

---

# Journal of Informatics and Web Engineering

Vol. 4 No. 1 (February 2025)

eISSN: 2821-370X

---

## Exploration of The Impact of Cyber Situational Awareness On Small and Medium Enterprises (SMEs) in Malaysia

Tan Chee Keong<sup>1\*</sup>, Sofiah Kadar Khan<sup>2</sup>, Umar Farooq Khattak<sup>3</sup>

<sup>1,2,3</sup> UNITAR International University, Tierra Crest, Jalan SS 6/3, Ss 6, 47301 Petaling Jaya, Selangor, Malaysia

\*Corresponding author: (unu2200704@student.unitar.my; ORCID:0009-0001-7151-7926)

*Abstract* - The objective of this study is to explore the cyber situational awareness (CSA) level among the employees of small and medium-sized enterprises (SME) in Malaysia, by extending Endsley's situation awareness (SA) theory. It is crucial to understand the level of cyber situational awareness among employees as it sheds light on how well the employees understand the cyber threats and if they can handle them effectively. Literature has reviewed that SMEs are subject to a greater danger of cyber-attacks. Therefore, employees' awareness of cyber situations is of the utmost significance in studying cyber security. A convenient non-probability sampling method was chosen due to less expensive to deploy and increase the efficiency of data collection processes. IBM SPSS was used to conduct descriptive exploration data analysis that provides insight into the employee's current CSA by categorizing the employees into good, average, and poor understanding of the CSA. A total of 443 surveys were collected in the study, the findings reveal that most employees are not adequately aware of cyber situations, and employees understand the need to adhere to cyber security policy within the organization but fail to comply. The study contributes to practical domain by identifying the current level of CSA, SMEs should be set forth to create a strong culture of cyber security awareness and compliance and prioritize cyber security as part of the organization's culture to improve overall employee engagement and motivation in dealing with cyber threats.

*Keywords*— Cyber Security, Small and Medium-sized Enterprises, Cyber Situation Awareness, Cyber Threats, Cyber Protection Behavior

*Received: 23 September 2024; Accepted: 18 December 2024; Published: 16 February 2025*

*This is an open access article under the [CC BY-NC-ND 4.0](https://creativecommons.org/licenses/by-nc-nd/4.0/) license.*



---

### 1. INTRODUCTION

The study focused on assessing the cyber situational awareness level among the employees of SMEs in Malaysia. The study primarily focused on understanding their awareness of cyber situation threats, understanding their readiness and ability to handle potential cyber threats effectively. Cyber situational awareness (CSA) is essential for investigating the potential of possible risks, weaknesses, and current state of cyber security. CSA helps SME businesses to understand the cyber threat landscape, enabling SMEs to inform decision of implementation cyber security protection

measures and controls to mitigate cyber risk and cultivates awareness of the need to act on potential cyber incidents [1].

SMEs are the primary target of 43% of cyberattacks, but only 14% are prepared to defend themselves with sufficient training and education, according to Accenture's Cost of Cybercrime Study [2], but they are often underestimate the severity and frequency of cyberattacks, leading to a lack of awareness and understanding regarding the risks they face subsequently facing huge amount of loses and losing their competitive advantage [3]. According to Cyber security Ventures, the monetary value that involves cybercrime activities is the largest ever recorded, estimated at a growth rate of fifteen percent year over year [4]. Cybercrime is expected to increase from its 2015 cost of \$3 trillion worldwide to an annualized \$10.5 trillion by 2025. The historical cybercrime data, including recent year-over-year (YoY) growth it was indicated by Steve Morgan, the chief editor of cybercrime, that the cost of cybercrime would total USD 6 trillion globally [5].

In recent years, Malaysia has seen a rapid growth in the SME sector. As digital technologies have become more widespread, it is no surprise that digitalization has become an important factor for Malaysian SMEs in terms of gaining their competitive advantage and survival [6]. The Malaysian economy is driven mainly by SMEs, with ninety per cent of the companies now active in Malaysia fall under the category of SME [7]. The SMEs in Malaysia are digitally inclined which prompts attention among researchers to further explore the impact of creating awareness to eliminate or decrease cybersecurity crimes. The digital economy in Malaysia has been seeing fast expansion over the past decade, currently is contributing to 22.6% to the entire country's GDP and expected to rise to 25.5% by 2025 [8]. However, the emergence of new digital technology usages, such as e-wallets, social media platforms, and mobile banking applications connected under the SME digitalization ecosystem, has provided an opportunity for the emergence of cybercrime activities. It is now becoming a significant concern for this digital economy technology [9]. Thus, there is a need to initiate a forward-thinking initiative that assists SMEs in expanding and thriving in the digital economic environment that is exceptionally challenging. It is necessary to educate SMEs and community to defend their business interests both now and, in the future, as Malaysia is currently on a path toward becoming increasingly SME-digitalized [7].

Renaud and Ophoff had highlighted there is limited research on cyber situation awareness in SMEs, which refers to individuals' awareness of the cyber threats they face and their ability to comprehend the potential consequences which advocated further research on the degree of awareness of cyberattack among employees [1]. The SMEs' constraint in protecting their business from cyber threats highlighted the need to understand their employees' CSA level. To the best of our knowledge, there is limited research directly examined the CSA among the employees of SMEs in Malaysia, making this study an important contribution to serve as foundation for future study and establish the baseline in this unexplored area. The exploration of this study is built with Dr Mica Endsley's foundation theory of situational awareness (SA). This study aimed to explore the level of CSA among the employees of SMEs in Malaysia to address the research objective.

*ROI: To examine the level of cyber situational awareness among the employees of SMEs in Malaysia.*

*RQ1: What is the current level of cyber situational awareness among the employee of SMEs in Malaysia.*

## 2. LITERATURE REVIEW

In the digital age, SMEs are facing an increasing vulnerability to cyberattacks [9]. One key factor to protect SMEs digital business is by increasing CSA among employees, being aware of the cyber threats they may encounter, taking proactive steps to safeguard their businesses, and understanding the precautionary measures required to shield themselves from potential attacks [1]. It is pertinent to understand the factors that influence CSA, furthermore cyber protection motivational behavior (CB) is crucial for developing effective cyber security strategies and interventions [1], [10]. Focus on SMEs context in cyber security aspect is critical [11]. Past studies identified that research and training programs had focused on larger organizations, leaving SMEs' unique needs and vulnerabilities unaddressed [12]. There is a need to conduct further research that addresses explicitly the cyber security challenges faced by SMEs and develop tailored strategies and training programs to enhance their cyber situation awareness [12]. Afterall, every industry faced unique concerns thus it is important to design tailored strategy that considering the factors involved to apply effective mitigation measures [13]. Increased CSA will lead to more assertive cyber protection behavior to enhance the cyber security posture in SME environment [1]. Existing literature on CSA and SMEs reveals significant gaps, particularly in the Malaysian context leading the need for more focuses research required in this area. While

there is no direct past studies conducted in Malaysia focuses on CSA among employees in SMEs, finding from other targeted group provides indirect benchmark. For example, study from Mammadov et al. in assessing the awareness level among the Organization of the Islamic Cooperation - Computer Emergency Response Team (OIC-CERT) member in cyber incident shows only 37% of respondents successfully responded to the awareness test. Only 10% react to the incident in a timely manner [14]. Another research from Zulkifli et al. in studying cyber security awareness in secondary school indicated that only 40% of teachers are aware of that birthday, name and address are considered as personal data which need extra protection. However, parents show higher awareness that reach up to 75% [15]. The exploration of CSA level among the employees of SMEs in Malaysia will provide a baseline, serves as starting point for future research in cyber security domain.

The exploration of this study is built with Dr Mica Endsley's foundation theory of situational awareness (SA). Dr Mica described SA as "the perception of the elements of the environment within a volume of time and space, the comprehension of their significance, and the projection of their status in the near future" [16] Past studies that were looked at reflected this point of view, making it clear that Endsley's definition and three-level SA model significantly influenced the narratives [17]. Figure 1 shows Endsley's model of situation awareness.

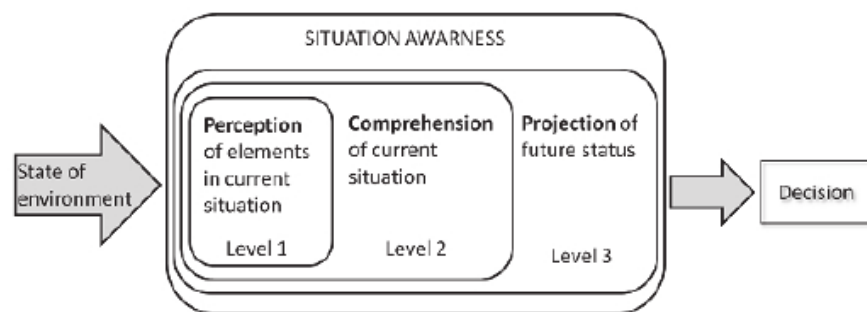


Figure 1. Endsley's Situation Awareness Model, Adapted from Endsley [17]

There are reportedly three different tiers of situational awareness, as described by Endsley.

**Perception (Level 1):** Awareness of necessary knowledge regarding a specific subject. Such knowledge may come to the individual by chance, but the decision-maker often must seek it out actively. Many SMEs don't know how critical cyber security is, and the fact that they don't take the proper precautions is a considerable concern [12]. SMEs may need to be made aware that cyber security risks pose a substantial threat and that cyber-attacks might force them out of business [1].

**Comprehension (Level 2):** Developing a consistent and complete interpretation of the circumstance across the board. It is not sufficient for a person to only be aware of the cyber threats and risks to ensure that they will succeed in reaching this level. What is required is an understanding of the importance of being mindful of cyber threats and acting appropriately. This level corresponds to SMEs knowing which controls and safeguards to implement [1]

**Projection (Level 3):** After reaching level 2, the individual will have the option of taking action to address the concerns. The person making the call might have biases and assumptions when they make the decision. Endsley says that to make the best decisions, people should make sure their beliefs are based on a solid knowledge or ask the right experts for this consultation [17]. On the other hand, people may also be misled, and if this is the case, their capacity to make the best choice will be hindered due to their erroneous beliefs. Even if they decide to act, they may not have the right resources.

Endsley's model of situational awareness was used to pull out several elements from the research that could affect SMEs' cyber situational awareness and factors that affect how SMEs use cyber security controls and precautions [1]. Endsley's theory is the most prominent SA theory in human-factors fields. Therefore, it's no surprise that his ideas are at the center of these discussions [18]. Nevertheless, Gutzwiller et al. indicates that the benefit of SA analysis and measurement has not yet been realized in cyberspace, unlike in other industries such as aviation, transportation, process control and nuclear power plant control, healthcare, and interactions with autonomous systems [19].

Renaud and Ophoff extend Endsley's situation awareness model to the context of cyber security and suggest that CSA is a critical element of cyber security practices. CSA pertains to the ability to comprehend and predict the condition of the environment, encompassing potential risks, weaknesses, and the current state of an entity's cyber security [1]. Technology plays a crucial part in terms of external environment and the ability for an organization to adapt to the changes in technology allows it to remain competitive [20]. CSA is an external environmental factor which can have a potential effect on the competitiveness of an organization and for it to remain sustainable [1]. SMEs may need to be made aware that cyber security risks pose a substantial threat and that cyber-attacks might force them out of business [1]. It is not sufficient for a person to only be aware of the cyber threats and risks to ensure understanding about available tools and controls and act accordingly. This study will expand Endsley's theory of situation awareness to present a model of SMEs' cyber situational awareness and the extent to which factors prompt the execution of cyber security implementation.

According to Gibbs, increased cyber security awareness has the potential to yield favorable outcomes in terms of employee behavior control and decision-making about cyber security investment and training [21]. According to Osbon and Simson [22], Robert Walters and Vacanysoft [23], and Zainal et al. [24], the following references have been cited; by taking proactive steps to strengthen their cyber security posture, SMEs can safeguard their sensitive data and maintain the trust of their customers and partners. Several studies have shown that human security factor is essential for protecting businesses from cyberattacks, past research focuses on cyber security skills of individual without clarifying where specific research gaps exist in cyber security behavior [25]. The exploratory method was chosen because there was a pressing need to have more comprehend research on cyber situation awareness in the context of SMEs, as pointed out by much past research [1], [19]. This approach enabled a deeper understanding of the initial stages of cyber situation awareness development and its impact on the cyber security protection strategies across SMEs [10].

### 3. RESEARCH METHODOLOGY

The research methodology used non-probability sampling techniques, specifically convenience sampling techniques, utilized an online survey created by Google Forms as an instrument and distributed it via several social media platforms and messaging channels. The convenience sampling technique was selected because it is often less expensive to deploy and easy and quick to collect data from those readily available to participate in the study [26]. This enhances the relevance and efficiency of the research by targeting only SME employees to meet the research objective and to save time and resources by focusing on a specific group of respondents [27].

The research starts with the pilot study phase to test the suitability of instruments for data collection, identifies potential issues, such as ambiguous questions, unclear instructions, or problematic response patterns. Several revisions were made to the survey questions based on feedback from the pilot group the subject method experts, enhancing its quality and ensuring its suitability for large-scale implementation [28]. Follow by the pilot study, mass survey was deployed based on the refined questionnaire to assess the level of CSA among the employees in SMEs. The survey consists of 3 sections tailored explicitly for different purposes. The first section verifies that only the participants working with SMEs in Malaysia are qualified to participate in the survey. The second section gathers demographic information about the participants, including the company's cyber security practices. The last section comprises 15 questions in quiz form using the scale measurements "Yes," "No," and "Partial" to assess the participants' cyber situational awareness level and evaluate their knowledge and readiness to handle potential cyber threats. Table 1 below shows the survey questionnaire used in this study.

Table 1. Survey Questionnaire

| Section               | Label          | Item Detail  | References     |
|-----------------------|----------------|--|----------------|
| Participant Screening | Not Applicable | I'm working in small medium-size Enterprise (SME) in Malaysia. | Not Applicable |

|                                   |         |  |                             |
|-----------------------------------|---------|--|-----------------------------|
| Demographic                       | SMEType | My organization has clearly written cyber security policies and has experts to manage cyber security protection.                                 | Not Applicable              |
|                                   | Gender  | Gender   | Not Applicable              |
|                                   | Age     | Age  | Not Applicable              |
|                                   | Edu     | Education Level  | Not Applicable              |
|                                   | CL      | Career Level   | Not Applicable              |
|                                   | WE      | Working Experience   | Not Applicable              |
|                                   | Cattack | Have you experienced any cyber-attack before? (Like computer virus infection, trojan, ransomware, phishing email, etc.)                          | Not Applicable              |
| Cyber situational awareness Level | CS1     | I am familiar with the term of "cyber security threats".   | [1], [29], [30], [31], [32] |
|                                   | CS2     | I know cyber security threats. (Like password attacks, email phishing, social phishing, malware, ransomware, etc).                               |                             |
|                                   | CS3     | I am aware that my company has set up strategies to manage and mitigate cyber security risks.  |                             |
|                                   | CS4     | I use a strong password for any account setup. (Minimum of 8 characters combined with number, alphabet, and symbol).                             |                             |
|                                   | CS5     | I do review the privacy setting in my social media account periodically.   |                             |
|                                   | CS6     | I do not discuss business-related information on social media. (Like Facebook, Instagram, WhatsApp, etc).  |                             |
|                                   | CS7     | I only browse the internet or download files from websites I know are secure and trustworthy.  |                             |
|                                   | CS8     | I know how to identify phishing emails.  |                             |
|                                   | CS9     | I will make sure the antivirus software in my computer is always up to date.   |                             |
|                                   | CS10    | I will make sure my computer is constantly updated with the latest security patches.   |                             |
|                                   | CS11    | I usually validate the links or respond to requests sent to my mobile apps with the sender before opening them. (Like SMS, WhatsApp, or WeChat). |                             |
|                                   | CS12    | I will back up my work data periodically.  |                             |
|                                   | CS13    | I understand the cyber security policy and guidance in my company.   |                             |
|                                   | CS14    | I will engage with experts to manage cyber security-related matters.   |                             |
|                                   | CS15    | It is important to implement information security standards within the company.  |                             |

A total of 490 respondents were collected, dataset went through data cleaning technique eliminate the problematic data that could lead to data accuracy and validity in this study. Data cleaning eliminated 47 records, and a balance of 443 records were used for data analysis. The study used IBM SPSS tool to conduct the frequency analysis, descriptive analysis, independent-sample t-tests, and One-Way ANOVA, to provide a robust analysis of the data collected and support the validity of the research.

#### 4. EXPERIMENTAL RESULTS AND DISCUSSIONS

##### 4.1 Descriptive Statistic for Respondent's Profiles

A high number of respondents working in the organization were classified as cyber security-abandoned and unskilled SMEs, 63%, while the remaining 37% were with the organization and had cyber security expertise and capability in managing the cyber threat defense. This revealed high concerns and prevalent challenges for the SME segment in Malaysia. Females slightly outnumbered males, constituting 55.5% of the sample compared to males. In terms of age, the highest percentage (40.60%) fell in the below-29-year-old (<29) category, indicative of a younger workforce in the study. There were people with a variety of educational backgrounds; the majority (46.70%) had a degree, then those with less than a degree (36.60%), and finally, postgraduates (16.70%). Career levels were relatively balanced, with "Junior Executive" (40.60%) being the most common, reflecting a diverse organizational hierarchy among respondents. Regarding working experience, a significant proportion (28.70%) had less than five years, indicating a combination of entry-level and seasoned professionals. Lastly, significantly, about half of the participants (51.50%) indicated that they had encountered cyber-attacks, underscoring the widespread occurrence and significance of cyber security risks. Details of respondent's profiles refer to Table 2.

Table 2. Respondent's Profiles

| Variable                  | Category  | Frequency (N=443) | %      |
|---------------------------|---|-------------------|--------|
| SME Cybersecurity classes | Cybersecurity Abandoned and Unskilled SMEs                | 279               | 63.00% |
|                           | Cybersecurity Expert-connected, Capable and Provider SMEs | 164               | 37.00% |
| Gender                    | Male  | 197               | 44.50% |
|                           | Female  | 246               | 55.50% |
| Age                       | <29   | 180               | 40.60% |
|                           | 30~39   | 100               | 22.60% |
|                           | 40~49   | 109               | 24.60% |
|                           | >= 50   | 54                | 12.20% |
| Education Level           | Less than Degree  | 162               | 36.60% |
|                           | Degree  | 207               | 46.70% |
|                           | Postgraduate  | 74                | 16.70% |

| Variable                 | Category                 | Frequency (N=443) | %      |
|--------------------------|--------------------------|-------------------|--------|
| Career Level             | Junior Executive         | 180               | 40.60% |
|                          | Senior Executive         | 140               | 31.60% |
|                          | Manager                  | 61                | 13.80% |
|                          | Senior Manager and Above | 62                | 14.00% |
| Working Experience       | <5 Years                 | 127               | 28.70% |
|                          | 5~9 Years                | 89                | 20.10% |
|                          | 10~19 Years              | 94                | 21.20% |
|                          | 20~29 Years              | 99                | 22.30% |
|                          | >=30 Years               | 34                | 7.70%  |
| Cyber-attacks Experience | No                       | 215               | 48.50% |
|                          | Yes                      | 228               | 51.50% |

#### 4.2 Analysis of Finding of Cyber Situational Awareness Level

The study focuses on assessing the CSA level of respondents within the study group. The primary objective focuses on understanding their knowledge, readiness and ability to handle potential cyber threats effectively. Following Kruger and Kearney's prototype for evaluating information security awareness [33], the respondents are classified into three groups based on their percentage results following below Table 3.

Table 3. Information Security Awareness Level [33]

| Awareness | Measurement (%) |
|-----------|-----------------|
| Good      | 80–100          |
| Average   | 60–79           |
| Poor      | 59 and less     |

This classification system evaluates participants' performance, aiding in recognizing strengths and areas needing enhancement. By referring to Table 4.10, scoring between 80% and 100% indicates a "Good" understanding level, demonstrating high proficiency in cyber situational awareness; scoring ranging from 60% to 79% will be in the "Average" category, indicating moderate proficiency. Conversely, 59% and below label participants as "Poor", highlighting areas for improvement needed for cyber security awareness or training. This classification system evaluates participants' performance, aiding in recognizing strengths and areas needing enhancement.

Table 4 below presents the CSA level of the respondents. The results show that 42% of respondents are in the "Poor" category, 18.30% fall under the "Average" category, and only 39.70% are categorized as "Good".

Table 4. Cyber Situational Awareness Level Analysis

| Cyber situational awareness | N   | Percentage (%) |
|-----------------------------|-----|----------------|
| Poor                        | 186 | 42.00          |
| Average                     | 81  | 18.30          |
| Good                        | 176 | 39.70          |

#### 4.3 Descriptive Exploration Analysis

The descriptive exploration analysis provides insight into how the respondents in this study understand the threats from cyberspace and if they know the necessary cyber protection and controls and understand the needs of adherence the best practices [1]. Table 5 explores numerical analysis in measuring the CSA level of the respondents.

Table 5. Cyber Situational awareness Level

| Cyber situational awareness   | Questions | Yes    | No     | Partial |
|---|-----------|--------|--------|---------|
| Awareness of Cyber security Threats                                   | C1        | 41.50% | 12.20% | 46.30%  |
|   | C2        | 47.90% | 12.60% | 39.50%  |
|   | C3        | 43.60% | 20.10% | 36.30%  |
| Awareness of Cyber security Protection and Controls                   | C4        | 65.20% | 9.50%  | 25.30%  |
|   | C5        | 36.10% | 28.40% | 35.40%  |
|   | C6        | 51.90% | 16.00% | 32.10%  |
|   | C7        | 56.00% | 13.30% | 30.70%  |
|   | C8        | 37.50% | 20.50% | 42.00%  |
|   | C9        | 41.50% | 19.40% | 39.10%  |
|   | C10       | 41.30% | 18.70% | 40.00%  |
|   | C11       | 51.90% | 18.50% | 29.60%  |
|   | C12       | 45.40% | 18.50% | 36.10%  |
| Awareness of the needs to implement the cyber security best practices | C13       | 43.80% | 19.60% | 36.60%  |



| Cyber situational awareness | Questions | Yes    | No     | Partial |
|-----------------------------|-----------|--------|--------|---------|
|                             | C14       | 47.40% | 20.50% | 32.10%  |
|                             | C15       | 62.10% | 12.20% | 25.70%  |

Regarding awareness of cyber security threats, 41.50% claim familiarity with the terminology, and 47.90% indicated knowing the general terms of cyber security threats such as password attacks, email phishing, social phishing, malware, and ransomware. Moreover, there needs to elevate awareness of the organization's strategies in fighting cyber threats, with only 43.60% acknowledging awareness of these strategies. This disparity could point to areas for improvement in how information on cyber security measures is shared within the organization.

Shifting the focus to the aspect that deals with knowledge about cyber security protection and controls, the analysis shows an optimistic scenario where a majority of 65.20% reported using solid passwords, showing a basic level of cyber security practice. On the other hand, following practices like regularly checking privacy settings on social media and the ability to identify phishing emails reflect lower compliance rates at 36.10% and 37.50%. Other cyber security practices, such as ensuring that antivirus and computers are constantly updated to the latest security patches, indicate lower compliance rates, at 41.50% and 41.30%, respectively. These numbers suggested that there might be a need for more attention to cyber security awareness among employees. 51.90% of respondents do not discuss business-related information over social media channels, and 56% indicated they will only browse the internet or download files from trustworthy websites.

The third aspect delves into awareness of the importance of establishing cyber security practices. A majority of 62.10% agreed on the nature of implementing information security protocols within their workplace. However, the actual implementation of this understanding varies regarding steps such as data backups and seeking advice from cyber security professionals, as responses show a range of opinions.

This analysis highlights the need for enhanced cyber security training and more precise communication strategies to instill a uniform culture of cyber security within the organization. It also indicates an opportunity for further research to understand why employees are aware of the inconsistent application of cyber security knowledge.

#### 4.4 Discussion

The study indicated a varying level of cyber situational awareness among the employees of SMEs in Malaysia. It demonstrated that only 39.70% of respondents equipped with adequate understanding of cyber security threats, which showed that the understanding of the application of cyber security protection and controls. The results are consistent with the indirect cybersecurity awareness studies conducted by Mammadov et al. [14] and Zulkifli et al. [15], which indicated that the cyber situational awareness of individuals is concerning. This highlights the need for interventions, such as targeted cyber security training, to enhance their situational awareness and improve their protective behavior. The findings also revealed that there is a lack of ability from employees in handling potential cyber threats. This is in line with the literature reviews indicating that most of the cyber security training and education are focused on large organizations [12], and small businesses may not receive adequate cyber security education and awareness compared to other organizations. SMEs do not implement cyber security measure effectively due to lack of financial support, tools, and expertise, which contribute a lower cyber situational awareness among the employees in SMEs [24], [34], [35], [36].

The awareness of cyber threats highlighted the critical improvement area required by SMEs, as less than half of the respondents demonstrated adequate awareness of cyber security threats; only 41.50% indicated they are familiar with the common terminology of cyber security threats (CS1), 47.90% recognized the cyber security threats (CS2), and 43.60% of them are aware of the mitigation strategy for combating cyber threats in the organization (CS3). This disparity suggested an opportunity to enhance communication in how information about cyber security threats and mitigation strategies is shared and understood within the organization to strengthen the overall cyber security posture.

Alshaikh supported the notion that enhanced communication through collaboration between internal and external parties can be further facilitated to improve cyber security awareness among employees [37].

In terms of cyber security practices and controls, the analysis showed an optimistic scenario for secure passwords, with 65.20% of them using the strong password (CS4). However, there were notable shortfalls in other controls such as privacy control for social media accounts whereby only 36.10% of respondents will review their policy setting in social media account periodically (CS5), and only 37.50% of them can reliably identify phishing emails (CS8). There was an increase in social engineering-based cyberattacks during the COVID-19 pandemic, as reported in the Hijji and Alam [38]. The lack of social media privacy control among the employees highlighted concerns about data privacy breaches and identity theft. SME is using social media for various aspects of business, including marketing and customer relationship management [39], driving the growth of online advertising, and acquiring new customers in the digital age [27]. It is crucial for SMEs to prioritize cyber security training to educate employees on how to implement secure social media privacy controls to protect both their data and customer information in the digital world.

A recent study indicated the impact of email phishing on businesses and leads to significant concern for SMEs [25]. Phishing scams will cause both financial loss and operational damage[29]. SMEs can adopt effective strategies such as having regular training sessions to educate employees about the signs of email phishing [38], using an advance phishing alert warning system to provide visual alerts and warnings by triggering the attention of employees from opening the potential email [40], conducting regular assessments, and employing simulated phishing attacks to ensure employees are well-trained in recognizing phishing attacks and keeping employees vigilant which can be incorporated as part of their training [38].

This study further revealed that employees' general information about cyber security practices. For instance, only 41.50% of respondents were keeping their computer antivirus up to date (CS9), and 41.30% of them consistently updated the security patches (CS10). The neglect of regular antivirus updates and software security patches poses a significant risk to business security and can leave companies vulnerable to cyberattacks which can lead to financial loss and business reputation damage. Li et al. suggested that when employees increase their self-efficacy, it will lead to better cyber protection behavior and effective engagement in cyber security practices [10]. Hence, SMEs should invest in educating their employees about the importance of cyber security, improving their knowledge and skills, and encouraging employees to implement cyber security practices to stay vigilant against cyber threats.

Sixty-two point one per cent of respondents agreed on the importance of establishing information security policies at their organization (CS15). However, the study revealed that the actual implementation of cyber security practices reflected a variety of perspectives. For instance, only 43.80% of respondents understand the cyber security policy and guidance in their organization (CS13) whereby 47.40% will engage with cyber security experts to manage cyber security-related matters (CS14). Employees understood the need to implement information security standards within the organization but failed to comply due to a variety of factors, such as perceived inconvenience, lack of motivation, and often forgetting to comply with the policies in their daily jobs [37]. The findings aligned with the predictive behavior following Endsley's SA theory whereby if the awareness of company cyber security policies and guidance is low, individuals do not take effective protective actions to prevent cyber threats. This had indicated why improving awareness of employees is critical to motivate employees' cyber protective behavior. Mou et al. suggested that culture plays an important role in cultivating cyber security protection behavior within the organization [41]. SMEs should set forth to create a strong culture of cyber security awareness and compliance and prioritize cyber security as part of the organization's culture to improve overall employee engagement and motivation in dealing with cyber threats.

## 5. CONCLUSION

In summary, this study had explored the CSA level among the employees of SMEs in Malaysia. This research is significant as it addresses gaps identified in studies related to cyber situational awareness and individuals' ability to recognize potential cyber threats especially in the context of SMEs, and there is a need to understand how to improve the individual's cyber protection behavior in cyber space [1]. Studies have revealed that employees of SMEs had limited awareness of cyber situations and possessed little skills and ability to engage with cyber threats. Hence, it is vital to establish training initiatives that not only enhance cyber awareness but also provide them with practical tools and upskilling resources to support organization effort in defending against cyber threats [42]. Besides, the study also revealed that 51.5% of the employees that experienced cyber-attacks, highlighting the SMEs are still primary target of cyberattacks. By understanding the cyber threat landscape and implementing targeted cyber security protection

measures and control will help SMEs better prepare themselves in facing the cyber threats. By addressing these requirements and hurdles, SMEs could better equip their workforce to recognize and handle cyber risks, ultimately fortifying their overall cyber security measures. This research is one of the very few studies to explore the CSA level among employees of SMEs in Malaysia. The result provides a good understanding about the awareness of employees of SMEs in cyberspace and helps to establish a baseline for future research in relevant domains.

From a theoretical implication, Endsley's model focused on the perception of elements within the environment, comprehension of their meaning, and projection of their future status. Extending Mica Endsley's situation awareness theory (SA) provided a crucial dimension to understanding how employees perceived and interpreted their environment in relation to cyber threats. The extension highlighted the cognitive processes behind cyber security awareness and decision-making. Investigating the cognitive processes behind the situation shed light on the elements that affected employees' ability to identify, understand, and eventually correctly react to cyber security risks. This study extended Endsley's theory of SA to present a model of SMEs' CSA and the extent to which factors prompted the execution of cyber security implementation. The SA research within a specific context frequently resulted in advancements; in general, increased awareness resulted in improved decision-making. From the perspective of policy implications, the study indicated that SMEs need to establish cybersecurity policies to enhance their overall security stance and boost employee readiness and proactive behavior. It is crucial for SMEs to institute formal security guidelines that specify how to safeguard sensitive information, address security breaches effectively, and continually revise security protocols. These cybersecurity policies should mandate a training and awareness program, detail a cyber incident response strategy, implement a cyber risk management framework, and develop comprehensive best practices for all operational activities vulnerable to cyber threats, such as email usage, social media interactions, computer and mobile device handling, and the protection and privacy of data. By crafting robust security policies and established effective communication about cyber situation and mitigation strategies within organization will strengthen individuals' protective behavior thus fostering SMEs cyber resilience.

Despite its contributions, this study has several limitations such as using a non-probability convenient sampling method and narrow focus on employees' viewpoints may overlook the role of management level. Besides, study used the quantitative method may overlook the subjective aspect of human experience. Future research is required by using alternative sampling strategies such as stratified sampling, comprehensive sampling differentiate by SME sector for focus group study, using mixed quantitative and qualitative methods to incorporate management and leadership viewpoints to understand their influence on cybersecurity culture.

Considering the cyber risks faced by SMEs, this research not only adds to the conversation about practical cyber security measures but also provides actionable recommendations. It laid the groundwork for crafting efficient approaches to boost motivation and actions for employees' safe cyber protection behavior, thereby aiding in the endurance and prosperity of SMEs in today's era. The ramifications of this study went beyond academia, providing hands-on advice for SMEs, policymakers, and cyber security experts aiming to strengthen the security of this sector of the economy.

## **ACKNOWLEDGEMENT**

The authors would also like to thank the participants who have provided their valuable insights and necessary data in this study. Additionally, to Unitar International University for offering the necessary knowledge and platform management support that made this study completed.

## **FUNDING STATEMENT**

The authors received no funding from any party for the research and publication of this article.

## **AUTHOR CONTRIBUTIONS**

Tan Chee Keong: Conceptualization, Data Curation, Methodology, Validation, Writing – Original Draft Preparation.  
Sofiah Kadar Khan: Administration, Supervision, Writing – Review & Editing.  
Umar Farooq Khattak: Project Administration, Supervision, Writing – Review & Editing.

## CONFLICT OF INTERESTS

No conflict of interests was disclosed.

## ETHICS STATEMENTS

The online survey questionnaire was designed to comprehensively assess the relationship among the variables. The research consists of four sections tailored explicitly for different research objectives. There was a data privacy consent included to inform the participants that the study took their privacy information seriously and assured that any data collected would not contain any personally identifiable information (PII) and would be used solely for academic research purposes. Refer below the consent show before the questionnaire starts:

“We take your privacy seriously and want to assure you that any data collected in this survey will be handled with the utmost care and confidentiality. The data collected does not contain any Personally Identifiable Information (PII) and will be used solely for academic research purposes. Once the research is completed, all data collected will be securely disposed of to ensure that your information remains protected. We are committed to maintaining the confidentiality and privacy of all participants involved in this survey.

If you have any questions or concerns regarding the privacy of your data, please don't hesitate to reach out to us.

Thank you for your participation and trust.

cktan981212@gmail.com”




## REFERENCES

- [1] K. Renaud and J. Ophoff, “A cyber situational awareness model to predict the implementation of cyber security controls and precautions by SMEs,” *Organizational Cybersecurity Journal: Practice, Process and People*, vol. 1, no. 1, pp. 24–46, Oct. 2021, doi: 10.1108/ocj-03-2021-0004.
- [2] Accenture, “How aligning security and the business creates cyber resilience State of Cybersecurity Resilience 2021,” 2021.
- [3] K. Gurchiek, “Lack of Awareness, Poor Security Practices Pose Cyber Risks,” *SHRM*, Jul. 2019, [Online]. Available: <https://www.shrm.org/resourcesandtools/hr-topics/technology/pages/lack-of-awareness-poor-security-practices-pose-cyber-risks.aspx>
- [4] Intrusion, “Cybercrime to cost the world 10.5 trillion annually by 2025,” *GlobeNewswire Newsroom*, Nov. 2020, [Online]. Available: <https://www.globenewswire.com/news-release/2020/11/18/2129432/0/en/Cybercrime-To-Cost-The-World-10-5-Trillion-Annually-By-2025.html>
- [5] S. Morgan, “Cybercrime To Cost The World \$10.5 Trillion Annually By 2025.” [Online]. Available: <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>
- [6] G. Lloyd, “The business benefits of cyber security for SMEs,” *Computer Fraud and Security*, no. 2020(2), pp. 14–17, 2020, doi: [https://doi.org/10.1016/S1361-3723\(20\)30019-1](https://doi.org/10.1016/S1361-3723(20)30019-1).
- [7] The MDEC Team, “SME Data Driven Playbook 2022.” [Online]. Available: <https://mdec.my/wp-content/uploads/2022/09/SME-Data-Driven-Playbook-MDEC-1.pdf>
- [8] V. Gomes, “Catalysing Malaysia’s digital economy,” *The Edge Markets*, Sep. 2022, [Online]. Available: <https://www.theedgemarkets.com/article/catalysing-malysias-digital-economy>
- [9] L. Yin Xia, A. H. Nor Aziati, A. Hamid Ahmad, and S. Seah, “The Factors and Challenges affecting Digital Economy in Malaysia,” 2021. [Online]. Available: <https://www.researchgate.net/publication/352118174>

- [10] L. Li, L. Xu, and W. He, "The effects of antecedents and mediating factors on cybersecurity protection behavior," *Computers in Human Behavior Reports*, vol. 5, Mar. 2022, doi: 10.1016/j.chbr.2021.100165.
- [11] M. Antunes, M. Maximiano, R. Gomes, and D. Pinto, "Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal," *Journal of Cybersecurity and Privacy*, vol. 1, no. 2, pp. 219–238, Jun. 2021, doi: 10.3390/jcp1020012.
- [12] A. Shojafar and H. Järvinen, "Classifying SMEs for Approaching Cybersecurity Competence and Awareness," in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Aug. 2021. doi: 10.1145/3465481.3469200.
- [13] Y. H.-S. Kam, K. Jones, R. Rawlinson-Smith, and K. Tam, "In Search of Suitable Methods for Cost-Benefit Analysis of Cyber Risk Mitigation in Offshore Wind: A Survey," *Journal of Informatics and Web Engineering*, vol. 3, no. 3, pp. 314–328, Oct. 2024, doi: 10.33093/jiwe.2024.3.3.20.
- [14] T. Mammadov, N. Abdul Rahman, M. Farhan Mohd Rahimi, C. Gov Azerbaijan, and C. Malaysia Kuala Lumpur, "Establishment of a Method to Measure the Awareness of OIC-CERT Members," *Journal of Cyber Security*, vol. 3, no. 1, 2021.
- [15] Z. Zulkifli, N. Nuha, A. Molok, N. Hayani, A. Rahim, and S. Talib, "CYBER SECURITY AWARENESS AMONG SECONDARY SCHOOL STUDENTS IN MALAYSIA," 2020.
- [16] M. R. Endsley, "Toward a theory of situation awareness in dynamic systems," *Hum Factors*, vol. 37, pp. 32–64, 1985.
- [17] M. R. Endsley, "A taxonomy of situation awareness errors," *Human Factors in Aviation Operations*, vol. 3, no. 2, pp. 287–292, 1995.
- [18] N. Walshe *et al.*, "Situation awareness and the mitigation of risk associated with patient deterioration: A meta-narrative review of theories and models and their relevance to nursing practice," Dec. 01, 2021, *Elsevier Ltd.* doi: 10.1016/j.ijnurstu.2021.104086.
- [19] R. Gutzwiller, J. Dykstra, and B. Payne, "Gaps and opportunities in situational awareness for cybersecurity," *Digital Threats: Research and Practice*, vol. 1, no. 3, Sep. 2020, doi: 10.1145/3384471.
- [20] F. Hoppe, N. Gatzert, and P. Gruner, "Cyber risk management in SMEs: insights from industry surveys," *Journal of Risk Finance*, vol. 22, no. 3–4, pp. 240–260, Nov. 2021, doi: 10.1108/JRF-02-2020-0024.
- [21] T. Gibbs, "Seeking economic cyber security: A Middle Eastern example," *Journal of Money Laundering Control*, vol. 23, no. 2, pp. 493–507, 2020, doi: 10.1108/jmlc-09-2019-0076.
- [22] E. Osborn and A. Simpson, "Risk and the Small-Scale Cyber Security Decision Making Dialogue - A UK Case Study," *Computer Journal*, vol. 61, no. 4, pp. 472–495, Apr. 2018, doi: 10.1093/comjnl/bxx093.
- [23] Robert Walters and Vacanysoft, "Cybersecurity-Building-Business-Resilience," 2020. Accessed: Dec. 20, 2024. [Online]. Available: <https://www.robertwalters.co.uk/content/dam/robert-walters/country/united-kingdom/files/whitepapers/Cybersecurity-Building-Business-Resilience.pdf>
- [24] N. C. Zainal, M. H. M. Puad, and N. F. M. Sani, "Moderating Effect of Self-Efficacy in the Relationship Between Knowledge, Attitude and Environment Behavior of Cybersecurity Awareness," *Asian Soc Sci*, vol. 18, no. 1, p. 55, Dec. 2021, doi: 10.5539/ass.v18n1p55.
- [25] U. D. Ani, H. He, and A. Tiwari, "Human factor security: evaluating the cybersecurity capacity of the industrial workforce," *Journal of Systems and Information Technology*, vol. 21, no. 1, pp. 2–35, Mar. 2019, doi: 10.1108/JSIT-02-2018-0028.
- [26] I. J. Ismail, "Entrepreneurial Start-up Motivations and Growth of Small and Medium Enterprises in Tanzania: The Role of Entrepreneur's Personality Traits," *FIIB Business Review*, vol. 11, no. 1, pp. 79–93, Mar. 2022, doi: 10.1177/23197145211068599.

- [27] J. F. Hair, M. Page, and N. Brunsveld, "Essentials of business research methods," 2020.
- [28] L. Zhang-Kennedy and S. Chiasson, "A Systematic Review of Multimedia Tools for Cybersecurity Awareness and Education," Jan. 31, 2021, *Association for Computing Machinery*. doi: 10.1145/3427920.
- [29] M. A. Alqahtani, "Cybersecurity Awareness Based on Software and E-mail Security with Statistical Analysis," *Comput Intell Neurosci*, vol. 2022, 2022, doi: 10.1155/2022/6775980.
- [30] CyberSecurity Malaysia, "Information Security Guidelines Small & Medium Enterprises (SMEs) for," 2011. Accessed: Dec. 19, 2024. [Online]. Available: [https://www.cybersafe.my/pdf/guidelines/guideline\\_SME.pdf](https://www.cybersafe.my/pdf/guidelines/guideline_SME.pdf)
- [31] W. C. H. Hong, C. Y. Chi, J. Liu, Y. F. Zhang, V. N. L. Lei, and X. S. Xu, "The influence of social education level on cybersecurity awareness and behaviour: a comparative study of university students and working graduates," *Educ Inf Technol (Dordr)*, vol. 28, no. 1, pp. 439–470, Jan. 2023, doi: 10.1007/s10639-022-11121-5.
- [32] M. Zwilling, G. Klien, D. Lesjak, L. Wiecheteck, F. Cetin, and H. N. Basim, "Cyber Security Awareness, Knowledge and Behavior: A Comparative Study," *Journal of Computer Information Systems*, vol. 62, no. 1, pp. 82–97, 2022, doi: 10.1080/08874417.2020.1712269.
- [33] H. A. Kruger and W. D. Kearney, "A prototype for assessing information security awareness," *Comput Secur*, vol. 25, no. 4, pp. 289–296, Jun. 2006, doi: 10.1016/j.cose.2006.02.008.
- [34] S. Chaudhary and V. Gkioulos, "SME Cybersecurity Awareness Program 1", 2020.
- [35] P. S. Ulrich, A. Timmermann, and V. Frank, "Organizational aspects of cybersecurity in German family firms – Do opportunities or risks predominate?," *Organizational Cybersecurity Journal: Practice, Process and People*, vol. 2, no. 1, pp. 21–40, Apr. 2022, doi: 10.1108/ocj-03-2021-0010.
- [36] H. Zwarts, J. Du Toit, and B. Von Solms, "A Cyber-Diplomacy and Cybersecurity Awareness Framework (CDAF) for Developing Countries," in *European Conference on Cyber Warfare and Security*, 2022.
- [37] M. Alshaikh, "Developing cybersecurity culture to influence employee behavior: A practice perspective," *Comput Secur*, vol. 98, Nov. 2020, doi: 10.1016/j.cose.2020.102003.
- [38] M. Hijji and G. Alam, "Cybersecurity Awareness and Training (CAT) Framework for Remote Working Employees," *Sensors*, vol. 22, no. 22, Nov. 2022, doi: 10.3390/s22228663.
- [39] O. Uvarova, "SMEs digital transformation in the EaP countries during COVID-19," 2021. [Online]. Available: <https://eap-csf.eu/wp-content/uploads/SMEs-digital-transformation-in-the-EaP-countries-during-COVID-19.pdf>
- [40] M. Cooper, Y. Levy, L. Wang, and L. Dringus, "Heads-up! An alert and warning system for phishing emails," *Organizational Cybersecurity Journal: Practice, Process and People*, vol. 1, no. 1, pp. 47–68, Oct. 2021, doi: 10.1108/ocj-03-2021-0006.
- [41] J. Mou, J. Cohen, A. Bhattacharjee, and J. Kim, "A Test of Protection Motivation Theory in the Information Security Literature: A Meta-Analytic Structural Equation Modeling Approach," *J Assoc Inf Syst*, vol. 23, no. 1, pp. 196–236, 2022, doi: 10.17705/1jais.00723.
- [42] T. Munusamy and T. Khodadi, "Building Cyber Resilience: Key Factors for Enhancing Organizational Cyber Security," *Journal of Informatics and Web Engineering*, vol. 2, no. 2, pp. 59–71, Sep. 2023, doi: 10.33093/jiwe.2023.2.2.5.

**BIOGRAPHIES OF AUTHORS**

|   |   |
|---|---|
|    | <p><b>Tan Chee Keong</b> is a Doctoral Business administration (DBA) candidate from Unitar International University. His research focuses on cyber situational awareness and the cyber protection behaviors of employees in Malaysia's SMEs. He has more than 20 years working experience in Information System, encompassed telecommunication (wired and wireless), data center operation, private and public cloud architect solution. He is currently affiliated with an MNC focusing on cloud platform business and cybersecurity operations. He can be contacted at the following email: unu2200704@student.unitar.my/cktan981212@gmail.com.</p> |
|    | <p><b>Sofiah Kadar Khan</b> is a senior lecturer from Unitar International University. Her research focuses on the study related to management: Leadership and Team Building and Organization Behavior. She had presented in several conferences including the 4<sup>th</sup> Regional Conference on Campus Sustainability, and 3<sup>rd</sup> International Conference on Business, Accounting, Finance and Economics (BAFE 2016). She can be contacted at the following email: sofiah.khan@unitar.my.</p>   |
|  | <p><b>Umar Farooq Khattak</b> is a senior lecturer and programmer leader (Postgraduate) from Unitar International University. He has over nine years experiences as a computer lecturer with different institutes. He can be contacted at the following email: umar.farooq@unitar.my.</p>   |
|   |   |