Available online at www.sciencedirect.com

ScienceDirect

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

Computers & Security

Impact of comprehensive information security awareness and cognitive characteristics on security incident management – an empirical study

Manisekaran Thangavelu[1], *Venkataraghavan Krishnaswamy*[1,*], *Mayank Sharma*[1]

Information Technology & Systems Area, Indian Institute of Management Kashipur, Kashipur, India

ARTICLE INFO

Article history:
Received 25 March 2021
Revised 7 June 2021
Accepted 7 July 2021
Available online 13 July 2021

Keywords:
Security awareness
Situation awareness
System awareness
Self-efficacy
Metacognitive awareness
Security incident management

ABSTRACT

Organizations deploy a team of dedicated security professionals and spend significant resources safeguarding their digital assets. Despite best efforts, security incidents are on the rise and remain a key challenge. The literature has focused inadequately on the lack of professionals' awareness of security, system, or situational aspects. Extant literature on the impact of awareness on threat management tasks is disjointed and does not adequately consider the metacognitive awareness and self-efficacy of security professionals. To this effect, we propose and empirically validate a model to study the relationship between security, system, situational awareness, and security professionals' ability to detect, assess, and mitigate threats. We also investigate the effects of metacognitive awareness and self-efficacy on the relationship between awareness and threat management tasks. We validate the model using a survey of 100 information security professionals. Results indicate a significant relationship between awareness, metacognitive awareness, self-efficacy, and threat management task performance. The analysis also demonstrates that metacognitive awareness and self-efficacy mediated the impact of awareness on threat management task performance. We discuss the effects and implications of this study for practice and research.

1. Introduction

Organizations need to protect their sensitive information and critical digital assets from external and internal threats. Threats may lead to information security incidents if not managed on time and may also result in financial and reputational losses besides disrupting business continuity (Singh and Cobbe, 2019; Tosun, 2021). Organizations implement security incident management (SIM), an incident response process, as a proactive defense to prevent incidents. SIM involves monitoring various events across systems and networks by skilled security professionals who identify and respond to any adverse security events on time. Despite significant resources spent by the organization, reports indicate an increasing trend in information security incidents (PwC, 2015). We use the term 'security' and 'information security' interchangeably in this paper.

* Corresponding author.
E-mail addresses: manishekaran.efpm2014@iimkashipur.ac.in (M. Thangavelu), venkat.krishnaswamy@iimkashipur.ac.in (V. Krishnaswamy), mayank.sharma@iimkashipur.ac.in (M. Sharma).
[1] www.iimkashipur.ac.in

https://doi.org/10.1016/j.cose.2021.102401

Industry studies and academic research have identified the causes of ineffective SIM from both technical and human perspectives. Among technical factors, the lack of sufficient tools and their poor use are predominant reasons (Oltsik, 2015). Among human factors, studies regard "awareness" as critical to effective incident management. The industry reports attribute ineffective security incident response to lack of awareness of (a) attack methodologies, (b) scope of the attacks, (c) system behavior, (d) system vulnerability, (e) system architecture, and (f) threat situations (Oltsik, 2015; Ponemon, 2019). On the other hand, academic studies emphasize the essentiality of the above factors for threat management in SIM (Yang et al., 2008; Alberts et al., 2004; D'Amico et al., 2005).

While the studies mentioned above provide several pointers toward the significance of awareness in incident response, there are two key challenges. One is to understand what constitutes awareness, and the other is how awareness translates into effective incident response. The motivation for this study stems from these challenges, and we address them by considering the literature on awareness, metacognition, and self-efficacy.

Regarding the first challenge of what constitutes awareness, studies describe the factors related to the system, situational, and security dimensions. Merriam-Webster dictionary defines awareness as "the quality or state of being aware: knowledge and understanding that something is happening or exists." Oxford dictionary defines awareness as "knowing something: knowing that something exists and is important." Bulgurcu et al. (2010, p.4) defined general information security awareness as employees' "overall knowledge and understanding of potential issues related to information security and their ramifications." Similarly, in this work, we consider awareness as a security professional's overall knowledge and understanding of practices, methods, systems, and their ramifications, directed at planning, monitoring, strategizing and executing tasks for incident management. The literature reveals three dimensions of awareness: security, system, and situational (Thangavelu et al., 2020). Security awareness is knowledge about the execution of security attacks. It deals with elements such as tactics, techniques, and procedures (TTPs) adopted by an attacker, attack methodologies, and understanding key indicators of compromise and motives behind attacks (Killcrece et al., 2003; Cichonski et al., 2012). System awareness refers to knowledge of normal and abnormal behavior of systems experiencing attacks, the system's importance to business, architecture details, the system's controls against attacks (Alberts et al., 2004), and a comprehensive view of IT assets (PwC, 2015; Oltsik, 2015). Situational awareness is knowledge about and the ability to correlate various events and states of systems with one's experience and other additional data from external sources to arrive at the contexts and states of attacks to determine past, current, and future states of attacks (D'Amico et al., 2005).

Regarding the second challenge of how awareness translates into effective threat management, we consider the literature related to metacognition and self-efficacy. Metacognition impacts task performance, especially those characterized by uncertainty and information overload, such as threat management. Metacognition literature shows that the performance of complex tasks requires a high degree of planning, monitoring, and evaluation connected to the regulation of cognition. Performance is also related to organizing and using the correct information and strategizing effectively, which are connected to the cognition of knowledge (Hogan et al., 2014). Awareness enhances the components of metacognitive awareness, namely the regulation of cognition and the knowledge of cognition (Eteläpelto, 1993). On the one hand, self-efficacy has been shown to enhance complex task performance (Bandura, 1994; Tzeng, 2009). On the other hand, Phelps et al. (2006) discuss how self-efficacy aids in persisting with them despite obstacles and challenges. This work shows how threat management tasks (TMTs), including threat detection, threat assessment, and threat mitigation, are affected by security professionals' awareness, metacognitive awareness, and self-efficacy.

To the best of our knowledge, the literature has not discussed the combined effect of the three dimensions of awareness and the role of the cognitive characteristics of security professionals on the performance of TMTs. Toward these effects, this work attempts to (1) empirically validate the effect of security, system, and situational awareness on TMT in the context of security professionals and (2) investigate the effect of cognitive elements of the relationship between awareness dimensions and TMT. The significance of this study is that the findings will offer insights into how awareness translates into TMT performance. Understanding the role of cognitive elements in SIM helps deepen understanding of professionals' threat management dynamics.

The article is structured as follows. Section 2 provides a literature review on TMTs, awareness, cognitive characteristics, and the research gaps. We discuss the theory and model development in Section 3. Section 4 describes the research methodology, data collection, and discussion of the results. Section 5 discusses the implications of the practice and research. Finally, the scope for future work is presented in Section 6, followed by limitations and conclusions in the final section.

2. Literature review

This section provides a background on (a) TMTs, (b) awareness, and (c) metacognition and establishes the research gaps.

2.1. *Threat management tasks*

Security threats emerge from any act that may cause harm to digital assets, and any event that arises from such threats leading to an impact on an organization is a security incident (Wilson et al., 1998). Literature provides various approaches and directions on SIM. For example, Wiik and Kossakowski (2005) describe a system dynamic approach, and Mitropoulos et al. (2006) delineated a synthesized approach to incident response. Zhang et al. (2009) presented a method for measuring attack impact by using the evidence of intrusion alerts and building rational incident response using cost-benefit analysis. Ahmad et al. (2012) studied the challenges and existing gaps in security incident response. Furthermore, Bartnes and Moe (2017) identified the challenges in incident response and described the impact of preparedness

to perform incident response tasks (Bartnes and Moe, 2017). Another study focused on building forensic investigation capabilities (Turner, 2006), while Knight and Nurse (2020) proposed a framework for post-incident activities, such as corporate communication. Recent studies have developed frameworks for real-time analytics to improve incident responses (Naseer et al., 2021).

SIM frameworks provide a canvas for activities aimed at preventing and curating security threats to avoid or manage business disruptions. In its release SP-800–61:R2 (Cichonski et al., 2012), the NIST outlines four stages in SIM. Stage 1 involves preparing and planning for the organization's readiness to respond to an incident. Stage 2 involves the tasks of detection and assessment. Threat detection involves monitoring events across all network nodes and segregating key indicators from these events, thereby determining the nature of the identified events from a security perspective (ISO 27035; Clark et al., 2007). Threat assessment deals with understanding the impact of any threats from events that can likely damage an organization (Werlinger et al., 2010). Stage 3 involves threat mitigation, which consists of security measures to eliminate attacks and restore the impacted system to its original state (Cichonski et al., 2012). Stage 4 involves activities related to post-incident analysis, such as root cause analysis. In this work, we are concerned with awareness related to the performance of threat detection, threat assessment, and threat mitigation.

2.2. *Awareness and threat management tasks*

Goodhue and Straub (1991) and, later, Straub and Welke (1998) evaluated the role of security managers' awareness in reducing incidents. After them, the predominant focus of studies has been on raising end-user awareness of security issues (Kruger and Kearney, 2006; Chen et al., 2006). Awareness of security professionals is different in context and concept from the general security awareness of employees in an organization. For security professionals, awareness is overall knowledge and understanding of practices, policies, methods, systems, and their ramifications, directed at planning, monitoring, strategizing and executing tasks for incident management. In other words, awareness is directed towards improving the performance of the TMT (Killcrece et al., 2003) and is the foundation upon which domain knowledge is continuously built (Trevethan 2017; Phelps et al., 2006). It is necessary for security professionals to have awareness from various perspectives (Ponemon, 2019). Table 1 summarizes information security awareness studies from the perspective of security professionals. We present select literature on security, systems, and situational awareness here.

2.2.1. *Security awareness*

Security awareness is the knowledge about the execution of security attacks. It provides knowledge about TTPs adopted for a specific attack and the motives of the attack. Security awareness of an attack helps to decipher the critical indicators of compromise (IOCs) and indicators of attacks (IOAs) and to construct attack situations (Cichonski et al., 2012; Fireeye, 2012). IOCs indicate the payloads of exploits, and IOAs indicate how payloads are weaponized, which creates a specific pattern across systems. On the other hand, awareness of the motives and capabilities of an attacker helps to judge the systems impacted by assessing how TTPs exploit vulnerabilities (Yang et al., 2008). Security awareness can help reduce false positives (Voitovych et al., 2016) and improve threat detection and assessment (Brown and Lee, 2019; Liu et al., 2010).

2.2.2. *System awareness*

System awareness is the knowledge related to systems in the network and their role in the organization's mission, inherent vulnerabilities, effects, and behavior of systems. Awareness of systems and network responses to specific attacks is essential to confirm detected threats and build the situational awareness needed for assessment and mitigation. In this regard, investigating these threats requires a comprehensive view of IT assets, the role of systems in the organization's business mission, existing vulnerabilities in the assets, and the behavior of systems upon the exploitation of such vulnerabilities and their impact on the business service (Alberts et al., 2004; Oltsik, 2015; Yang et., 2008). For example, when a system generates anomalous traffic connecting to multiple systems in the network, the behavioral pattern might explain how stages of attack are executed in a network and understand TTPs (Yuill et al., 2000). This helps to identify all the systems vulnerable to the threat and the scope of the attack. Similarly, awareness of the existing defense controls and architecture helps to judge which systems in the network are prone to impact and focus on the prioritization of remediation. In summary, system awareness concerns system behavior, existing vulnerabilities, defense controls, and the role of systems in achieving the business mission.

2.2.3. *Situation awareness*

Situational awareness is the knowledge about the state of attacks and situations of the imminent past, current, and projected future state through event visualization. Endsley (1995, p.4) defined situational awareness as "the perception of the elements (here, threats) in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status shortly." In the context of cybersecurity, it is related to monitoring and correlation of various system events and deriving the meaningful patterns of an attack (threat perception), comprehending the patterns by applying one's personal experience or available additional information (threat comprehension), and finally determining the future state of the attack (threat projection) (Franke and Brynielsson, 2014; D'Amico et al., 2005). Situational awareness helps in understanding the scope of attack by generating hypotheses (D'Amico et al., 2005; D'Amico and Kocka, 2005), decision making (Onwubiko, 2009), and depicting states of attack (Cheng et al., 2012).

Situational awareness is essential to performing TMT, as security attacks are dynamic and evolve from time to time (Franke and Brynielsson, 2014; D'Amico et al., 2005a; Onwubiko, 2009; Alberts et al., 2004). When professionals possess the awareness to identify and track network and system behavior indicators, they can perceive the threats in the environment. However, comprehending threats requires the ability to integrate necessary secondary information from prior

Table 1 – Information security awareness studies on TMT for security professionals

Author and study area	Awareness dimension			Threat management tasks			Cognitive factors (Yes/No)	Method
	SecA	SitA	SysA	TD	TA	TM		
Goodhue and Straub (1991) Model of managerial perceptions of systems risk	Y	Y	N	N	N	Y	N	Case study
Straub and Welke (1998) Coping with system risk and security awareness	Y	Y	N	N	N	N	N	Case study
Yuill et al. (2000) Knowledge of vulnerable assets and capability, intent, and opportunity and cyber-attack detection	Y	N	Y	Y	N	N	Y	Experiment
Tan et al. (2003) Factors influencing managers in their decision not to perform security investigations	N	Y	N	Y	Y	N	N	Case study
Alberts et al. (2004) Effect of systems and assets, business mission, the effect of threats, malicious activities in threat assessment and mitigation	N	Y	Y	N	Y	Y	N	Conceptual
Yang et al. (2008) Enhanced cyber situational view of plausible futures for network security analysts	Y	Y	N	Y	Y	Y	N	Experiment
Erbacher et al. (2010) Cognitive task analysis of network analysts and managers	N	Y	N	Y	Y	Y	N	Conceptual
Cheng et al. (2012) Integrated cyberspace situational awareness system for efficient cyber-attack detection, analysis, and mitigation	Y	Y	N	Y	Y	Y	N	Experiment
Ruefle and Murray. (2014) Situational awareness and incident response	N	Y	N	Y	Y	N	N	Conceptual
Voitovych et al. (2016) Removal of false-positive events and focus on critical indicators	Y	N	N	Y	N	N	N	Empirical
Brown and Lee (2019) Enhancing threat detection using cyber threat intelligence	Y	Y	N	Y	Y	N	N	Empirical
Rongrong et al. (2018) Enhancing cyber situational awareness using threat, vulnerability for security professionals	N	Y	Y	Y	N	N	N	Experiment

Note: SecA – Security Awareness, SitA – Situational awareness, SysA – System awareness, TD – Threat detection, TA –Threat assessment, TM – Threat mitigation.

experience or other information from external sources. Projecting the threat will require more information across diverse systems to deduce probable future scenarios by correlating all the information available thus far. Perception provides a better focus on threat detection. Comprehension helps in an accurate threat assessment (Liu et al., 2010; Alberts et al., 2004) and mitigation (Mathew, 2005). Projection enhances the comprehensive visibility of threats and provides insights into possible futuristic impacts (Oltsik, 2015; Ruefle and Murray, 2014), thereby enabling security professionals to develop correct remediation measures.

While the factors of security awareness are related to the execution of security attacks, system awareness is related to how systems respond to threats, and situational awareness relates to how one can use various information from internal and external sources. Based on the discussion above, a summary of the literature on awareness and TMT is presented in Table 1.

2.3. *Metacognition and self-efficacy*

TMTs are complex, dynamic, and context-oriented. It involves considerable human efforts, as the tasks have a high degree of uncertainty; they evolve and unfold, requiring analysis of massive volumes of traffic and threat indicators, and this may cause information overload (Ruefle and Murray, 2014; Helkala et al., 2015a, 2015b; Ponemon, 2019).

Conceptualizing the thought processes of an individual performing complex tasks, Reeve and Brown (1985, p.1) defined metacognitive awareness (MCA) as "the ability of an individual to control his cognitive processes and direct them toward specific tasks." MCA comprises distinct components: regulation of cognition (RC) and knowledge of cognition (KC). RC refers to the coordination of cognition processes, including planning, monitoring, and evaluating tasks, whereas KC refers to an individual's knowledge of their cognition, which is related to procedural, declarative, and conditional knowledge (Schraw and Dennison, 1994). Declarative knowledge implies knowing "about" things. Procedural knowledge means knowing "how" to do something. Conditional knowledge means knowing when and why to use declarative and procedural knowledge (Schraw and Dennison, 1994). The literature shows that task-specific awareness promotes both procedural and declarative knowledge, which are subcomponents of KC (Shreve, 2009; Eteläpelto, 1993). Task-specific awareness also enhances the regulation of cognition through planning, monitoring, and evaluation of their cognitive efforts, which are subcomponents of RC (Shreve, 2009; Eteläpelto, 1993).

The extant literature supports a close relationship between metacognition and self-efficacy. It has been reported that MCA improves self-efficacy (Schmidt and Ford, 2006; Legg and Locker, 2009) and predicts self-efficacy (Coutinho, 2008). While metacognitive abilities influence one's cognitive orientation and strategy, an individual needs sustained motivation, judgment, and confidence to persist with the complexity of the tasks and cope with stress during their execution. Being confident, persistent, and showing sustained motivation are elements of an individual's self-efficacy. Bandura (1998, p,9) defined self-efficacy as "people's beliefs about their capabilities to produce designated levels of performance." Numerous studies have demonstrated how efficacy affects the performance of complex, context-oriented dynamic tasks by elevation of confidence and motivation (Tzeng, 2009; Pajares, 2002; Livingston, 2003). In this study, computer security self-efficacy (CSSE) is defined as "an individual's self-belief in performing specific computer security-related tasks that accomplish threat detection, assessment, and mitigation" (Rhee et al., 2009,p.3). Security professionals need to possess self-efficacy to initiate and persist with tasks despite obstacles and challenges (Phelps et al., 2006).

TMT performance requires a high degree of planning, monitoring, and evaluation of tasks, as well as persistent and sustained motivation by security professionals. However, as seen in Table 1, the literature on information security has not considered the role of metacognitive awareness and self-efficacy in translating awareness to TMT performance. We elaborate on this research gap in the next section.

2.4. *Research gaps and objectives*

We identify the following research gaps concerning the impact of security professionals' awareness on TMT. One may posit that awareness can be acquired by gathering knowledge through training and experience. However, there are two challenges. One challenge is understanding what constitutes the awareness that must be obtained. The other critical challenge is understanding the process by which a security professional identifies and applies relevant knowledge to detect, assess, and mitigate threats. In using knowledge to perform tasks, one may have to reflect and effect problem-solving routines and persist with them in the face of complex, uncertain, and evolving environments characterized by rich and diverse information.

On the first challenge, as observed in Table 1, studies have considered awareness relating to security, system, or situational, and rarely all three together. As described in Section 2.2, they represent distinct dimensions of awareness, and hence an incomplete treatment would lead to the insufficient conceptualization of its role in performing TMT. Thangavelu et al. (2020) consolidated the literature and identified three awareness dimensions that purportedly affected incident response. However, the impact of awareness on task performance requires empirical validation. On the second challenge, we emphasize the need to study the effect of metacognitive awareness and self-efficacy of security professionals on task performance, as evident in other contexts (Hogan et al., 2014; Livingston, 2003). Awareness is considered an antecedent to cognition in studies examining security behavior (Hanus and Wu, 2016). Task-specific awareness can help improve the metacognitive abilities of security professionals (Eteläpelto, 1993; Shreve, 2009). The extant literature indicates a close relationship between MCA and self-efficacy. MCA has been shown to improve self-efficacy (Schmidt and Ford, 2006; Legg and Locker, 2009), which in turn affects task performance (Coutinho, 2008). However, as seen in Table 1, there is insufficient literature on the importance of awareness, metacognitive awareness, and self-efficacy on TMT performance.

Therefore, this study's research objective is to investigate the relationship between awareness (security, system, and

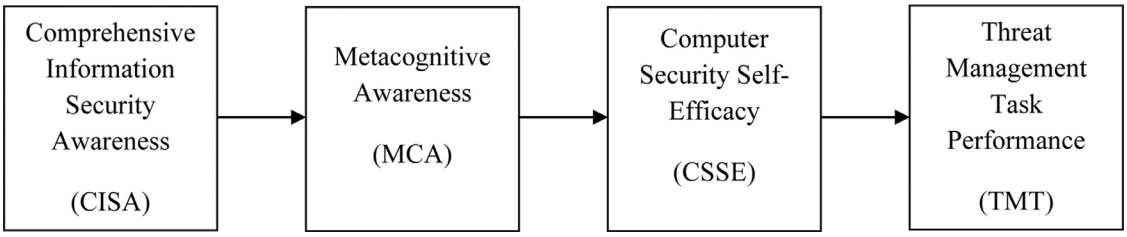

Fig. 1 – Conceptual approach.

situational), metacognitive awareness, self-efficacy, and TMT performance by security professionals.

3. Research model

A research model that relates awareness and cognition to TMTs helps deepen understanding and empirically validate the relationship. We adopt a socio-technical approach to describe the effect of comprehensive information security awareness (CISA) and cognitive dimensions, namely metacognitive awareness (MCA) and CSSE, on TMT performed by security professionals. Fig.1 presents our conceptual approach depicting the relationships between CISA, MCA, CSSE, and TMT. We hypothesize the relationships between these constructs in this section.

3.1. CISA

The literature attributes an inadequate incident response to an ineffective response by professionals due to their lack of security, system, or situation awareness. Discussions in section 2.2 clearly show that these awareness dimensions are distinct yet complement each other in terms of the knowledge required for the effective performance of TMT. We bring them together in the form of CISA.

Effective TMTs require threat visibility across the network. Achieving threat visibility depends on an accurate assessment of the dynamic states of the system. For example, (Woods, 1988) explained that correct situational assessment required tracking the system states correctly as the events evolve and unfold in a complex system environment. In a threat management context, security awareness provides insights into how the attack is weaponized with exploits (TTPs, motives, indicators, etc.) (Hutchins et al., 2011). On the contrary, system awareness provides insight into how the system responds to that attack and the states of the system (behavior, defense response, etc.) (Alberts et al., 2004). These two insights help deduce an accurate picture of an attack by comprehending and projecting the states of systems with additional information from external and internal sources. Conversely, when an attack is materialized, analyzing it helps to picture and comprehend the system states and respective attack stages (Chen et al., 2006). While system awareness is related to how organizations respond to external threat actors, security awareness provides views on the adversary's ability and motivation. Situational awareness provides more contexts for the attack from the organization and environment, correlating them to the context. Table 2 depicts the distinct nature of these awareness dimensions yet their complementary role in enabling TMTs. Thus, a security professional must possess system, security, and situational awareness, which we define as CISA, to manage a security incident and perform TMT effectively.

3.2. CISA and MCA

Metacognitive awareness has two distinct components. The first component, KC, relates to what a person knows about their cognitive abilities, processes, and resources related to the performance of specific cognitive tasks (Schraw and Dennison, 1994). The second component, RC, regulates the level of planning and modifying one's thinking processes and problem-solving ability using available information (Pintrich and Groot, 1990; Schraw and Dennison, 1994). Literature beyond information security observes that MCA impacts uncertain, contextual, and complex tasks (Haynie et al., 2010), such as internet use characterized by information overload (Hogan et al., 2014).

Task-related awareness promotes KC through metacognitive knowledge (Eteläpelto, 1993). Studies show that awareness influences KC by fostering the development of procedural, declarative, and conditional knowledge, which are subcomponents of KC (Shreve, 2009; Armbruster, 1983; Anderson, 1982). In turn, Campbell et al. (1993) established the effect of procedural and declarative knowledge on task performance. When security professionals are aware of TTPs and the motives behind the attacks, and of how the system weakness is exploited by an attacker using TTP and the behavior of the system that is exploited, they know their strengths and weaknesses and align their resources accordingly (declarative knowledge) while performing the tasks. Similarly, when they possess the awareness to infuse information from disparate systems, they recollect the most important data required, organize the information, and align their strategy to achieve threat visibility (procedural knowledge). They are likelier to know how and when to use the available information (conditional knowledge) in achieving threat visibility. Thus, CISA enhances security professionals' KC by enhancing procedural, declarative, and conditional knowledge. Therefore, we propose the following hypothesis,

H1. CISA enhances the knowledge of cognition of professionals during security incident management

Research indicates that task-specific awareness influences RC (Eteläpelto, 1993) through cognitive monitoring. Cognitive

Table 2 – Security, system, and situational awareness and TMT

Security awareness		System awareness		Situation awareness	
Components	TMT impacted	Components	TMT impacted	Components	TMT impacted
Tactics, Techniques and Procedures	TD, TA, TM	System Characteristics	TD, TA	Percept	TD
Motives	TD, TA	System Architecture	TA, TM	Comprehend	TD, TA
Indicator	TD	System Behavior	TD, TA	Project	TM

(** TD – Threat detection, TA – Threat assessment, TM – Threat mitigation)

monitoring is any activity that regulates one's own thought processes. Task-related awareness is a precondition for developing cognitive monitoring comprising planning, monitoring, and evaluating one's progress in any action (Shreve, 2009). When security professionals possess CISA, they can plan tasks by identifying specific goals and choosing the best options to complete those goals before undertaking the tasks. For example, when a system triggers anomalous traffic due to malware, they must perform several steps: identifying malware indicators and payloads, finding the possible affected systems, and removing them without causing any business impact. Possessing system, security, and situational awareness allow them to identify and set goals for each step and plan what needs to be performed (planning). Subsequently, periodical checks are made to ascertain the completion of prerequisites for subsequent tasks (monitoring). It also helps them assess how they have completed the tasks and routines required to produce the intended effect (evaluation). Therefore, CISA can improve security professionals' planning, monitoring, and evaluation processes and enhance cognition regulation. Hence, we propose the following hypothesis.

H2. CISA enhances the regulation of cognition of professionals during security incident management

3.3. *Metacognitive awareness and computer security self-efficacy*

MCA impacts self-efficacy (Legg and Locker, 2009) through procedural knowledge (Arachchilage and Love, 2014; Rogers, 2020) and declarative knowledge (Schmidt and Ford, 2006; Rogers, 2020). Conditional knowledge also plays a vital role in impacting self-efficacy and improving task performance (Bouffard, 1994). KC influences perceptions of the task in terms of both its understanding and difficulty, thereby improving the strategies one chooses to employ in performing tasks (Hadwin. et al., 2018). When security professionals are aware of the strategy, they can adaptively respond to environmental demands (Zimmerman, 2000). Individuals with higher levels of KC have been shown to exhibit higher confidence and improved performance (De Carvalho Filho and Yuzawa, 2010).

KC gained from procedural, conditional, and declarative knowledge through CISA may enhance confidence in performing TMTs. Let us take an example to illustrate this. Suppose security professionals encounter a possible network intrusion activity; they will mine the critical information regarding the origin and destination, understand the network and destination system behavior, and gather necessary information from multiple systems (declarative and procedural knowledge). KC handles organizing this information in a better way. To summarize, professionals with a higher degree of KC are likely to use the information more effectively in the context of network intrusion (conditional knowledge). The result is that they can confidently judge the impacted systems in the network and select the best strategy to mitigate that abnormality. Therefore, declarative, conditional, and procedural knowledge can help professionals enhance their judgment and confidence in the performance TMTs. Thus, we propose the following hypothesis.

H3. Knowledge of cognition enhances the CSSE of security professionals during security incident management

RC has a significant positive correlation with self-efficacy (Cera et al., 2013; Rogers, 2020). Cera et al. (2013) showed that metacognition involves cognitive orientation comprising planning, monitoring, and evaluation abilities, which are part of the RC. This, in turn, regulates individual human actions and enhances self-efficacy. Regulation of efforts can reduce stress and fatigue and motivate professionals to persist with complex tasks (Winne and Hadwin 1998; Coutinho, 2008). The higher the RC, the higher the confidence and performance (De Carvalho Filho et al., 2010).

Extending these arguments to the context of information security, CSSE will improve when professionals direct their cognitive efforts by better planning, monitoring, and evaluating tasks. For example, if malicious traffic is confirmed to be a malware attack, security professionals must monitor similar systems that are likely to be impacted and plan specific steps to avoid further propagation of attacks. Security professionals need to plan each step, choose the best options, and evaluate whether tasks are completed effectively. They can then align their cognitive resources in an orderly manner, which will improve their confidence, judgment, and motivation. Therefore, we propose the following hypothesis.

H4. Regulation of cognition enhances the CSSE of security professionals during security incident management

3.4. *CSSE and TMT*

TMTs include threat detection, assessment, and mitigation, which pose a significant challenge to security professionals. Challenges include information overload arising from voluminous traffic across networks and systems, dynamic changes in system states, and segregation of key information from a mas-

sive volume of events. These challenges may result in stress and fatigue for security professionals. To overcome this stress and fatigue, security professionals need to sustain their motivational efforts, judge critical information better, and maintain a high confidence level to perform these challenging tasks. Literature shows that self-efficacy influences the performance of complex and dynamic tasks (Hepler and Feltz, 2012; Zimmerman, 2000). Self-efficacy is also reported to positively impact the performance of well-defined cyber-oriented tasks (Choi et al., 2013) and help security professionals initiate and persist with tasks (Phelps et al., 2006). Thus, CSSE may help security professionals persist with their efforts in accomplishing TMTs.

Threat assessment is the process of analyzing the probability of the detected threat becoming real and its severity. It helps to prioritize actions for remediation of incidents (Werlinger et al., 2010). Assessment of the incident's scope and impact is stressful, as impacted systems change dynamically as the attack unfolds (Ponemon, 2019). This necessitates assessing the situations and states of attacks to identify affected systems by fusing information from multiple sources (D'Amico et al., 2005). This, in turn, requires a higher level of confidence and motivation to arrive at a correct decision in uncertain situations (Hepler and Feltz, 2012; Zimmerman, 2000). Workman et al. (2009) established that people's actions to assess threats depend on their efficacy levels.

In short, CSSE will help security professionals to identify the impacted systems, the state of the affected systems, and the scope of the attack with confidence and belief. Aided with business context knowledge will help them further prioritize their efforts according to threat severity effectively. Therefore, professionals with higher CSSE may adapt better to the dynamicity of threats and perform appropriate steps for threat assessments. Thus, we propose the following hypothesis.

H5. CSSE enhances the performance of threat assessment tasks

Threat detection involves analyzing the various security events, understanding the pattern of such events, and arriving at a correct decision regarding whether threat events are real or false (Clark et al., 2007). Security professionals need to segregate actual threats from various insignificant events, which is complicated (Anuar et al., 2012). It is akin to finding a needle in a haystack and involves zeroing–in the critical information from a diverse set of information from multiple systems and heavy network traffic. A high level of confidence in their judgment is necessary to analyze and comprehend the security events. Strong persistence and sustained motivation are demanded in such tasks (Zimmerman, 2000).

For example, when a security professional is confident in analyzing malware issues, they will make efforts to detect and mitigate them (Ng et al., 2009). Security professionals who exhibit higher CSSE are more confident initiating and persisting with threat detection tasks (Phelps, 2006). Therefore, we propose the following hypothesis.

H6. CSSE enhances the performance of threat detection tasks

Threat mitigation involves a set of activities to select appropriate countermeasures, apply those measures, and restore the affected system to a normal state. Security professionals require a high degree of judgment and confidence in achieving this. CSSE is a significant factor in influencing individual efforts to undertake a recommended strategy and selecting and using countermeasures (Workman et al., 2009; Ng et al., 2009; Rhee et al., 2009). During threat mitigation, a security professional can confidently judge the best course of remedial measures by assessing the scope and impact of threats. Therefore, security professionals with higher CSSE will possess stronger motivation and sustain their efforts to prevent threats by using the best countermeasures. Consequently, we propose the following hypotheses.

H7. CSSE enhances the performance of threat mitigation tasks

Fig. 2 presents the conceptual model depicting the effect of information security awareness (CISA) and cognitive dimensions, namely metacognitive awareness (MCA), which includes RC, KC, and CSSE on TMTs, namely threat assessment (TA), threat detection (TD), and threat mitigation (TM) performed by security professionals.

4. Research methodology

4.1. *Item development*

We developed measures of CISA by closely following our definitions of the constructs in this study. Based on our CISA and TMT conceptualization, we operationalized CISA as a second-order construct composed of three first-order awareness constructs: security awareness, system awareness, and situational awareness. We operationalized the TMT constructs, comprising three first-order constructs: TD, TA, and TM. The construct CISA was formatively measured, while TMT was reflectively measured from their items. The criterion to determine whether the constructs are formative or reflective is driven by the researcher's conceptualization of the construct. Either the construct may give rise to its indicators or view the indicators as its defining characteristics (Diamantopoulos and Siguaw, 2006). As security awareness, system awareness, and situation awareness define CISA characteristics, CISA is an aggregate construct, where indicators define the effects to construct. Hence, it is formative. On the other hand, for the first-order constructs TA, TD, and TM, the casualty flows from the construct to indicators. Hence, these can be treated as reflective (Workman et al., 2009). We adopted the metacognitive awareness inventory used in education research (Schraw and Dennison, 1994) and adapted it to the SIM context. The measurement items for CSSE were adopted from Ng et al. (2009) and modified to the SIM context. Table 3 presents all the constructs, types, sources, and the number of their measurement items. Item-wise details are given in Annexure 2.

4.2. *Instrument pretesting and refinement*

We shared the initial measurement items of CISA and TMT with security professionals who had experience in informa-

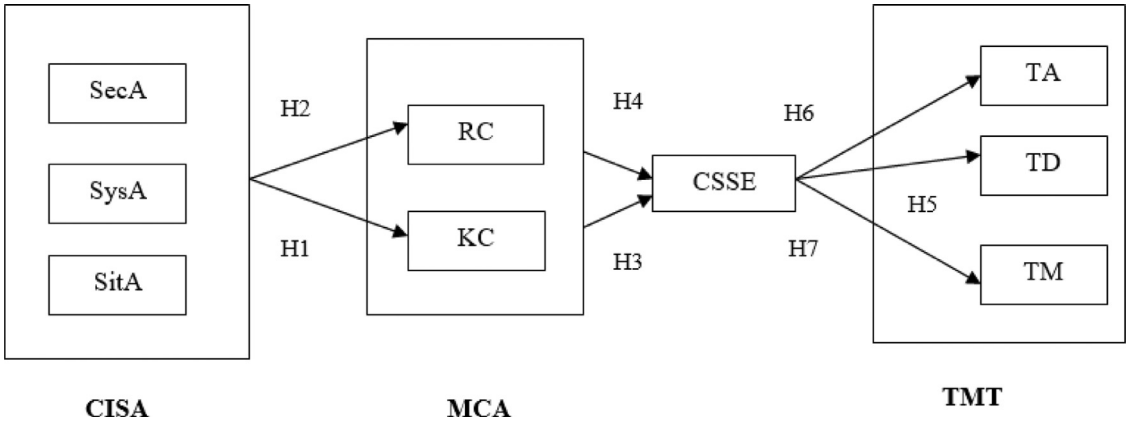

Fig. 2 – Conceptual model.

Table 3 – Measurement items and sources

Construct	Type	Source	Items
Comprehensive information security awareness (CISA)	Formative	Developed for this study	Second-order construct
Security Awareness (SecA)	Formative	Erbacher et al. (2010) Cichonski et al. (2012) Cheng et al. (2012) Oltsik (2015)	5
System Awareness (SysA)	Formative	Cheng et al. (2012) Oltsik (2015) Ponemon (2019)	6
Situation Awareness (SitA)	Formative	D'Amico et al. (2005)	4
Threat detection (TD)	Reflective	Cichonski et al. (2012) Clark et al. (2007)	3
Threat assessment (TA)	Reflective	Workman (2009) Cichonski et al. (2012) Oltsik (2015)	4
Threat mitigation (TM)	Reflective	Cichonski et al. (2012)	
Planning (RC)	Reflective	Schraw and	3
Monitoring (RC)	Reflective	Dennison,1994	3
Evaluation (RC)	Reflective		4
Declarative Knowledge (KC)	Reflective		6
Procedural Knowledge (KC)	Reflective		2
Conditional knowledge (KC)	Reflective		3
Computer Security Self Efficacy (CSSE)	Reflective	Ng et al., 2009	4

tion SIM and collected their feedback. Security professionals recommended modifying items related to SitA and TD, as they felt that the items were abstract and hard to understand. We reworded these items based on their feedback. Next, we developed an online questionnaire that was reviewed by security professionals. Based on their feedback, we improved the appearance of the online survey. The items and scales were then subjected to pilot testing conducted with 30 respondents drawn from various organizations. The respondents completed the questionnaire, commented on the wording, length, and instructions, and reported concerns if they had any. The validity and reliability of the measurement items were investigated using the responses of 30 participants. Based on the data and participant feedback analysis, all measurement items were deemed adequate and ready to be used in the main survey. All constructs were measured with multiple items on five-point Likert scales. The measurement items are shown in Annexure 2.

4.3. *Data collection*

We collected data by administering a web-based questionnaire survey. We contacted 300 security professionals employed by a diverse set of organizations and approached them through social network profiles (LinkedIn). The identities of the participants were kept confidential. We received 106 responses over two months, out of which 100 responses were valid. Annexure 1 provides the demographic details of the security professionals involved in the survey.

4.4. *Data analysis and results*

The component-based partial least squares (PLS) approach was used to evaluate the psychometric properties of the measurement scales and test the research hypotheses proposed in this study. As a component-based approach, PLS is appropriate for this study because it focuses on predicting data and is well suited for exploratory models and theory development. Another advantage of PLS is that sample size, and residual distributions are not a concern for smaller sample sets (Gefen et al., 2000; Willaby et al., 2015). The Smart-PLS software package (version 3.3.2) (Ringle et al., 2005) was used for the estimations.

4.4.1. *Measurement validation*

We first assessed the validity of the indicators at the construct level. For reflective constructs, convergent validity can be observed from the item loadings and the average variance extracted (AVE). Factor loadings for all items were significant and ranged from 0.72 to 0.93, well exceeding the required threshold of 0.6 (Hair et al., 2013). Composite reliability (Cronbach's alpha) scores for the first-order constructs were higher than the recommended cut-off of 0.8, and the AVE for the first-order constructs ranged from 0.7 to 0.9, well above the cut-off of 0.50 (Hair et al., 2013). There are two recommendations for validating formative constructs at the construct level: first, by examining the extent to which the formative constructs' indicators were multicollinear to each other. Multicollinearity is not desirable for formative constructs. Hence, VIF values ideally must be less than 10. A more conservative value of 3.3 was proposed by Petter et al. (2012). Multicollinearity index, except for two items, was less than 5. Second, it can be assessed by calculating Edward's adequacy coefficient (R^2_a) by summing the squared correlations between formative constructs and its indicators and dividing it by the number of items. This indicates the significance of formative construct items (MacKenzie et al., 2011). The literature considers that R^2_a values above 0.50 reflect that the variance in the indicators is shared with the formative constructs and indicate an acceptable criterion for formative constructs. We calculated R^2_a values for first-order formative constructs of CISA. The observed values were well above the cut-off value of .50. Hence, the validation of formative constructs satisfied both recommendations; thus, the formative construct indicators can be considered valid. A summary of the validity of the constructs is provided in Table 4.

4.4.2. *Reliability and discriminant validity*

For reflective constructs, we assessed the constructs' composite reliability coefficient (Cronbach's alpha). As Table 4 indicates, all coefficients were over .80, well above the prescribed value of .70 (Nunnally, 1978), indicating good measurement reliability. We assessed the convergent validity of the measurements by the following criteria: (1) Each item should have a higher loading on its hypothesized construct than on other constructs, and (2) the square root of each construct's AVE should be greater than its correlations with other constructs (Fornell and Larcker, 1981). First, following Gefen et al. (2000), we conducted a PLS confirmatory analysis. The results demonstrate that items have much higher self-loadings than cross-loadings (Annexure 3). Second, we computed each construct's AVE, and the AVE's square root was greater than the construct's cross-correlations with other constructs (Table 5). Additionally, we calculated each construct's composite reliability coefficient. Hensler et al. (2015) differed in the use of Fornell and Larcker's (1981) criterion for validating discriminant validity and recommended a new criterion called the heterotrait–monotrait ratio (HTMT). The HTMT ratio is based on the average correlations of indicators across constructs measuring different phenomena relative to the average correlations of indicators within the same construct. According to Henseler et al. (2014), an HTMT ratio below 0.85 demonstrates discriminant validity. HTMT values for all reflective constructs were found to be below 0.85. However, few items of RC and KC (indicated as M3, E4, PK2, DK4, DK5, and CK3) did not meet these requirements. They were dropped from the analysis. After dropping these items, the cross-loadings of items and HTMT ratios were improved to an acceptable level. It should be noted that the HTMT method can only be used to assess the discriminant validity of reflective constructs (Henseler et al., 2014).

We assessed the reliability and discriminant validity for formative constructs of CISA. Literature provides two recommendations to evaluate the discriminant validity of formative constructs: (1) Formative constructs should correlate less perfectly with other constructs ranging less than .69, against the prescribed criteria of less than 0.71(MacKenzie et al., 2011), and (2) indicators of the formative constructs should load highly on their corresponding constructs in comparison to other constructs (Klein and Rai, 2009). Formative constructs of first-order constructs satisfied both these criteria, ensuring adequate discriminant validity (Refer to Annexure 3 for details). Kock (2015) suggested full collinearity test as a preferable method to Harman's single factor test to detect common method bias. The test yielded VIF values less than 3.9, well within the threshold of 5.0. We also conducted Harman's single factor test, and the cumulative variance of the factors was 46.4%, which was also within the threshold of 50% (Kock, 2020). Thus, the tests show that there is no effect of common method bias on our results.

4.5. *Findings and results*

Fig. 3 shows the model testing results. CISA accounts for 64% variance in the RC and 65% for the cognition of knowledge. CISA significantly determines RC ($b = 0.801$, $p < 0.01$) and CK ($b = 0.809$, $p < 0.01$), confirming support for H1 and H2. The results indicate that CISA can improve the MCA of security professionals for SIM. This confirms that CISA helps professionals plan and organize TMTs effectively. They can also continuously monitor and evaluate their efforts as they acquire adequate declarative knowledge from CISA and regulate their cognitive efforts.

The literature has observed that task management efficacy is expected to increase when there is an improvement in declarative and procedural knowledge (Martocchio and Hertenstein, 2003; Moores et al., 2006). Improvements in the MCA levels of security professionals elevate their efficacy levels (Moores et al., 2006). Current study results also demonstrate this fact. CSSE is affected by both metacognitive aware-

Table 4 – Measurement validation for formative constructs

Construct	Measures	Weight	Significance	VIF	Edwards Coefficient (Edwards,2001)
Security awareness	SecA1	0.283	$p < 0.05$, Significant	2.865	0.764
	SecA2	0.262	$p < 0.05$, Significant	4.971	
	SecA3	0.291	$p < 0.05$, Significant	6.642	
	SecA4	0.295	$p < 0.05$, Significant	3.150	
Situation awareness	SitA1	0.317	$p < 0.05$, Significant	4.650	0.793
	SitA2	0.286	$p < 0.05$, Significant	3.600	
	SitA3	0.271	$p < 0.05$, Significant	2.450	
	SitA4	0.294	$p < 0.05$, Significant	2.745	
System awareness	SysA1	0.197	$p < 0.05$, Significant	3.400	0.748
	SysA2	0.210	$p < 0.05$, Significant	5.900	
	SysA3	0.193	$p < 0.05$, Significant	2.860	
	SysA4	0.194	$p < 0.05$, Significant	3.960	
	SysA5	0.199	$p < 0.05$, Significant	2.670	

Table 5 – Measurement validation of constructs of reflective variables

	Cronbach's alpha	AVE	CISA	CSSE	KC	RC	TA	TD	TM
CSSE	0.963	0.900	0.738	**0.948**					
KC	0.928	0.700	0.809	0.794	**0.837**				
RC	0.928	0.667	0.801	0.633	0.787	**0.817**			
TA	0.883	0.743	0.537	0.644	0.561	0.421	**0.862**		
TD	0.879	0.804	0.381	0.477	0.427	0.341	0.700	**0.897**	
TM	0.929	0.780	0.450	0.551	0.488	0.430	0.765	0.716	**0.883**

ness elements. RC and KC account for 63% of the variance in CSSE ($b = 0.716$, $p < 0.01$ and $b = 0.009$, $p < 0.01$). Results support H3 and H4, indicating the mediating effect of metacognitive awareness between CISA and CSSE. This supports the existing theory of metacognition that there is a strong relationship between the metacognitive elements and a professional's efficacy level in complex and dynamic tasks (Coutinho, 2008; Legg and Locker, 2009). Therefore, CISA improved professionals' confidence levels in performing SIM by improving their metacognitive abilities.

CSSE determines 22% of variance in threat detection, 41% variation in threat assessment, and 30% variation in TM. TMTs are significantly influenced by CSSE on threat detection ($b = 0.477$, $p < 0.01$), threat assessment ($b = 0.644$, $p < 0.01$), and threat mitigation ($b = 0.551$, $p < 0.01$). This confirms the support for H5, H6, and H7. Therefore, enhancement in CSSE improves the performance of threat detection, assessment, and mitigation in SIM. Enhanced CSSE can motivate professionals to cope with strenuous event monitoring to track the various states and system behavior and accurately deduce the attacks. It also helps to focus attention on necessary events, thereby improving threat detection and assessment. Literature shows that when there is an increase in CSSE, it aids in better mitigation of information security threats (Ng et al., 2009). Improvements in the efficacy level of security professionals lead to effective threat detection, assessment, and mitigation.

The results support the hypotheses and the conceptual model. Overall, the study's findings support the idea that CISA can significantly enhance both the RC and knowledge cognition of security professionals, which in turn positively correlates to the CSSE of professionals in SIM contexts. The summary of the findings is provided in Table 6.

Table 6 – Results of hypothesis testing

Hypotheses	Description	Result
H1	CISA enhances the knowledge of cognition of professionals during security incident management	Supported
H2	CISA enhances the regulation of cognition of professionals during security incident management	Supported
H3	Knowledge of cognition enhances the CSSE of security professionals during security incident management	Supported
H4	Regulation of cognition enhances the CSSE of security professionals during security incident management	Supported
H5	CSSE enhances the performance of threat assessment tasks	Supported
H6	CSSE enhances the performance of threat detection tasks	Supported
H7	CSSE enhances the performance of threat mitigation tasks	Supported

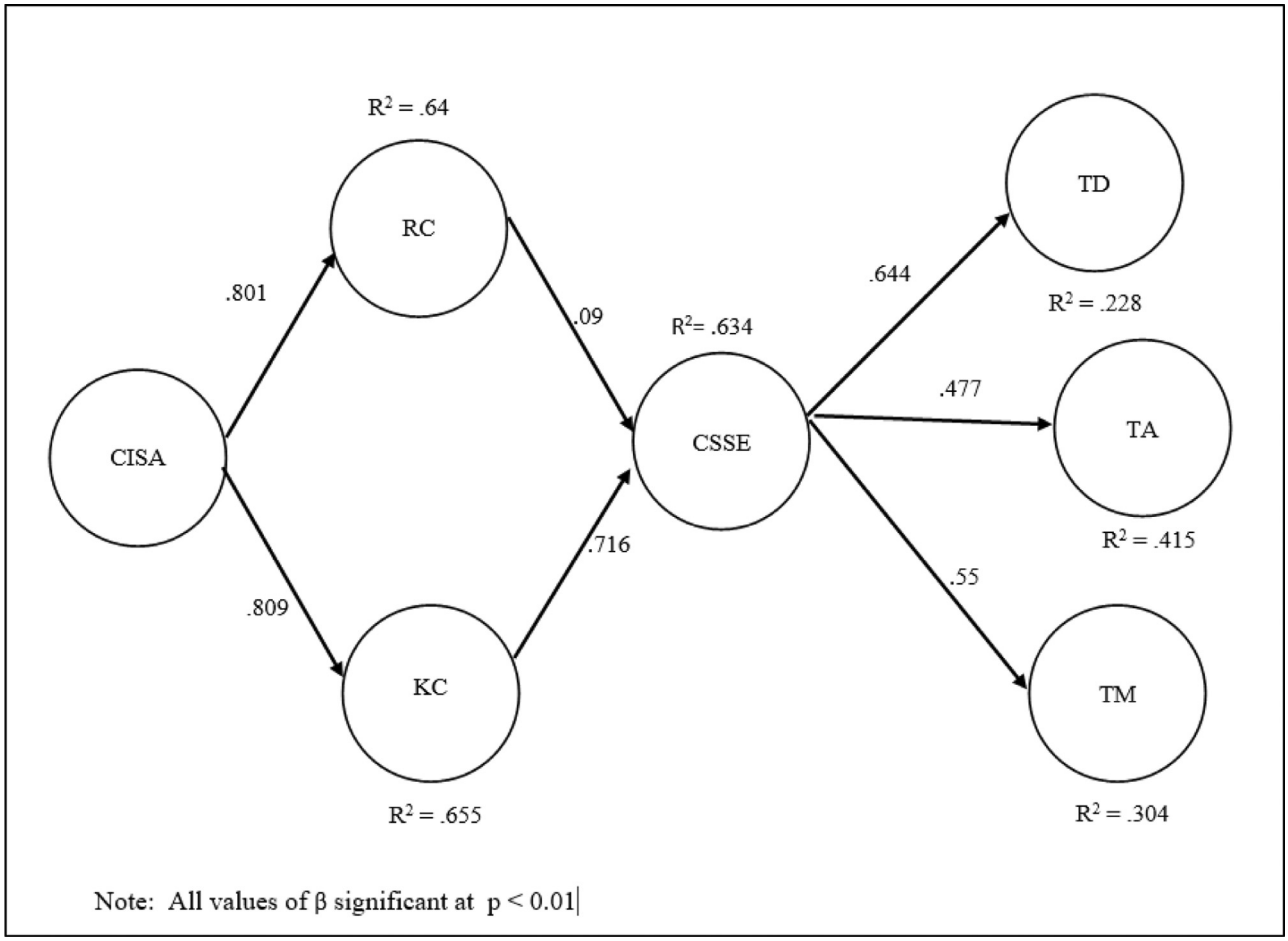

Fig. 3 – Model Testing Results.

4.6. *Mediation analysis*

We adopted the bootstrapping method proposed by Hair et al. (2011) to analyze the mediating effect after introducing the mediating variables of MCA and CSSE in the relationship between CISA and TMT. As shown in Table 7, the impact of CISA on TD, TA, and TM is mediated by MCA and CSSE. This is indicated by the coefficient values of indirect effects, which are higher than the coefficient values of direct effects. It was also observed that CSSE mediated the impact of the RC and KC components of MCA on TD, TA, and TM. Therefore, we can conclude that CISA impacts TMT via MCA and CSSE. Table 7 presents a summary of the mediation tests.

4.7. *Moderation analysis*

We conducted a moderation analysis of four demographic variables: age, gender, education, and the experience level of security professionals. As seen in Table 8, the results indicate that only experience moderated the effect of CSSE on TD among the demographic variables. Prior studies have reported mixed results for the impact of gender, age, and experience on metacognition (Lewis, 2016; Callan et al., 2016). On self-efficacy, studies report negative effects for age, no significant effect for education, and mixed results for gender (Burger et al., 2010; Hsiao et al., 2018). Both self-efficacy and metacognition are domain-specific (Pajares, 1996). In our case, no significant effect for demographic variables was observed for MCA, CSSE, and TMT, except for the moderating effect of experience on CSSE and TD. Table 9 depicts the descriptive statistics on awareness levels, self-efficacy, and TMT organized by demographic variables. As seen in Table 9, we did not find any pattern among demographic variables and awareness levels, self-efficacy, and TMT.

5. Discussion and implications

This research has implications for both practice and research. Towards practice, we: (a) propose CISA as an approach for reducing stress and fatigue of security professionals, (b) describe how CISA contributes to training foundations and demonstrate it for tactical threat intelligence, (c) offer a means for assessing and improving security professional's awareness and performance, and (d) suggest measures for evaluating and improving metacognitive awareness and self-efficacy. Towards research, we discuss: (a) the application of metacognitive and self-efficacy theories, (b) the use of inventory developed in this study for other cybersecurity contexts, and (c) the need to consider comprehensive awareness.

Table 7 – Summary of mediating effects tests

Mediation tested	Total effect		Direct effect		Indirect effect Point estimate
	Coefficient	t value	Coefficient	t value	
CISA on TD by KC and CSSE	0.373	1.058	-0.002***	0.14	0.375
CISA on TA by KC and CSSE	0.520	1.106	0.067**	0.421	0.453
CISA on TM by KC and CSSE	0.010	3.668	-0.056**	0.331	0.06
CISA on TD by RC and CSSE	0.372	3.388	0.039**	0.223	0.333
CISA on TA by RC and CSSE	0.518	4.809	0.182***	1.131	0.336
CISA on TM by RC and CSSE	0.532	5.142	-0.170**	0.958	0.549

*** $p < 0.5$,** $p < 0.01$,*$p < 0.001$.

5.1. *Practice*

The first implication of this study it provides an approach for reducing the stress and fatigue of security professionals. While Bartnes et al. (2016) and Bartnes and Moe (2017) identify challenges in SIM and explain the role of preparedness in improving incident management, our study augments these studies by proposing CISA as a method for preparing security professionals. Our study shows that CISA can help security professionals overcome fatigue and stress associated with working in uncertain and evolving contexts, information overload, diversity in information, and the maze of interconnected systems (Ponemon, 2019). CISA achieves this by improving their knowledge of cognition, thereby regulates professional's cognitive efforts while monitoring, planning, and evaluating security tasks. Such regulated and enhanced cognitive efforts build security professionals' confidence and efficacy in threat detection, assessment, and mitigation. As a result, professionals in security operation centers can adapt to demanding cognitive requirements of complex tasks and effectively perform threat management tasks.

The second implication of CISA is that it offers a foundation for security training and building artifacts. Literature and NIST emphasize the need for training for security professionals (Wilson et al., 1998; Horrocks, 2001).Moore et al. (2006) appealed for enhancing self-efficacy and metacognition through training programs. So, the question is, how do we strengthen self-efficacy and metacognition? We may do so by incorporating CISA in the design of training programs. We assert, based on this study's results, which show that CISA can enhance metacognitive awareness and self-efficacy. CISA comprises security, system, and situational awareness and can be ingrained into training artifacts containing tutorials, case studies, simulations, visual aids demonstrating the weaponization of exploits, and pictorial representation of the sequence of steps and rules. While several methods are available for developing security training (Hart et al., 2020), the CISA provides the foundational elements to create such training programs. We now discuss how CISA based training can enhance tactical threat intelligence.

Security professionals need to gather and analyze tactical threat intelligence and ensure that their defenses are ever prepared and ready. Due to a lack of automated tools, they often need to perform this task manually (Wagner et al., 2019). Take the case of WannaCry ransomware; when it was on the wild using an exploit called EternalBlue, the threat intelligence revealed that it exploited the vulnerability in Windows server message block (SMB) services. In such cases, prior training based on CISA would have helped them in the following ways. Towards security awareness, the training would impart knowledge of TTPs, motives, and indicators related to an SMB attack (How older SMB versions in unpatched systems are exploited by pool grooming, a type of heap spray of kernel memory structures, by custom-crafted ring 0 kernel shellcode) (Tounsi and Rais, 2018). Toward system awareness, the training would impart knowledge on how SMB specific TTPs propagate and attack organizational systems (Windows endpoints and server assets via IPC$) and what defensive controls protect the systems against SMB threats (IDS, data execution prevention, address space layout randomization) and how can such controls be planned and executed (deploying digital certificate trust between shares, disabling SMBv1 and control on port 445). System awareness perspective would also help them overcome the challenges in the intelligence cycle comprising processing, exploitation, and analysis of information (Webb et al., 2014). On situational awareness, the training would be towards converting the available intelligence into actionable intelligence by perceiving the current state, comprehending the situation, and projecting the future state of the attack (sending malicious traffic via SMB, simultaneous ex-

Table 8 – Summary of the moderating effects of demographic variables

Moderation tested	Std deviation	t value	P values
Age on CISA and RC	.069	.080	.936
Age on CISA and KC	.082	.237	.813
Age on KC and CSSE	.148	.636	.525
Age on RC and CSSE	.153	.093	.926
Age on CSSE and TD	.115	1.231	.219
Age on CSSE and TA	.110	1.404	.161
Age on CSSE and TM	.116	.373	.709
Experience on CISA and RC	.072	.561	.575
Experience on CISA and KC	.080	.141	.833
Experience on KC and CSSE	.115	.878	.380
Experience on RC and CSSE	.141	.478	.633
Experience on CSSE and TD	.096	2.55	.011*
Experience on CSSE and TA	.096	1.895	.059
Experience on CSSE and TM	.123	.226	.821
Gender on CISA and RC	.051	.007	.995
Gender on CISA and KC	.071	.281	.779
Gender on KC and CSSE	.114	.125	.901
Gender on RC and CSSE	.140	.132	.895
Gender on CSSE and TD	.093	1.904	.057
Gender on CSSE and TA	.107	1.700	.090
Gender on CSSE and TM	.110	1.940	.053
Education on CISA and RC	.086	1.035	.301
Education on CISA and KC	.129	1.221	.233
Education on KC and CSSE	.133	1.406	.296
Education on RC and CSSE	.131	.687	.492
Education on CSSE and TD	.132	1.440	.151
Education on CSSE and TA	.103	1.161	.246
Education on CSSE and TM	.127	.278	.781

Table 9 – Demographic variables, CISA, self-efficacy, and TMT

	Frequency	SecA	SySA	SitA	CSSE	TD	TA	TM
Gender								
Male	86	4.33	4.35	4.37	4.16	4.08	4.09	4.13
Female	14	4.29	4.36	4.48	4.29	4.21	4.14	4.20
Age group								
21-25	21	4.40	4.54	4.51	4.25	4.08	4.06	4.14
26-35	51	4.25	4.30	4.31	4.17	4.18	4.14	4.15
36-45	27	4.35	4.32	4.40	4.11	3.95	4.04	4.10
Experience								
<5 years	28	4.33	4.54	4.49	4.25	4.11	4.06	4.17
Between 5 to 10	26	4.16	4.26	4.27	4.05	4.16	4.20	4.13
Between 11 to 15	24	4.43	4.45	4.50	4.42	4.20	4.23	4.26
16-20	15	4.15	4.02	4.04	3.92	3.85	3.92	4.05
>21	7	4.53	4.47	4.55	4.32	4.04	3.89	4.02
Education								
3 year Diploma	4	4.13	4.50	4.56	4.50	4.50	4.19	4.50
3/4 years Bachelors	35	4.19	4.21	4.30	4.05	4.08	4.07	4.08
4 Plus Post-graduate	31	4.46	4.48	4.51	4.25	4.13	4.23	4.22

*SecA – Security Awareness, SysA – System Awareness, SitA – Situation Awareness, CSSE – Computer Security Self Efficacy, TD –Threat detection, TA – Threat assessment, TM – Threat mitigation, Value are averages on a scale of 1-5.

ploitation of x86 and x64 CPU architectures of server assets, analyzing the network traffic of NT). The mined threat intelligence would enable the security professionals to deploy immediate countermeasures (trust deployment using digital certificates, anti-virus rules) and monitoring mechanisms (inline custom IDS rules on port 445, indicator-based monitoring) to fortify the defense against the threat actors (Barnum, 2014). Thus, gaining adequate first-hand CISA-based training can help professionals in tactical threat intelligence.

The third implication of this study is its utility as a tool for evaluating security professionals' awareness and their performance. Such evaluations can provide specific pointers for customized training on skill enhancement. The literature recommends the need for systematic assessment after knowledge sessions on building capabilities for incident response (Bartnes et al., 2016). Managers can assess professional's awareness by using the CISA scales developed in this study. They can identify a security professional's weaknesses using the TMT scales by conducting simulated tests on the network and validate whether professionals can identify the events of mock tests and provide timely alerts. Armed with the evaluations, security managers can identify the weaknesses and reasons for their failure. Based on the findings, security managers redesign training programs and address the professional's identified deficiencies.

The fourth implication is that our study establishes the importance of metacognitive awareness and self-efficacy in improving TMT. La Fluer et al. (2021) demonstrate that scenario-based experimental paradigms enable team-level security skillset assessment and development using realistic simulations of an operational environment. Such exercises would improve not only not the skills but also the confidence and self-efficacy. The inventory proposed in this study can be used as a tool for assessing security professionals' metacognitive awareness and self-efficacy, which would serve as inputs for gauging competency and role-mapping. Skill development and role-mapping would improve the confidence and efficacy of security professionals. Managers could deploy other confidence-building measures such as job rotation and create an environment where one could afford to make mistakes and learn from them. Overall, these implications can support a proactive security operation that can safeguard organizations from determined malicious external entities. This may improve organizations' reputation and legal compliance and increase their value in the long run.

5.2. *Research*

Existing research focuses on process improvements (Mitropoulos et al., 2006; Bartnes et al., 2016; Ahmad et al., 2021) and technical design and solutions to improve threat management (Zhang et al., 2009; Naseer et al., 2021). This study complements existing literature by considering human factors in security incident management and offers direction to prepare security professionals by incorporating awareness as recommended in the literature (Killcrece et al., 2003; Bartnes et al., 2016; Horrocks, 2001).

In this regard, our study addresses two key challenges. The first challenge includes identifying what constitutes awareness comprehensively, and the second challenge is to understand how comprehensive awareness translates into effective threat management. To the best of our knowledge, our research model is the first that integrates awareness with metacognition and self-efficacy in the information security context. The key implication is that this study not only focuses on what constitutes awareness but also the mechanism in which it translates into task performance.

The first implication is that this study extends the literature on efficacy and metacognition and fills the knowledge gap highlighted by Knox et al. (2017) on the need for research integrating metacognitive strategies in the cybersecurity domain. While studies of Webb et al. (2014) and Varga et al. (2021) offer a cyber situational awareness model and information necessary for situational assessment of threats, our framework incorporates cognitive factors to evaluate how situational assessment translates into threat management. We have shown that task performance is affected by awareness, metacognition, and self-efficacy. Mediation analysis strengthens the need for incorporating metacognition and self-efficacy in studies related to awareness and incident response. The takeaway is that information security studies on awareness, and task performance would have to factor in metacognition and self-efficacy. For example, Abraham and Chengalur-Smith (2019) argue that learning affects information security task performance and the long-term results of the organization. Bartnes and Moe (2017) describe how learning to learn will improve their incident response practices in organizations. In line with these studies, our model offers a base to develop SIM practices and investigate their impact on the organization.

The second implication for research is that our model's applicability to other dynamic contexts in information security. For example, risk management is context-oriented, and this framework can be adapted to study the efficacy of risk management professionals. We have developed a metacognitive awareness inventory for security professionals and operationalized the constructs of regulation and KC to cybersecurity contexts. We also operationalized the constructs of TMTs in SIM. This contribution goes beyond regular threat management research. As Bartnes and Moe (2017) highlight the need for systematic evaluation of training to improve SIM, the constructs and inventory developed in this study can be used for such evaluation. For example, researchers can use the inventory and evaluate the developers' cybersecurity awareness for secure coding practice from a cognitive standpoint for secure software development.

The third implication is that our study establishes the need for a comprehensive treatment of awareness. This study emphasizes the demarcation of awareness into system, security, and situation dimensions. Chen et al. (2006) consider cybersecurity situational awareness a subset of cybersecurity awareness, and Cheng et al. (2012) consider system factors as subcomponents of situational and security awareness. Their treatment is more suitable for developing technical system design. However, it may be less beneficial from a human perspective because security professionals' decision-making involves diverse sets of information during uncertain situations. Webb et al. (2014) show that information overload inhibits situational assessment. Their cognitive abilities might not be better utilized if the boundaries are not clear. In line with

Endsley's (2015) situational awareness model, by demarcating the boundaries of external context (related to TTPs, motive, and capabilities as security awareness) and organizational factors (related to system awareness) from situational factors, we established how different aspects of awareness come together in threat management. We illustrated this in designing training programs for SMB attacks in the implications for practice. Therefore, we recommend that research that extends on previous works such as Mitropoulos et al., (2006), Bartnes et al., (2016), Bartnes and Moe (2017), and Ahmad et al., 2021) related to information security consider awareness holistically.

6. Scope for future work

Our study considered metacognition and efficacy as two central driving factors for our research model and can be extended to cover multiple cognitive functions. For instance, a future study may extend this model by including executive functions like attention control, which correlates with awareness and task performance. Attention control as an executive function has been found to play an important role in context-oriented situations (O'Brien and O'Hare, 2007). Another area for future research could also include studying the effect of task-related factors like complexity and uncertainty on MCA. Self-efficacy has several dimensions, such as magnitude, strength, and generalizability (Compeau and Higgins, 1995), and the impact of these individual dimensions on TMT can be studied in the future. Future work may also consider factors like organizational factors such as culture and control to understand their impact on learning and security incident management, going beyond specific tasks such as TMT. Furthermore, training artifacts based on CISA can be designed using a system design approach (D'Arcy et al., 2009) or design science research. Qualitative studies may be used to study their effect on organizations.

7. Limitations and Conclusion

This study has several limitations. First, the sample was small. Security professionals were reluctant to answer the survey despite the assurance that the data shared would be kept confidential. Willaby et al. (2015) suggested that a sample size as small as 100 was sufficient for acceptable power in model testing when PLS is used and when size effects are moderate. While we have used PLS and observed moderate to stronger size effects, nevertheless, we would recommend that the survey be replicated on a larger scale. Although the sampling was random and collected from security professionals across global industries, most respondents were from Asia-Pacific. One may surmise that this may have led to bias in the results. However, the psychometric properties of most of the items demonstrated good results, thus alleviating these concerns. While the respondents were primarily from the APAC region, they had considerable work experience in global organizations located throughout the world. Therefore, we believe the bias, if any, might be negligible. Cognitive abilities such as efficacy have triadic mutual interaction with personal, organizational, and environmental factors (Bandura, 1998). However, the threat environment's influence is more dominant on individual efficacy at the SIM process level than at the organizational level because a security incident is related to situational, environmental, and context-specific phenomenon. As our focus was specifically on the aspects of a security incident, we did not include the impact of organizational factors and their controllability in this study. We focused on personal (awareness and cognitive elements) and environmental (TMT) aspects. Although personality influences the relationship between CSSE and TMT, we did not consider it in this study as it is a more stable behavior that persists across situations in multiple domains than in any specific situation (Pajares, 2002). For example, other individual cognitive factors, such as self-observation, self-evaluation, and self-reaction, contribute to the same level of variance across multiple domains and do not exclusively play a role in TMT. Moreover, they are closely related to the RC (Pajares, 2002). Thus, by factoring MCA, our model represents a complete framework of individual cognitive variance.

We proposed a model conceptualizing the impact of CISA, MCA, and CSSE on TMT and empirically validated it through a survey of security professionals. The results established a significant effect of CISA, MCA, and CSSE on TMT. The results indicated that CISA can significantly regulate security professionals' efforts and orient their cognitive resources, thereby enhancing their CSSE and performance of TMTs. We discussed the significance of the study to practice and research and future work.

Author Credits Statement

Manisekaran Thangavelu: Conceptualization, Methodology, Data curation, Investigation, Visualization, Original draft preparation, Reviewing and Editing.

Venkataraghavan Krishnaswamy: Conceptualization, Methodology, Validation, Reviewing and Editing.

Mayank Sharma: Conceptualization, Methodology, Validation, Reviewing and Editing,

Funding

None.

Declaration of Competing Interest

None.

Supplementary materials

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.cose.2021.102401.

Appendix

Table A1, Table A2 and Table A3

Table A1 – Demographic details of participants

Detail	n=100	Percentage	Detail	n=100	Percentage	Detail	n=100	Percentage
Gender			Size			Country of residence		
Male	86	86.00	1000-4999	10	9.43	Australia	3	3.0
Female	14	14.00	5000-9999	14	13.20	Canada	2	2.0
Age group			500-999	19	17.92	Germany	2	2.0
21-25	19	19.00	Less than 500	16	15.09	India	63	63.0
26-35	53	53.00	More than 10000	41	44.33	Netherlands	3	3.0
36-45	27	27.00	**Certifications**			Middle east	10	10.0
46+	1	1.00	CEH	26	26.00	Singapore	5	5.0
Job function			CISA	3	3.00	United Kingdom	3	3.0
Security analyst	23	23.0	CISM	4	4.00	United States of America	3	3.0
Security consultant	21	21.00	CISSP	12	12.00	**Business domain**		
Security head	9	9.0	GIAC	2	2.00	Banking, Finance, Securities and Insurance	20	20.00
Security lead	7	7.0	1-3 certificates as above	27	27.00	Health care	2	2.00
Security manager	25	25.0	4-7 certificates as above	7	7.0	Manufacturing	4	4.00
Security senior analyst	15	15.0	No certificates	19	19.00	Product engineering	5	5.00
Revenue			**Regions worked**			More than one vertical	46	46.00
1- 5 Million	7	7.0	Asia	29	29.00	**Size of the security team**		
1 to 5 Billion	15	15.0	Europe	15	15.00	<5	5	5.00
10- 50 Million	16	16.0	Middle East	3	3.00	5-10	7	7.00
500 Million - 1 Billion	13	13.00	North America	22	22.00	10-20	14	14.00
50-500 Million	9	9.00	2-3 regions as above	21	21.00	21-30	10	10.00
5-10 Million	10	10.00	4-6 regions as above	16	16.00	31-40	15	15.00
Less than 1 Million	5	5.00				41-50	25	25.00
More than 5 Billion	25	25.00				51+	24	24.00
Education			**Experience (In years)**					
3 years Diploma	4	4.0	<5	28	28.00			
3/4 years Bachelor	34	34.0	6-10	26	26.00			
4 Plus Post-graduate	29	29.0	11-15	24	24.00			
Others	33	33.0	16-20	15	15.00			
			21+	7	7.00			

Table A2 – Item Description

Construct / Item	Source	Description
Security Awareness (SecA)		*This construct was developed for study with inputs from the sources mentioned.*
		As an information security professional managing security incident, I possess the awareness/knowledge
SecA1		to understand motives behind security attacks and threats
	Erbacher et al., 2010	
SecA2	Cheng et al., 2012	for constructing an attack path from indicators of security attacks and threats
SecA3	Cheng et al., 2012	to decipher methodologies adopted by the attacker
SecA4	Oltsik, 2015	to understand the key indicators of a specific method of Tactics, Techniques, and Procedures
SecA5*		to detect evidence for security investigations
	Cichonski et al., 2012	
System Awareness (SySA)		*This construct was developed for study with inputs from the sources mentioned.*
		As an information security professional managing security incident, I possess the awareness/knowledge
SysA1	Ponemon, 2019	to understand the system behavior in a normal state
SysA2		about inherent vulnerabilities of IT systems and the effects of their exploitation
SysA3		to understand the system behavior in an abnormal state
SysA4	Oltsik,2015	about existing mitigating controls or defenses to protect the IT systems
SysA5	Oltsik,2015	about the business value of IT systems and their mission
SysA6	Cheng et al., 2012	about system architecture to construct attack path
Situational Awareness (SitA)		*This construct was developed for study with inputs from the sources mentioned.*
		As an information security professional managing security incident, I possess the awareness/knowledge
SitA1	D'Amico et al.,2005	to precept or identify an attack situation from correlated information from attack indicators
SitA2		to construct an attack path from various situations by analyzing system behavior
SitA3		for deciphering the attack pattern either using prior experience or available threat intelligence
SitA4		to project the near future attack situation from the current state
Threat Detection (TD)		*This construct was developed for study with inputs from the sources mentioned.*
		While resolving information security incidents
TD1	Clark et al., 2007	I can decipher the key security events related to an attack from huge volumes
TD2	Clark et al., 2007	I can correctly enumerate the segregated events concerning specific impacted systems
TD3		I can construct the possible attack vectors and ascertain that threat is real from system evidence and its behavior
	Cichonski et al., 2012	
Threat Assessment (TA)		*This construct was developed for study with inputs from the sources mentioned.*
		While resolving information security incidents
TA1	Oltsik, 2015	I can accurately pin the scope of the attack and identify the impacted systems
TA2		I can effectively judge the impact of the attack
	Workman,2009	
TA3		I can effectively judge the likelihood of the attack becoming real
	Workman,2009	
TA4		I can effectively prioritize the incident
	Cichonski et al., 2012	
Threat Mitigation (TM)		*This construct was developed for study with inputs from the sources mentioned.*

(*continued on next page*)

Table A2 (*continued*)

		While resolving information security incidents
TM1	Cichonski et al.,2012	I can apply suitable countermeasures and fixes to prevent the impact of ongoing attack
TM2		I can apply suitable countermeasures and fixes to prevent the impact of future attacks
TM3		I can effectively restore the impacted system to its original state
TM4		I can apply suitable preventive measures to stop the attack from penetrating other systems and network
TM5		I can confirm that the restored system functions normally
Regulation of Cognition (RC)		*The construct was adopted from the source and modified to suit the TMT context*
		While managing information security incidents
P1 (Planning)	Schraw& Dennison, 1994	I think about what I need to do before I begin a task
P2 (Planning)		I set specific goals before I begin a task
P3 (Planning)		I think of several ways to perform a task and choose the best one.
M1 (Monitoring)		I ask myself periodically if I am meeting my intended incident tasks
M2 (Monitoring)		I consider several alternatives to an incident investigation before I act
M3 (Monitoring)		I ask myself questions about how well I am performing new types of security incident analysis.
E1 (Evaluation)		I know how well I did once I finish a task
E2 (Evaluation)		I ask myself if there was a better way to do things after I finish a task
E3 (Evaluation)		I ask myself if I have considered all options after I completed the tasks
E4 (Evaluation)		I ask myself if I learned as much as I could have once, I finished a task
Knowledge of Cognition (KC)		*The construct was adopted from the source and modified to suit the TMT context*
		While managing information security incidents
DK1 (Declarative Knowledge)	Schraw& Dennison, 1994	I understand my strengths and weaknesses in a security investigation
DK2 (Declarative Knowledge)		I know what kind of information is most important to perform the task
DK3 (Declarative Knowledge)		I think I am good at organizing information for incident management
DK4 (Declarative Knowledge)		I am good at remembering information needed for performing incident response tasks
DK5 (Declarative Knowledge)		I have control over how well I perform a task.
DK6 (Declarative Knowledge)		I am inclined to act when I am aware of the incident issues
PK1 (Procedural Knowledge)		I try to use strategies that have worked in the past.
PK2 (Conditional Knowledge)		I have a specific purpose for each strategy I use.
CK1 (Conditional Knowledge)		I use different strategies, depending on the situation.
CK2 (Conditional Knowledge)		I can motivate myself to perform when I need to.
CK3 (Conditional Knowledge)		I use my intellectual strengths to compensate for my weaknesses
Computer Security Self-efficacy (CSSE)		*The construct was adopted from the source and modified to suit the TMT context*
CSSE1	Ng et al., 2009	While managing information security incidents, I feel confident to undertake security attack investigation
CSSE2		analyze events and understand their nature
CSSE3		apply information and strategies to investigate possible security attack
CSSE4		apply information and strategies to reduce or mitigate possible security attack

* item dropped in final analysis SecA5, SitA2,M3,E4, PK1,PK2,CK3,DK4 and DK5

Table A3 – Cross Loading of Items.

Construct/Items	CISA	RC	KC	CSSE	TD	TA	TM
SecA1	**0.776**	0.577	0.672	0.582	0.290	0.425	0.320
SecA2	**0.744**	0.590	0.609	0.519	0.150	0.283	0.193
SecA3	**0.821**	0.650	0.672	0.614	0.286	0.422	0.321
SecA4	**0.725**	0.598	0.570	0.562	0.292	0.417	0.360
SitA1	**0.810**	0.649	0.656	0.670	0.323	0.453	0.342
SitA3	**0.756**	0.647	0.570	0.609	0.392	0.464	0.389
SitA4	**0.809**	0.657	0.645	0.598	0.373	0.493	0.516
SysA1	**0.767**	0.593	0.642	0.534	0.270	0.365	0.255
SysA2	**0.789**	0.629	0.641	0.607	0.299	0.428	0.283
SysA3	**0.698**	0.544	0.580	0.506	0.312	0.353	0.206
SysA4	**0.749**	0.594	0.613	0.581	0.345	0.447	0.359
SysA5	**0.728**	0.633	0.539	0.516	0.286	0.347	0.252
SysA6	**0.759**	0.666	0.558	0.504	0.211	0.368	0.298
P1	0.621	**0.822**	0.593	0.557	0.198	0.343	0.293
P2	0.665	**0.811**	0.595	0.451	0.248	0.339	0.376
P3	0.665	**0.813**	0.676	0.562	0.336	0.365	0.443
M1	0.641	**0.781**	0.681	0.518	0.282	0.278	0.280
M2	0.663	**0.799**	0.598	0.507	0.294	0.333	0.376
E1	0.716	**0.900**	0.660	0.577	0.282	0.371	0.351
E2	0.679	**0.823**	0.706	0.576	0.286	0.366	0.301
E3	0.575	**0.776**	0.628	0.573	0.311	0.348	0.392
DK1	0.698	0.654	**0.857**	0.666	0.374	0.482	0.446
DK2	0.705	0.671	**0.819**	0.717	0.338	0.469	0.416
DK3	0.631	0.679	**0.857**	0.677	0.389	0.488	0.374
DK6	0.619	0.663	**0.858**	0.683	0.392	0.513	0.431
CK1	0.688	0.615	**0.788**	0.629	0.396	0.474	0.444
CK2	0.678	0.659	**0.871**	0.674	0.369	0.498	0.443
CSSE1	0.718	0.618	0.734	**0.955**	0.488	0.641	0.518
CSSE2	0.668	0.614	0.748	**0.944**	0.400	0.589	0.475
CSSE3	0.726	0.670	0.785	**0.935**	0.475	0.612	0.560
CSSE4	0.684	0.608	0.742	**0.960**	0.444	0.599	0.534
TD1	0.283	0.257	0.349	0.356	**0.864**	0.582	0.615
TD2	0.360	0.322	0.385	0.467	**0.898**	0.632	0.653
TD3	0.371	0.333	0.409	0.447	**0.926**	0.664	0.657
TA1	0.507	0.381	0.481	0.531	0.597	**0.898**	0.610
TA2	0.339	0.245	0.370	0.492	0.558	**0.761**	0.676
TA3	0.469	0.421	0.518	0.574	0.599	**0.864**	0.641
TA4	0.520	0.388	0.547	0.613	0.655	**0.917**	0.711
TM1	0.392	0.306	0.397	0.472	0.650	0.696	**0.875**
TM2	0.463	0.390	0.508	0.547	0.601	0.672	**0.901**
TM3	0.308	0.391	0.389	0.442	0.699	0.674	**0.809**
TM4	0.387	0.367	0.383	0.455	0.606	0.678	**0.899**
TM5	0.423	0.442	0.463	0.507	0.621	0.665	**0.928**

REFERENCES

Abraham S, Chengalur-Smith I. Evaluating the effectiveness of learner controlled information security training. Comput. Security 2019;87. doi:10.1016/j.cose.2019.101586.

Ahmad A, Hadgkiss J, Ruighaver A. Incident response teams – Challenges in supporting the organisational security function. Comput. Security 2012;31(5):643–52. doi:10.1016/j.cose.2012.04.001.

Ahmad A, Maynard SB, Desouza KC, Kotsias J, Whitty MT, Baskerville RL. How can organizations develop situation awareness for incident response: A case study of management practice. Comput. Security 2021;101. doi:10.1016/j.cose.2020.102122.

Alberts, C., Dorofee, A., Killcrece, G., Ruefle, R., & Zajicek, M. (2004). Defining incident management processes for CSIRTs: A work in progress. https://doi.org/10.21236/ada453378

Anuar NB, Papadaki M, Furnell S, Clarke N. Incident prioritisation using analytic hierarchy process(AHP): Risk Index Model (RIM). Security and Commun. Netw. 2012;6:1087–116. doi:10.1002/sec.673.

Arachchilage NA, Love S. Security awareness of computer users: A phishing threat avoidance perspective. Comput. Hum. Behav. 2014;38:304–12. doi:10.1016/j.chb.2014.05.046.

Bandura A. Self-efficacy. In: Encyclopedia of human behavior, 4. New York: Academic Press; 1994. p. 71–81.

Bandura A. Personal and collective efficacy in human adaptation and change. Adv. psychol. sci. 1998;1:51–71.

Bartnes M, Moe NB, Heegaard PE. The future of information security incident management training: A case study of electrical power companies. Comput. Security 2016;61:32–45. doi:10.1016/j.cose.2016.05.004.

Barnum S. Standardizing cyber threat intelligence information with the structured threat information expression (stix). Mitre Corporation 2014;11:1–22 version 1.1.

Bartnes M, Moe NB. Challenges in IT security preparedness exercises: A case study. Comput. Security 2017;67:280–90. doi:10.1016/j.cose.2016.11.017.

Bouffard-Bouchard T. Effect of activating conditional knowledge on self-efficacy and comprehension monitoring. Int. J. Behav. Development 1994;17(3):577–92. doi:10.1177/016502549401700311.

Brown R, Lee RM. The Evolution of Cyber Threat Intelligence (CTI): 2019 SANS CTI Survey. Singapore: SANS Institute; 2019.

Bulgurcu B, Cavusoglu H, Benbasat I. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Q. 2010:523–48.

Burger CJ, Raelin JA, Reisberg RM, Bailey MB, Whitman D. In: 2010 ASEE Southeast Section Conference. Self-efficacy in female and male undergraduate engineering students: Comparisons among four institutions; 2010.

Callan GL, Marchant GJ, Finch WH, German RL. Metacognition, strategies, achievement, and demographics: Relationships across countries. Educational Sci.: Theory & Practice 2016;16(5).

Campbell JP, McCloy RA, Oppler SH, Sager CE. A Theory of Performance. In: Schmitt N, Borman WC, editors. In: Personnel Selection in Organizations. San Francisco: Jossey-Bass; 1993. p. 3570.

Cera R, Mancini M, Antonietti A. Relationships between metacognition, self-efficacy and self-regulation in learning. ECPS - Educational, Cultural and Psychol. Stud. 2013(7):115–41. doi:10.7358/ecps-2013-007-cera.

Chen CC, Shaw RS, Yang SC. Mitigating information security risks by increasing user security awareness: A case study of an information security awareness system. Inf. Technol., Learning & Performance J. 2006;24(1).

Cheng Y, Sagduyu Y, Deng J, Li J, Liu P. Integrated situational awareness for cyber-attack detection, analysis, and mitigation. Sensors and Sys. Space Appl. V 2012. doi:10.1117/12.919261.

Choi M, Levy Y, Hovav A. The role of user computer self-efficacy, cybersecurity countermeasures awareness, and cybersecurity skills influence on computer misuse. Proceedings of the Pre-International Conference of Information Systems (ICIS) SIGSEC–Workshop on Information Security and Privacy (WISP), 2013.

Cichonski P, Millar T, Grance T, Scarfone K. Computer security incident handling guide. NIST Spec. Publ. 2012;800(61):1–147.

Clark JA, Murdoch J, McDermid JA, Sen S, Chivers H, Worthington O, Rohatgi P. Threat modelling for mobile ad hoc and sensor networks. In: Annual Conference of ITA; 2007. p. 25–7.

Compeau DR, Higgins CA. Computer self-efficacy: Development of a measure and initial test. MIS quarterly 1995:189–211.

Coutinho S. Self-efficacy, metacognition, and performance. North Am. J. Psychol. 2008;10(1).

D'Amico A, Whitley K, Tesone D, O'Brien B, Roth E. Achieving cyber defense situational awareness: A cognitive task analysis of information assurance analysts. Proceedings of the Human Factors and Ergonomics Society Annual Meeting 2005;49(3):229–33. doi:10.1177/154193120504900304.

D'Amico A, Kocka M. Information assurance visualizations for specific stages of situational awareness and intended uses: lessons learned. IEEE Workshops on Visualization for Computer Security (VizSec'05) 2005. doi:10.1109/vizsec.2005.13.

D'Arcy J, Hovav A, Galletta D. User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. Inf. Syst. Res. 2009;20(1):79–98. doi:10.1287/isre.1070.0160.

De Carvalho Filho MK, Yuzawa M. The effects of social cues on confidence judgments mediated by knowledge and regulation of cognition. The J. Experimental Education 2010;69(4):325–43. doi:10.1080/00220970109599491.

Diamantopoulos A, Siguaw JA. Formative versus reflective indicators in organizational measure development: A comparison and empirical illustration. Br. J. Manage. 2006;17(4):263–82. doi:10.1111/j.1467-8551.2006.00500.x.

Edwards JR. Multidimensional constructs in organizational behavior research: an integrative analytical framework. Organizational Research Methods 2001;4(2):144–92. doi:10.1177/109442810142004.

Endsley MR. undefined. Human Factors: The J. Hum. Factors and Ergonomics Society 1995;37(1):32–64. doi:10.1518/001872095779049543.

Endsley MR. Situation awareness misconceptions and misunderstandings. J. *Cognitive Eng. Decision Making* 2015;9(1):4–32. doi:10.1177/1555343415572631.

Erbacher RF, Frincke DA, Wong PC, Moody S, Fink G. Cognitive task analysis of network analysts and managers for network situational awareness. Visualization and Data Anal. 2010 2010. doi:10.1117/12.845488.

Eteläpelto A. Metacognition and the expertise of computer program comprehension. Scandinavian J. Educational Res. 1993;37(3):243–54.

Fireeye (2012) The Importance of Security Awareness, Threat Research, Fireeye, URL: https://www.fireeye.com/blog/threat-research/2012/10/importance-security-awareness.html (last accessed: 6th June 2021).

Franke U, Brynielsson J. Cyber situational awareness – A systematic review of the literature. Comput. Security 2014;46:18–31. doi:10.1016/j.cose.2014.06.008.

Fornell C, Larcker DF. Evaluating structural equation models with unobservable variables and measurement error. J. Marketing Res. 1981;18(1):39–50. doi:10.1177/002224378101800104.

Gefen D, Straub D, Boudreau M. Structural equation modeling and regression: Guidelines for research practice. Commun. Association for Info. Sys. 2000;4. doi:10.17705/1cais.00407.
Goodhue DL, Straub DW. Security concerns of system users. Info. Manage. 1991;20(1):13–27. doi:10.1016/0378-7206(91)900.
Hadwin AF, Bakhtiar A, Miller M. Challenges in online collaboration: effects of scripting shared task perceptions. Intern. J. Comput.-Support. Collab. Learn 2018;13:301–29. doi:10.1007/s11412-018-9279-9.
Hair JF, Ringle C, Sarstedt M. PLS-SEM: Indeed a silver bullet. J. Marketing Theory and Practice 2011;19(2):139–52.
Hair JF, Ringle CM, Sarstedt M. Partial least squares structural equation modeling: Rigorous applications, better results and higher acceptance. Long Range Plann. 2013;46(1-2):1–12. doi:10.1016/j.lrp.2013.01.001.
Hart S, Margheri A, Paci F, Sassone V. Riskio: A serious game for cyber security awareness and education. Comput. Security 2020;95. doi:10.1016/j.cose.2020.101827.
Hanus B, Wu YA. Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. Info. Sys. Manage. 2016;33(1):2–16.
Haynie JM, Shepherd D, Mosakowski E, Earley PC. A situated metacognitive model of the entrepreneurial mindset. J. Bus. Venturing 2010;25(2):217–29. doi:10.1016/j.jbusvent.2008.10.001.
Helkala K, Knox B, Josok O. In: 2015 IEEE Frontiers in Education Conference (FIE). How the application of coping strategies can empower learning; 2015a. doi:10.1109/fie.2015.7344120.
Helkala K, Knox S, Lund M. Effect of motivation and physical fitness on cyber tasks. In: Proceedings of International Symposium on Human Aspects of Information Security & Assurance; 2015b. p. 108–19.
Henseler J, Ringle CM, Sarstedt M. A new criterion for assessing discriminant validity in variance-based structural equation modeling. J. Acad. Marketing Sci. 2014;43(1):115–35. doi:10.1007/s11747-014-0403-8.
Hepler TJ, Feltz DL. Take the first heuristic, self-efficacy, and decision-making in sport. J. Experimental Psychol.: Applied 2012;18(2):154–61. doi:10.1037/a0027807.
Horrocks I. Security training: Education for an emerging profession? Comput. Security 2001;20(3):219–26. doi:10.1016/s0167-4048(01)00306-6.
Hogan MJ, Dwyer CP, Harney OM, Noone C, Conway RJ. Metacognitive skill development and applied systems science: A framework of Metacognitive skills, self-regulatory functions and real-world applications. Intelligent Sys. Reference Library 2014:75–106. doi:10.1007/978-3-319-11062-2_4.
Hsiao JCY, Moser C, Schoenebeck S, Dillahunt TR. The role of demographics, trust, computer self-efficacy, and ease of use in the sharing economy. In: Proceedings of the 1st ACM SIGCAS Conference on Computing and Sustainable Societies; 2018. p. 1–11.
Hutchins EM, Cloppert MJ, Amin RM. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. Leading Issues in Inf. Warfare & Security Res. 2011;1(1):80.
ISO/IEC 27035. In: Revised as *ISO/IEC 27035:2016*. Information technology – Security techniques – Information security incident management; 2011. URL: https://www.iso.org/standard/44379.html (last accessed: 20th June 2019).
Killcrece, G., Kossakowski, K., Ruefle, R., & Zajicek, M. (2003). State of the practice of computer security incident response teams (CSIRTs). https://doi.org/10.21236/ada421664
Klein, Rai. Interfirm strategic information flows in logistics supply chain relationships. MIS Quarterly 2009;33(4):735. doi:10.2307/20650325.
Knight R, Nurse JR. A framework for effective corporate communication after cyber security incidents. Comput. Security 2020;99. doi:10.1016/j.cose.2020.102036.
Knox BJ, Lugo RG, Jøsok Ø, Helkala K, Sütterlin S. Towards a cognitive agility index: the role of metacognition in human computer interaction. In: International Conference on Human-Computer Interaction. Cham: Springer; 2017. p. 330–8.
Kock N. Common method bias in PLS-SEM: A full collinearity assessment approach. Int. J. e-Collaboration (ijec) 2015;11(4):1–10.
Kock N. Harman's single factor test in PLS-SEM: Checking for common method bias. Data Anal. Perspectives J. 2020;2(2).
Kruger H, Kearney W. A prototype for assessing information security awareness. Comput. Security 2006;25(4):289–96. doi:10.1016/j.cose.2006.02.008.
La Fleur C, Hoffman B, Gibson CB, Buchler N. Team performance in a series of regional and national US cybersecurity defense competitions: Generalizable effects of training and functional role specialization. Comput. Security 2021;104. doi:10.1016/j.cose.2021.102229.
Legg AM, Locker Jr, L. Math performance and its relationship to math anxiety and metacognition. North Am. J. Psychol. 2009;11(3).
Lewis RA. Predictors of US Teachers' Use of Metacognition in Mathematics Instruction. Walden University; 2016. Doctoral dissertation.
Livingston, J. A. (2003). Metacognition: An Overview.
Liu P, Jia X, Zhang S, Xiong X, Jhi YC, Bai K, Li J. Cross-layer damage assessment for cyber situational awareness. In: Cyber Situational Awareness. Boston, MA: Springer; 2010. p. 155–76.
MacKenzie Podsakoff, Podsakoff. Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques. MIS Quarterly 2011;35(2):293. doi:10.2307/23044045.
Martocchio JJ, Hertenstein EJ. Learning orientation and goal orientation context: Relationships with cognitive and affective learning outcomes. Hum. Resource Develop. Q. 2003;14(4):413–34. doi:10.1002/hrdq.1077.
Mathew S, Britt D, Giomundo R, Upadhyaya S, Sudit M, Stotz A. In: MILCOM 2005 - 2005 IEEE Military Communications Conference. Real-time multistage attack awareness through enhanced intrusion alert clustering; 2005. doi:10.1109/milcom.2005.1605934.
Mitropoulos S, Patsos D, Douligeris C. On Incident Handling and Response: A state-of-the-art approach. Comput. Security 2006;25(5):351–70. doi:10.1016/j.cose.2005.09.006.
Moores TT, Chang JC, Smith DK. Clarifying the role of self-efficacy and metacognition as predictors of performance. ACM SIGMIS Database: the DATABASE for Advances in Info. Sys. 2006;37(2-3):125–32. doi:10.1145/1161345.1161360.
Naseer H, Maynard SB, Desouza KC. Demystifying analytical information processing capability: The case of cybersecurity incident response. Decision Support Systems 2021;143. doi:10.1016/j.dss.2020.113476.
Ng B, Kankanhalli A, Xu Y. Studying users' computer security behavior: A health belief perspective. Decision Support Sys. 2009;46(4):815–25. doi:10.1016/j.dss.2008.11.010.
Nunnally J. Psychometric theory. 2nd edition. New York: McGraw-Hill; 1978.
O'Brien KS, O'Hare D. Situational awareness ability and cognitive skills training in a complex real-world task. Ergonomics 2007;50(7):1064–91.
Onwubiko C. In: 2009 IEEE International Conference on Intelligence and Security Informatics. Functional requirements of situational awareness in computer network security; 2009. doi:10.1109/isi.2009.5137305.

Oltsik J. Tackling Attack Detection and Incident Response. Enterprise Strategy Group; 2015. URL https://www.cbronline.com/wp-content/uploads/dlm_uploads/2016/10/rp-esg-tackling-attack-detection-incident-response.pdf (last accessed: 20th June 2019).
Pajares F. Self-efficacy beliefs in academic settings. Rev. educational res. 1996;66(4):543–78.
Pajares, F. (2002). Self-efficacy beliefs in academic contexts: An outline.
Petter Rai, Straub. The critical importance of construct measurement specification: A response to Aguirre-urreta and Marakas. MIS Quarterly 2012;36(1):147. doi:10.2307/41410411.
Phelps Daniel, Gathegi John. Information System Security: Self-Efficacy and Implementation Effectiveness. AMCIS, 2006 Proceedings, 2006. http://aisel.aisnet.org/amcis2006/404.
Pintrich PR, De Groot EV. Motivational and self-regulated learning components of classroom academic performance. J. Educ. Psychol. 1990;82(1):33–40. doi:10.1037/0022-0663.82.1.33.
Ponemon (2019) "Improving the Effectiveness of the Security Operations Center", https://www.devo.com/wp-content/uploads/2019/07/2019-Devo-Ponemon-Study-Final.pdf (Last accessed, May 2021)
PwC report, " Information security breaches survey" 2015 | technical report. URL: https://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-03.pdf, (last accessed: 20th June 2019).
Reeve RA, Brown AL. Metacognition reconsidered: Implications for intervention research. J. Abnorm. Child Psychol. 1985;13(3):343–56. doi:10.1007/bf00912721.
Rhee H, Kim C, Ryu YU. Self-efficacy in information security: Its influence on end users' information security practice behavior. Comput. Security 2009;28(8):816–26. doi:10.1016/j.cose.2009.05.008.
Ringle, C. M., Wende, S., & Will, A. (2005). SmartPLS 3.0
Rogers, M. M. (2020). Metacognition and Living Above Zero.
Rongrong X, Xiaochun Y, Zhiyu H. Framework for risk assessment in cyber situational awareness. IET Inf. Secur. 2018;13(2):149–56.
Ruefle, R.M., & Murray, M. (2014). CSIRT requirements for situational awareness. doi:10.21236/ada596848.
Schmidt AM, Ford JK. Learning within a learner control training environment: The interactive effects of goal orientation and metacognitive instruction on learning outcomes. Pers. Psychol. 2006;56(2):405–29. doi:10.1111/j.1744-6570.2003.tb00156.x.
Schraw G, Dennison RS. Assessing metacognitive awareness. Contemp. Educ. Psychol. 1994;19(4):460–75.
Shreve GM. Recipient-orientation and metacognition in the translation process. Dimitriu, Rodica & Miriam Shlesin 2009.
Singh J, Cobbe J. The security implications of data subject rights. IEEE Security & Privacy 2019;17(6):21–30. doi:10.1109/msec.2019.2914614.
Straub DW, Welke RJ. Coping with systems risk: Security planning models for management decision making. MIS Quarterly 1998;22(4):441. doi:10.2307/249551.
Tan T, Ruighaver AB, Ahmad A. Incident Handling: Where the need for planning is often not recognised. In: 1st Australian computer, network & information forensics conference; 2003. p. 1–10.
Thangavelu M, Krishnaswamy V, Sharma M. Comprehensive Information Security Awareness (CISA) in Security Incident Management (SIM): A Conceptualization. South Asian J. Manage. 2020;27(2).
Tosun OK. Cyber-attacks and stock market activity. Int. Rev. Fin. Anal. 2021.
Tounsi W, Rais H. A survey on technical threat intelligence in the age of sophisticated cyber attacks. Computers & Security 2018;72:212–33. doi:10.1016/j.cose.2017.09.001.
Trevethan R. Deconstructing and assessing knowledge and awareness in public health research. Frontiers in Public Health 2017;5. doi:10.3389/fpubh.2017.00194.
Turner P. Selective and intelligent imaging using digital evidence bags. Digital Investigation 2006;3:59–64. doi:10.1016/j.diin.2006.06.003.
Tzeng J. The impact of general and specific performance and self-efficacy on learning with computer-based concept mapping. Comput. Hum. Behav. 2009;25(4):989–96. doi:10.1016/j.chb.2009.04.009.
Varga S, Brynielsson J, Franke U. Cyber-threat perception and risk management in the Swedish financial sector. Comput. Security 2021;105. doi:10.1016/j.cose.2021.102239.
Voitovych O, Baryshev Y, Kolibabchuk E, Kupershtein L. In: 2016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T. Investigation of simple denial-of-service attacks; 2016. doi:10.1109/infocommst.2016.7905362.
Wagner TD, Mahbub K, Palomar E, Abdallah AE. Cyber threat intelligence sharing: Survey and research directions. Comput. Security 2019;87. doi:10.1016/j.cose.2019.101589.
Webb J, Ahmad A, Maynard SB, Shanks G. A situation awareness model for information security risk management. Comput. Security 2014;44:1–15. doi:10.1016/j.cose.2014.04.005.
Werlinger R, Muldner K, Hawkey K, Beznosov K. Preparation, detection, and analysis: The diagnostic work of IT security incident response. *Information Manage*. Comput. Security 2010;18(1):26–42. doi:10.1108/09685221011035241.
Willaby HW, Costa DS, Burns BD, MacCann C, Roberts RD. Testing complex models with small sample sizes: A historical overview and empirical demonstration of what partial least squares (PLS) can offer differential psychology. Personality and Individual Differences 2015;84:73–8. doi:10.1016/j.paid.2014.09.008.
Wiik J, Kossakowski KP. In: 17th Annual FIRST Conference on Computer Security Incident Handling. Dynamics of incident response Singapore; 2005.
Wilson M, de Zafra DE, Pitcher SI, Tressler JD, Ippolito JB. Information technology security training requirements: A role-and performance-based model. NATIONAL INST OF STANDARDS AND TECHNOLOGY GAITHERSBURG MD COMPUTER SECURITY DIV 1998.
Winne PH, Hadwin AE. In: Studying as self-regulated learning. Routledge; 1998. p. 291–318.
Woods DD. Coping with complexity: the psychology of human behavior in complex systems. In: Tasks, errors, and mental models. Taylor & Francis, Inc; 1988. p. 128–48.
Workman M, Bommer WH, Straub D. The amplification effects of procedural justice on a threat control model of information systems security behaviours. Behav. Inf. Technol. 2009;28(6):563–75. doi:10.1080/01449290802556021.
Yang SJ, Byers S, Holsopple J, Argauer B, Fava D. In: 2008 IEEE International Conference on Intelligence and Security Informatics. Intrusion activity projection for cyber situational awareness; 2008. doi:10.1109/isi.2008.4565048.
Yuill J, Wu F, Settle J, Gong F, Forno R, Huang M, Asbery J. Intrusion detection for incident-response, using a military battlefield-intelligence process. Comput. Networks 2000;34(4):671–97. doi:10.1016/s1389-1286(00)00142-0.
Zhang Z, Ho PH, He L. Measuring IDS-estimated attack impacts for rational incident response: A decision theoretic approach. Comput. Security 2009;28(7):605–14. doi:10.1016/j.cose.2009.03.005.
Zimmerman BJ. Attaining Self-Regulation: A Social Cognitive Perspective. In: Boekaerts PRP, Zeidner M, editors. In: Handbook of Self-regulation. San Diego, CA: Academic Press; 2000. p. 13–41.

Manisekaran holds a Master's degree in Engineering science from the Indian Institute of Technology Madras. He is currently pursuing his executive fellowship in management from the area of Information technology and systems, Indian institute of management, Kashipur. Manisekaran is a Certified Information Systems Security Professional and a member of ISACA and ISC2. He has more than 16 years of experience in investigation of security incidents, network security and governance, risk and compliance of ISO27001, SOX, HIPPA, PCI, SOC, etc.

Venkataraghavan Krishnaswamy is an Associate Professor in the Information Systems and Technology area of the Indian Institute of Management Kashipur. His research interests are in the incorporation of consumer behavioural aspects into the design of information systems, specifically electronic negotiation systems and the adoption of emerging information technologies. He has industry experience of eight years. Before joining academia, he worked as a Principal Data Scientist and had developed predictive models for customer segmentation and multi-brand loyalty. He has published in journals such as Annals of Tourism Research, Group Decision and Negotiation and Information System Frontiers.

Mayank Sharma is an Assistant Professor at the Indian Institute of Management Kashipur. He is associated with the information systems and technology area. He did his Fellow Program in Management from Indian Institute of Management Lucknow. He has prior industry experience of four years. His current research interests are in the area of online communities, social networks and behavioural aspects of information systems. He has published in journals such as Annals of Tourism Research and International Journal of Productivity and Performance Management.