi.org/10.2307/25148781

Lim, X. J., Ng, S. I., Basha, N. K., Cheah, J. H., & Ting, H. (2020). To move or not to move? A study of sustainable retirement village in Malaysia. *Current Psychology*, 1–17. https://doi.org/10.1007/s12144-020-00734-z

Liu, Y., Srai, J. S., & Evans, S. (2016). Environmental management: The role of supply chain capabilities in the auto sector. *Supply Chain Management, 21*(1), 1–19. https://doi.org/10.1108/SCM-01-2015-0026/FULL/XML

Loh, X. K., Lee, V. H., Loh, X. M., Tan, G. W. H., Ooi, K. B., & Dwivedi, Y. K. (2021). The dark side of mobile learning via social media: how bad can it get? *Information Systems Frontiers*, 1–18. https://doi.org/10.1007/s10796-021-10202-z

Loh, X. M., Lee, V. H., Tan, G. W. H., Hew, J. J., & Ooi, K. B. (2019). Towards a cashless society: The imminent role of wearable technology. *Journal of Computer Information Systems*. https://doi.org/10.1080/08874417.2019.1688733

Lu, Y., Wu, J., Peng, J., & Lu, L. (2020). The perceived impact of the Covid-19 epidemic: Evidence from a sample of 4807 SMEs in Sichuan Province, China. *Environmental Hazard.*, 1–18. https://doi.org/10.1080/17477891.2020.1763902

Lücker, F., Seifert, R. W., & Biçer, I. (2019). Roles of inventory and reserve capacity in mitigating supply chain disruption risk. *International Journal of Production Research, 57*(4), 1238–1249. https://doi.org/10.1080/00207543.2018.1504173

Manso, C. G., Rekleitis, E., Papazafeiropoulos, F., & Maritsas, V. (2015). Information security and privacy standards for SMEs. *European Union Agency for Network and Information Security*. https://doi.org/10.2824/829076

Martens, M., De Wolf, R., & De Marez, L. (2019). Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general. *Computers in Human Behavior, 92*, 139–150. https://doi.org/10.1016/j.chb.2018.11.002

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. https://doi.org/10.1080/07421222.2017.1394083

Menard, P., Warkentin, M., & Lowry, P. B. (2018). The impact of collectivism and psychological ownership on protection motivation: A cross-cultural examination. *Computers and Security, 75*, 147–166. https://doi.org/10.1016/j.cose.2018.01.020

Namdar, J., Li, X., Sawhney, R., & Pradhan, N. (2018). Supply chain resilience for single and multiple sourcing in the presence of disruption risks. *International Journal of Production Research, 56*(6), 2339–2360. https://doi.org/10.1080/00207543.2017.1370149

Ng, F. Z. X., Yap, H. Y., Tan, G. W. H., Lo, P. S., & Ooi, K. B. (2022). Fashion shopping on the go: A Dual-stage predictive-analytics SEM-ANN analysis on usage behaviour, experience response and cross-category usage. *Journal of Retailing and Consumer Services, 65*, Article 102851. https://doi.org/10.1016/j.jretconser.2021.102851

NIST. (2015). Best practices in cyber supply chain risk management. *Conference Materials*, 1–3.

Nycz, M., Martin, M.J., & Polkowski, Z. (2015). The cyber security in SMEs in Poland and Tanzania. Proceedings of the 2015 7th International Conference on Electronics, Computers and Artificial Intelligence, ECAI 2015, AE27–AE34. https://doi.org/10.1109/ECAI.2015.7301182.

Papadopoulos, T., Baltas, K. N., & Balta, M. E. (2020). The use of digital technologies by small and medium enterprises during COVID-19: Implications for theory and practice. *International Journal of Information Management, 55*, Article 102192. https://doi.org/10.1016/j.ijinfomgt.2020.102192

Paulsen, C. (2016). Cybersecuring small businesses. *Computer, 49*(8), 92–97. https://doi.org/10.1109/MC.2016.223

Pettit, T. J., Fiksel, J., & Croxton, K. L. (2010). Ensuring supply chain resilience: Development of a conceptual framework. *Journal of Business Logistics, 31*(1), 1–21. https://doi.org/10.1002/j.2158-1592.2010.tb00125.x

Pettit, T. J., Croxton, K. L., & Fiksel, J. (2013). Ensuring supply chain resilience: development and implementation of an assessment tool. *Journal of Business Logistics, 34*(1), 46–76. https://doi.org/10.1111/JBL.12009@10.1111/(ISSN)2158-1592.RESEARCH-ON-SUPPLY-CHAINS-IN-CRISIS

Queiroz, M. M., Ivanov, D., Dolgui, A., & Wamba, S. F. (2020). Impacts of epidemic outbreaks on supply chains: Mapping a research agenda amid the COVID-19 pandemic through a structured literature review. *Annals of Operations Research*. https://doi.org/10.1007/s10479-020-03685-7

Rahul De', Pandey, N., & Pal, A. (2020). Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practice. *International Journal of Information Management, 55*, Article 102171. https://doi.org/10.1016/J.IJINFOMGT.2020.102171

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The Journal of Psychology, 91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Sadok, M., Alter, S., & Bednar, P. (2020). It is not my job: Exploring the disconnect between corporate security policies and actual security practices in SMEs. *Information and Computer Security, 28*(3), 467–483. https://doi.org/10.1108/ICS-01-2019-0010

Santos-Olmo, A., Sánchez, L., Caballero, I., Camacho, S., & Fernandez-Medina, E. (2016). The importance of the security culture in SMEs as regards the correct management of the security of their assets. *Future Internet, 8*(4), 30. https://doi.org/10.3390/fi8030030

Sarkis, J. (2020). Supply chain sustainability: Learning from the COVID-19 pandemic. *International Journal of Operations and Production Management, 41*(1), 63–73. https://doi.org/10.1108/IJOPM-08-2020-0568

Schleper, M. C., Gold, S., Trautrims, A., & Baldock, D. (2021). Pandemic-induced knowledge gaps in operations and supply chain management: COVID-19′s impacts on retailing. *International Journal of Operations & Production Management, 41*(3), 193–205. https://doi.org/10.1108/IJOPM-12-2020-0837

Shaheen, I., Azadegan, A., Hooker, R., Lucianetti, L., Shaheen, I., Hooker, R., … Lucianetti, L. (2019). Leadership for mitigating ripple effects in supply chain disruptions: A paradoxical role. *International Series in Operations Research & Management Science, 276*. https://doi.org/10.1007/978-3-030-14302-2_5

Sharma, S., Singh, G., Sharma, R., Jones, P., Kraus, S., & Dwivedi, Y. K. (2020). Digital health innovation: Exploring adoption of COVID-19 digital contact tracing apps. *IEEE Transactions on Engineering Management*. https://doi.org/10.1109/TEM.2020.3019033

Shillair, R., Cotten, S. R., Tsai, H. Y. S., Alhabash, S., Larose, R., & Rifon, N. J. (2015). Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior, 48*, 199–207. https://doi.org/10.1016/j.chb.2015.01.046

Shmueli, G., Ray, S., Velasquez Estrada, J. M., & Chatla, S. B. (2016). The elephant in the room: Predictive performance of PLS models. *Journal of Business Research, 69*(10), 4552–4564. https://doi.org/10.1016/j.jbusres.2016.03.049

Simon, J., & Omar, A. (2020). Cybersecurity investments in the supply chain: Coordination and a strategic attacker. *European Journal of Operational Research, 282*(1), 161–171. https://doi.org/10.1016/j.ejor.2019.09.017

Siponen, M., Adam Mahmood, M., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information and Management, 51*(2), 217–224. https://doi.org/10.1016/j.im.2013.08.006

Stacey, P., Taylor, R., Olowosule, O., & Spanaki, K. (2021). Emotional reactions and coping responses of employees to a cyber-attack: A case study. *International Journal of Information Management, 58*, Article 102298. https://doi.org/10.1016/j.ijinfomgt.2020.102298

Tan, G. W. H., & Ooi, K. B. (2018). Gender and age: Do they really moderate mobile tourism shopping behavior? *Telematics and Informatics, 35*(6), 1617–1642. https://doi.org/10.1016/j.tele.2018.04.009

Tew, H. T., Tan, G. W. H., Loh, X. M., Lee, V. H, Lim, W. L., & Ooi, K. B. (2021). Tapping the next purchase: embracing the wave of mobile payment. *Journal of Computer Information Systems, 62*(3), 527–535. https://doi.org/10.1080/08874417.2020.1858731

Urciuoli, L., & Hintsa, J. (2017). Adapting supply chain management strategies to security–an analysis of existing gaps and recommendations for improvement. *International Journal of Logistics Research and Applications, 20*(3), 276–295. https://doi.org/10.1080/13675567.2016.1219703

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 and Management, 56*(8), Article 103157. https://doi.org/10.1016/j.im.2019.03.002

Wan, S. M., Cham, L. N., Tan, G. W. H., Lo, P. S., Ooi, K. B., & Chatterjee, R. S. (2021). What's Stopping You from Migrating to Mobile Tourism Shopping? *Journal of Computer Information Systems*, 1–16. https://doi.org/10.1080/08874417.2021.2004564

Wang, J. W., Gao, F., & Ip, W. H. (2010). Measurement of resilience and its application to enterprise information systems. *Enterprise Information Systems, 4*(2), 215–223. https://doi.org/10.1080/17517571003754561

Warkentin, M., Johnston, A. C., Shropshire, J., & Barnett, W. D. (2016). Continuance of protective security behavior: A longitudinal study. *Decision Support Systems, 92*, 25–35. https://doi.org/10.1016/j.dss.2016.09.013

Wedawatta, G., & Ingirige, B. (2012). Resilience and adaptation of small and medium-sized enterprises to flood risk. *Disaster Prevention and Management: An International Journal, 21*(4), 474–488. https://doi.org/10.1108/09653561211256170

Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and Information Security Awareness. *Computers and Security, 88*, Article 101640. https://doi.org/10.1016/j.cose.2019.101640

Woltjer, R. (2017). Workarounds and trade-offs in information security-An exploratory study. *Information and Computer Security, 25*(4), 402–420. https://doi.org/10.1108/ICS-02-2016-0017

Wong, C. H., Tan, G. W. H., Loke, S. P., & Ooi, K. B. (2014). Mobile TV: a new form of entertainment? *Industrial Management & Data Systems, 114*(7), 1050–1067. https://doi.org/10.1108/IMDS-05-2014-0146

Wong, C. H., Tan, G. W. H., Ooi, K. B., & Lin, B. (2015). Mobile shopping: the next frontier of the shopping industry? An emerging market perspective. *International Journal of Mobile Communications, 13*(1), 92–112. https://doi.org/10.1504/IJMC.2015.065892

Wong, L. W., Leong, L. Y., Hew, J. J., Tan, G. W. H., & Ooi, K. B. (2020). Time to seize the digital evolution: Adoption of blockchain in operations and supply chain management among Malaysian SMEs. *International Journal of Information Management, 52*, Article 101997. https://doi.org/10.1016/J.IJINFOMGT.2019.08.005

Wong, L. W., Tan, G. W. H., Lee, V. H., Ooi, K. B., & Sohal, A. (2020). Unearthing the determinants of Blockchain adoption in supply chain management. *International Journal of Production Research, 58*(7), 2100–2123. https://doi.org/10.1080/00207543.2020.1730463

Wong, L.-W., Tan, G. W.-H., Lee, V.-H., Ooi, K.-B., & Sohal, A. (2021). Psychological and system-related barriers to adopting blockchain for operations management: An artificial neural network approach. *IEEE Transactions on Engineering Management*, 1–15. https://doi.org/10.1109/TEM.2021.3053359

Xue, L., Zhang, C., Ling, H., & Zhao, X. (2013). Risk mitigation in supply chain digitization: System modularity and information technology governance. *Journal of Management Information Systems, 30*(1), 325–352. https://doi.org/10.2753/MIS0742-1222300110

Yan, L. Y., Tan, G. W. H., Loh, X. M., Hew, J. J., & Ooi, K. B. (2021). QR Code and Mobile Payment: The disruptive forces in retail. *Journal of Retailing and Consumer Services, 58*, Article 102300.

Yuan, Y. P., Tan, G. W. H., Ooi, K. B., & Lim, W. L. (2021). Can COVID-19 pandemic influence experience response in mobile learning? *Telematics and Informatics, 64*, Article 101676. https://doi.org/10.1016/j.tele.2021.101676

Zhang, X., Liu, S., Chen, X., Wang, L., Gao, B., & Zhu, Q. (2018). Health information privacy concerns, antecedents, and information disclosure intention in online health communities. *Information and Management, 55*(4), 482–493. https://doi.org/10.1016/j.im.2017.11.003

Zhao, K., Scheibe, K., Blackhurst, J., & Kumar, A. (2019). Supply chain network robustness against disruptions: Topological analysis, measurement, and optimization. *IEEE Transactions on Engineering Management, 66*(1), 127–139. https://doi.org/10.1109/TEM.2018.2808331

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H.N. (2020). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. Https://Doi.Org/10.1080/08874417.2020.1712269. https://doi.org/10.1080/08874417.2020.1712269.