Implementation of Cybersecurity Situation Awareness Model in Saudi SMEs

Monerah Faisal Almoaigel, Ali Abuabid
Informa Technology Department, College of Computing and Informatics, Saudi Electronic University, Riyadh, Saudi Arabia

***Abstract*—Saudi Small and Medium-sized Enterprises (SMEs) are witnessing rapid growth in technology and innovation. However, this growth is accompanied by increased cybersecurity threats, which pose significant challenges for SMEs. Cyber threats are becoming more complex and sophisticated, with SMEs becoming prime targets due to their weaker cybersecurity defenses. Hence, there exists a rich literature on critical challenges facing SMEs. Existing literature on these challenges addresses many research issues (e.g., finance, technology adoption, and management) associated with SMEs. However, one critical issue that has so far received no rigorous attention is cybersecurity situation awareness for research in the SME context. Thus, this study used a quantitative approach aiming to empirically test a model of cybersecurity situational awareness that can support SMEs in Saudi Arabia to implement cybersecurity measures and precautions with efficacy. An online survey of 350 participants was conducted to collect the research data. The study identified a significant positive relationship between Cyber Situational Awareness (Csa) and Implementation of Cybersecurity Controls (Icsc), suggesting that enhancing awareness can contribute to better control implementation. The study identified a significant positive relationship between Cyber Situational Awareness (Csa) and Implementation of Cybersecurity Controls (Icsc), suggesting that enhancing awareness can contribute to better control implementation. Finally, the paper provides several interesting findings and outlines future research directions.**

Keywords*—*Cyber situation awareness; cybersecurity control and precaution; Saudi; SMEs

I. Introduction

The Kingdom of Saudi Arabia is rapidly growing in technology and innovation, with Small and Medium-sized Enterprises (SMEs) playing a significant role in this growth. However, this growth comes with increased cybersecurity threats, which pose significant challenges for SMEs. Cyber threats are growing in complexity and sophistication, and SMEs are becoming a primary target for cyber attackers due to their weaker cybersecurity posture. Therefore, SMEs might adopt a robust cybersecurity strategy that includes cyber situation awareness (CSA) to combat cyber threats effectively. SMEs are increasingly becoming targets for cyber attackers. SMEs in the UK alone are targeted by cyber-attacks more than seven million times yearly [1]. Similarly, in Saudi Arabia, a study by [2] found that SMEs were particularly vulnerable to cyber-attacks due to their limited resources and expertise.

One of the main reasons for the high rate of cyber-attacks on SMEs is their perceived vulnerability. Hackers often assume that SMEs have weaker security measures than larger organizations, making it easier to attack targets [3]. Furthermore, SMEs often lack the resources to invest in advanced cybersecurity technologies and hire dedicated staff [2]. As a result, they may be more susceptible to common attacks such as phishing, ransomware, and social engineering.

Cyber-attacks' impact on SMEs can be significant regarding financial losses and reputational damage. A study by [4] found that SMEs in the Netherlands lost an average of £65,000 per cyber-attack. Furthermore, the reputational damage caused by a cyber-attack can be particularly damaging for SMEs, as they may struggle to regain the trust of their customers and partners.

Researchers have proposed various solutions to address these challenges to improve SMEs' cybersecurity posture. These include investing in essential security measures such as firewalls and antivirus software, implementing employee training programs to improve cybersecurity awareness, and developing incident response plans to ensure businesses are prepared to respond to cyber-attacks [5].

Despite the serious consequences of cyber-attacks, SMEs often lack the resources and expertise to implement effective cyber security measures. Therefore, there is a need for a cyber situational awareness model that can assist SMEs in Saudi Arabia to implement cyber security controls and precautions effectively. Thus, this study aims to empirically test a model of cybersecurity situational awareness that can support SMEs in Saudi Arabia to implement cybersecurity measures and precautions with efficacy. Specifically, this study aims to validate the proposed model using empirical data collected from SMEs in Saudi Arabia to ensure its applicability and usefulness in the local context.

Overall, this paper is expected to contribute by providing a practical and effective framework for SMEs in Saudi Arabia to implement cyber security measures, thereby reducing their vulnerability to cyber-attacks. In other words, the extension of Endsley's theory of situation awareness to the cyber security domain can contribute to developing a more comprehensive understanding of how situational awareness can be leveraged to enhance cyber security in SMEs.

The remainder of this paper offers a comprehensive analysis of related literature in Section II. Then, the research approach used in this paper is discussed in Section III and followed by the findings that are presented and discussed in Section IV. Finally, the paper ends by summarizing the key findings, contributions, limitations, and future work in Section V.

II. Literature Analysis

A. Cybersecurity Situation Awareness Model

Situational awareness is a term that originated in the field of aviation in the 1940s and refers to a pilot's ability to accurately understand their current situation and the potential risks and opportunities in the environment around them [6]. Over time, situational awareness has been applied to various fields, including military operations, cybersecurity, and emergency response [7]. In the context of cybersecurity, situational awareness refers to the ability of an organization or individual to understand the current state of their cyber environment, including potential threats and vulnerabilities, and to use this understanding to make informed decisions about how to protect their assets and respond to potential incidents [1].

A cyber situation awareness model is a framework or methodology designed to help organizations improve their situational awareness in the cybersecurity domain. Such a model typically includes a set of processes and tools that enable an organization to monitor its network infrastructure and collect and analyze data about potential threats and vulnerabilities. It makes informed decisions about responding to incidents or improving its security posture [8]. Many different cyber situational awareness models have been developed, each with strengths and weaknesses. Some models are designed for specific industries or organizational contexts, while others are more general. Some models rely heavily on automated tools and data analytics, while others emphasize human expertise and decision-making.

One of the most widely used frameworks in the field of cybersecurity is the Kill Chain framework, which was first introduced by Lockheed Martin in 2011 [9]. The Kill Chain framework is designed to help organizations understand the different stages of a cyber-attack, from initial reconnaissance to final data exfiltration, and to develop appropriate defenses at each stage. The cybersecurity industry has widely adopted many organizations' frameworks to guide their cybersecurity strategies.

Another framework that has gained traction is the Diamond Model, introduced in 2014 by a group from the US Army Research Laboratory [10]. The Diamond Model is based on the premise that cyber-attacks are dynamic. Understanding the relationship between an attacker, a victim, an infrastructure, and an impact helps organizations better understand the threats they face and develop appropriate defenses. The US government and other organizations have used the framework to improve their situational awareness and incident response capabilities [11].

Moreover, the Cyber Security Situation Awareness Framework (CSSAF) was developed by researchers from the University of Plymouth in the UK and is designed to help organizations improve their situational awareness by integrating data from multiple sources, including network traffic, system logs, and threat intelligence feeds [12]. Several organizations have used the CSSAF to improve their cybersecurity posture, and the framework effectively detects and mitigates cyber-attacks.

The MITRE ATT&CK framework is a relatively new situational awareness framework introduced in 2015 [13]. The framework is designed to help organizations understand the tactics, techniques, and procedures (TTPs) that attackers commonly use and to develop appropriate defenses based on this knowledge. Many organizations use the MITRE ATT&CK framework to guide their cybersecurity strategies [14]. The following section will detail the cyber situation awareness models for SMEs in Saudi Arabia.

B. Cybersecurity Situation Awareness Model and Saudi SMEs

Saudi SMEs are businesses with less than 250 employees and annual revenue of less than 200 million SAR [15]. SMEs play a critical role in the economy of Saudi Arabia. Moreover, SMEs represent about 99% of all businesses in the country and employ around two-thirds of the private sector workforce [16].

Despite their significant contribution to the economy, SMEs in Saudi Arabia face several challenges, including access to financing, limited access to skilled labor, and a complex regulatory environment [17]. These challenges can be particularly acute in cybersecurity, where SMEs often lack the resources and expertise to effectively protect themselves against cyber threats. One of the main reasons for the high rate of cyber-attacks on SMEs is their perceived vulnerability. Hackers often assume that SMEs have weaker security measures than larger organizations, making it easier to attack targets [3]. Furthermore, SMEs often lack the resources to invest in advanced cybersecurity technologies and hire dedicated cybersecurity staff [2]. As a result, they may be more susceptible to common attacks such as phishing, ransomware, and social engineering. Cyber-attacks' impact on SMEs can be significant regarding financial losses and reputational damage. The research in [4] found that SMEs lost an average of £65,000 per cyberattack. Furthermore, the reputational damage caused by a cyberattack can be particularly damaging for SMEs, as they may struggle to regain the trust of their customers and partners.

Several recent studies have examined SMEs' challenges and opportunities in Saudi Arabia. For instance, the study in [18] found that accessing finance was one of the most significant challenges facing SMEs in Saudi Arabia. With struggling to secure funding, SMEs needed to grow and expand. The study also identified a lack of skilled labor and bureaucratic red tape as significant obstacles to growth. In addition, the study in [2] found that many SMEs in Saudi Arabia were not adequately prepared to protect themselves against cyber threats. This study also highlighted that only 30% of Saudi SMEs had implemented cybersecurity controls or precautions. Among those that had, many were using outdated or ineffective approaches, such as antivirus software and firewalls.

To address these challenges, researchers (e.g., [19], [20], and [1]) have proposed a range of solutions aimed at improving the cybersecurity posture of SMEs. These include investing in essential security measures such as firewalls and antivirus software, implementing employee training programs to improve cybersecurity awareness, and developing incident response plans to ensure businesses are prepared to respond to cyberattacks. Overall, the high cyberattack rate on SMEs highlights these businesses' need for greater awareness and investment in cybersecurity measures. While there is no one-size-fits-all solution to these challenges, a proactive and comprehensive approach to cybersecurity can help SMEs mitigate the risks of cyberattacks and protect their businesses.

SMEs should adopt a robust cybersecurity strategy that includes cyber situation awareness (CSA) to combat cyber threats effectively and benefit from greater access to training and resources on cybersecurity best practices. For instance, [21] proposed a framework for improving cybersecurity awareness and education among SMEs. This might help to reduce the risk of cyberattacks and improve the overall security posture in Saudi SMEs.

Furthermore, the research in [22] proposed a model that includes the following components: data collection, data processing, threat identification, and response. They suggest that the model can be used to develop effective cybersecurity strategies for SMEs. Similarly, [23] proposed a cybersecurity awareness model that includes four components: data collection, data analysis, data dissemination, and response. The model can enhance cyber security control and precaution in SMEs.

To gain a comprehensive understanding of the actual cybersecurity practices in Saudi SMEs. The researchers use the proposed model by [1], an extension of Endsley’s situational awareness theory [6], to portray SMEs' cybersecurity situational awareness. Fig. 1 portrays the proposed SME cyber security situational awareness model.

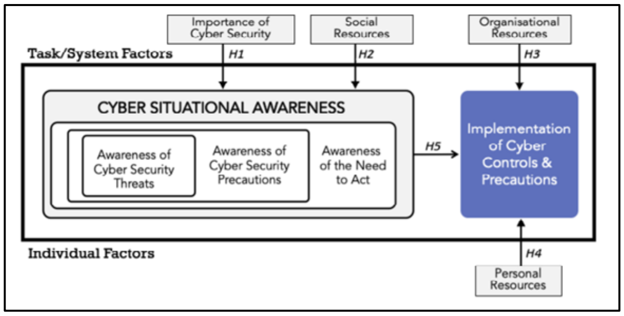

Importance of Cyber Security
Social Resources
Organisational Resources
Task/System Factors
H1
H2
H3
CYBER SITUATIONAL AWARENESS
Awareness of Cyber Security Threats
Awareness of Cyber Security Precautions
Awareness of the Need to Act
H5
Implementation of Cyber Controls & Precautions
Individual Factors
H4
Personal Resources

Fig. 1. Cyber security situational awareness in SMEs. (Karen et al., 2021).

The importance of cybersecurity helps SMEs administration understand that maintaining cyber security mechanisms enhances their business continuity. The availability of social resources enhances the awareness of SME administration about cybersecurity threats, precautions that should be applied to respond to these threats, and how they act accordingly. In contrast, the availability of organizational and personal resources facilitates the implementation of cyber controls and precautions. Table I summarizes the hypothesis that needs to be tested to validate the model.

- The first hypothesis (H1) suggests that the level of cyber situational awareness, which refers to understanding potential cybersecurity threats and vulnerabilities, is influenced by how much the SMEs understand the importance of cyber security in the context of Saudi SMEs [1]. This means that SMEs in Saudi Arabia are more likely to better understand potential cybersecurity threats and vulnerabilities if they recognize the importance of cybersecurity.
- The second hypothesis (H2) proposes that social resources influence the level of cyber situational awareness in Saudi SMEs [2] . This means that Saudi SMEs are more likely to be aware of potential cybersecurity threats and vulnerabilities if they access relevant social resources such as expert advice, training, or support from other SMEs.
- The third hypothesis (H3) contends that organizational resources influence the implementation of cyber security controls and precautions in Saudi SMEs [2]. This means that Saudi SMEs are more likely to implement cybersecurity controls and precautions effectively if they have the necessary organizational resources, such as funding, technology, and personnel.
- The fourth hypothesis (H4) presents that personal resources influence the implementation of cyber security controls and precautions in Saudi SMEs [1]. This means that individuals within Saudi SMEs are more likely to implement cybersecurity controls and precautions effectively if they have the necessary personal resources, such as technical skills and knowledge.
- The fifth hypothesis (H5) proposes that the level of cyber situational awareness influences the adoption of cyber security controls and precautions in Saudi SMEs [1]. This means that Saudi SMEs are more likely to adopt adequate cybersecurity controls and precautions to protect their information systems if they are aware of potential cybersecurity threats and vulnerabilities.

TABLE I. PROPOSED RESEARCH HYPOTHESIS

No.	Hypothesis Description
H1	The level of cyber situational awareness in SMEs is influenced by their understanding of the importance of cyber security.
H2	Their social resources influence the cyber situational awareness in SMEs.
H3	Implementing cyber security controls and precautions in SMEs is influenced by their organizational resources.
H4	Implementing cyber security controls and precautions in SMEs is influenced by their personal resources.
H5	Their level of cyber situational awareness influences the adoption of cyber security controls and precautions in SMEs.

III. RESEARCH APPROACH

This study used an online survey approach to understand SME perceptions of factors affecting cybersecurity situational awareness. An online survey was considered appropriate due to fast access to individuals, increased ability to reach difficult contact participants, and ease of having automated data collection, which reduced researchers' time and effort [24]. Furthermore, online surveys save researchers money due to the electronic data collection [25].

The study was conducted in the spirit of the positivist research tradition and followed four stages: literature analysis to develop the theoretical concepts, survey instrument development, administration of the survey, and empirical data analysis. The literature analysis identified a set of cybersecurity situational awareness factors. These served as the foundation for developing an initial survey instrument divided into four parts: profile of responding managers, characteristics of participating business, factors affecting cybersecurity situational awareness in SMEs, and implementation of cybersecurity controls and precautions.

The target online survey participants are SMEs in Saudi Arabia registered with the Small and Medium Enterprises General Authority (Monsha'at) (Small and Medium Enterprises General Authority, 2023). It develops several supporting programs and projects that advance a culture of self-employment, private enterprise, and innovation. It also provides funding sources and develops standards and policies for SMEs.

The online survey was sent (via email and SMEs' social media accounts) to the Saudi SMEs, and 350 responded to the online survey. The obtained low response was not a shock, [26] stated that online survey has often been plagued by low response.

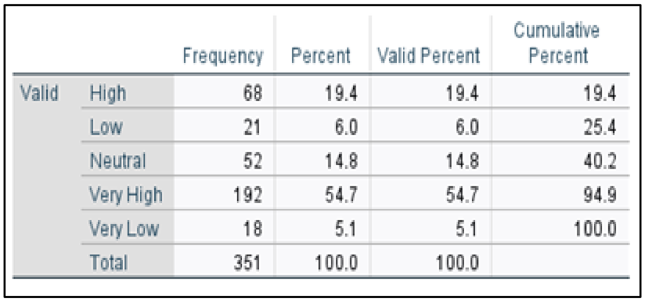
IV. Results and Discussion

A. Importance of Cyber Security (Ics)

The research aimed to assess the importance of cyber security for SMEs, and the participants were asked two items to gather insights into the importance of cyber security in their SMEs. The results revealed that 54.7% of the participants acknowledged that cybersecurity is critical to their business. In contrast, only 5.1% believed it to be of very low importance. Fig. 2 shows descriptive statistics of the importance of cybersecurity 1 (Ics1).

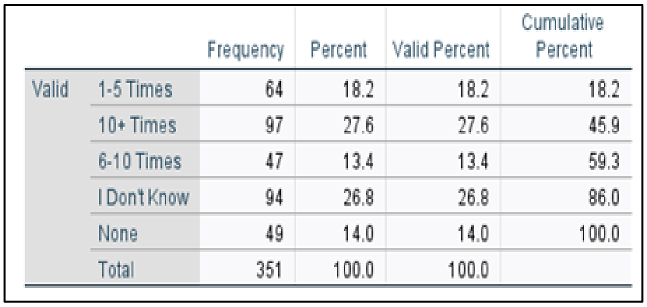
To further understand the participants' approach to recognizing cyber security risks that may affect their business, they were asked about the measures they had taken in the previous year. The responses were diverse, with most participants (a significant portion) indicating that their companies had implemented 10 or more measures to mitigate risks. The second-highest response came from participants who were unsure about the measures taken by their organization. Surprisingly, the lowest response came from participants who felt that none of the options provided were suitable, suggesting a lack of proactive measures. Fig. 3 shows the descriptive statistics of the importance of cybersecurity 2 (Ics2).

Upon analyzing these results, it became evident that participants who perceived their businesses to be at a very high risk of cyber security threats were more inclined to implement more measures to safeguard their operations. Conversely, those who considered the risk shallow exhibited either a lack of awareness regarding the measures taken or a complete absence of proactive actions. Interestingly, despite acknowledging a high risk, some participants did not appear concerned or motivated to take appropriate measures.



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	High	68	19.4	19.4	19.4
	Low	21	6.0	6.0	25.4
	Neutral	52	14.8	14.8	40.2
	Very High	192	54.7	54.7	94.9
	Very Low	18	5.1	5.1	100.0
	Total	351	100.0	100.0	

Fig. 2. Descriptive statistics of the importance of cybersecurity 1(Ics1).



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1-5 Times	64	18.2	18.2	18.2
	10+ Times	97	27.6	27.6	45.9
	6-10 Times	47	13.4	13.4	59.3
	I Don't Know	94	26.8	26.8	86.0
	None	49	14.0	14.0	100.0
	Total	351	100.0	100.0	

Fig. 3. Descriptive statistics of the importance of cybersecurity 2(Ics2).

These findings highlight the varying levels of awareness and response to cyber security risks among businesses. While some organizations take significant measures to protect their assets, others may not fully recognize the potential consequences or lack the necessary resources or knowledge to address these risks adequately. It emphasizes the importance of raising awareness, enhancing education, and promoting a proactive approach to cyber security across all businesses, regardless of their personal resource levels. Fig. 4 shows the correlation between Important of Cybersecurity (Ics1) and (Ics2).

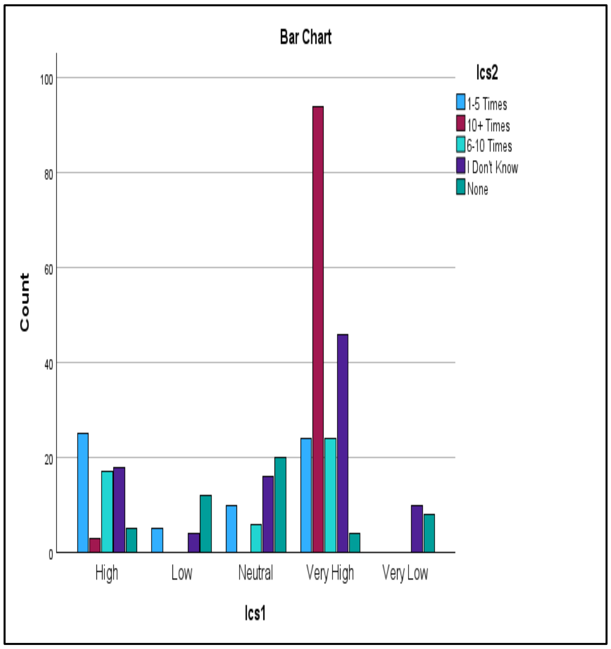


Fig. 4. Correlation between Importance of Cybersecurity (Ics1) and (Ics2).

B. Social Resources (Sr)

As part of the social analysis, the researchers formulated three items for the participants to gather insights into the perceptions surrounding cybersecurity practices in Saudi SMEs. The questions focused on competitor measures, customer data safety, and B2B suggestions regarding cyber security. The responses to these questions were consistent, with the highest number of participants strongly agreeing that cybersecurity practices are in high demand across all cases. This indicates a widespread recognition among participants that implementing robust cybersecurity measures is crucial in various aspects of business operations. Fig. 5 illustrates the correlation analysis of Social Resources (Sr1), (Sr2), and (Sr3).

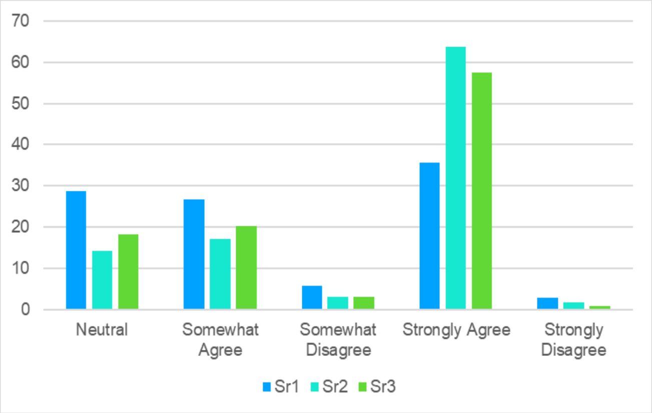


Fig. 5. Correlation analysis of social resources (Sr1), (Sr2) and (Sr3).

Firstly, when asked about their competitors' measures in implementing cybersecurity, many participants strongly agreed that such practices are highly sought after. This suggests that businesses in the same industry increasingly adopt cybersecurity measures to protect their valuable assets and sensitive information. Secondly, participants were asked about the safety of customer data. Once again, a considerable majority strongly agreed that ensuring customer data security is paramount. This underscores the growing awareness among businesses regarding the potential risks associated with data breaches and the need to safeguard customer information. Lastly, regarding B2B suggestions regarding cybersecurity aspects, participants strongly agreed that cybersecurity practices are in high demand. This indicates that Saudi SMEs engaging in B2B relationships are becoming more proactive in emphasizing the importance of cybersecurity and expecting their partners to implement robust measures to protect shared information and maintain a secure business environment.

Taken together, these findings paint a clear picture that in the context of Saudi SMEs, cyber security practices are highly regarded and in-demand from a social perspective. SMEs and their stakeholders recognize the significance of implementing effective security measures to mitigate the risks posed by cyber threats. This growing emphasis on cybersecurity highlights the need for continuous improvement and adaptation to address the evolving landscape of cyber threats in the SME’s environment.

C. Organizational Resources (Or)

To perform organizational analysis, the researchers devised four items to gain insights into participants' perspectives on cybersecurity within their respective organizations. These questions focused on organizational-provided cybersecurity information, information-seeking behaviors, agreement that SMEs struggle to manage all the advice provided, and the impact of on-air cybersecurity advice on their work. Upon analyzing the responses, varied opinions across all question designs within this category were observed. Most participants tended to provide responses leaning towards the Neutral or Somewhat Agree spectrum. This indicates a lack of strong agreement or certainty regarding the organizational perspectives on cybersecurity or the scenarios presented.

Firstly, participants were asked about the availability of cybersecurity information provided by their organizations. The responses varied, with many participants expressing neutrality or a somewhat agreeable stance. This suggests that the participants may not view the organizational provision of cybersecurity information as highly reliable or effective. Secondly, participants were asked about their information-seeking behaviors regarding cybersecurity. Once again, the responses tended towards a neutral or somewhat agreeable position. This implies that participants may not actively seek out additional cybersecurity information beyond what is provided by their organization, or they may feel uncertain about the effectiveness of their information-seeking efforts. Fig. 6 displays the correlation analysis of Organizational Resources (Or1), (Or2), (Or3) and (Or4).

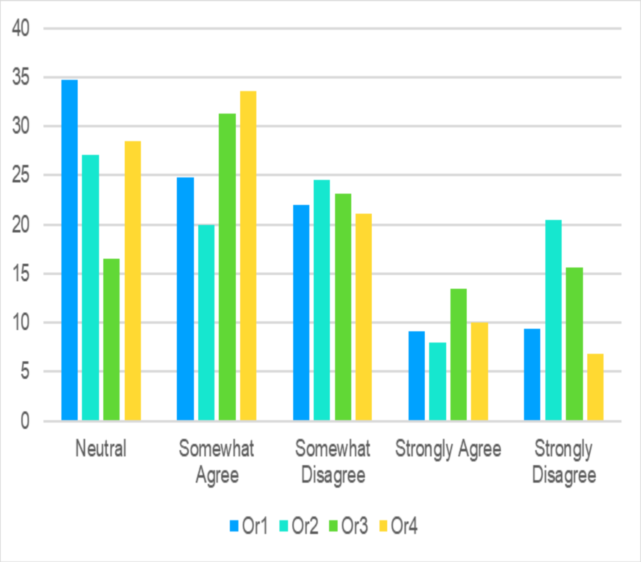


Fig. 6. Correlation analysis of organizational resources (Or1), (Or2), (Or3) and (Or4).

Furthermore, participants were presented with a statement regarding SMEs' ability to manage all the cybersecurity advice provided to them. The responses predominantly reflected a neutral or somewhat agreeable perspective. This suggests that participants may perceive SMEs to face challenges in effectively managing and implementing the abundance of cybersecurity advice available. Lastly, participants were asked about the impact of on-air cybersecurity advice on their work. The responses once again leaned towards a neutral or somewhat agreeable standpoint. This indicates that participants may find it difficult to assess the relevance or applicability of on-air cybersecurity advice to their specific organizational context, potentially making their work more challenging.

The analysis of these independent responses reveals a lack of solid agreement or certainty among participants regarding their organizational perspectives on cybersecurity. The prevalence of neutral or somewhat agreeable responses suggests that participants may harbor reservations or uncertainties about the effectiveness, relevance, or practicality of their organizations' cybersecurity measures and advice. This highlights the importance of addressing these concerns and fostering more precise communication and understanding between organizations and employees regarding cybersecurity practices.

D. *Personal Resources (Pr)*

In personal resource analysis, the researchers posed five items to participants regarding their personal abilities in handling, managing, or implementing cybersecurity measures on their own. Additionally, they were inquired about their perceptions of personal information safety. The responses from participants yielded various results, mirroring the findings from the analysis of organizational resources. In many cases, participants expressed a somewhat agreeable or disagreeable stance toward the statements, indicating a potential lack of knowledge or familiarity with cybersecurity. Most participants may possess limited understanding or proficiency in this area, while a minority group demonstrated strong knowledge and capability to handle unforeseen cybersecurity situations.

Firstly, participants were asked about their personal abilities in managing cybersecurity. The responses revealed a range of opinions, with many participants leaning towards a somewhat agreeable or disagreeable standpoint. This suggests that many participants may lack the necessary skills or knowledge to handle cybersecurity matters on their own effectively. Fig. 7 illustrates the correlation analysis of Personal resources (Pr1), (Pr2), (Pr3), (Pr4) and (Pr5).

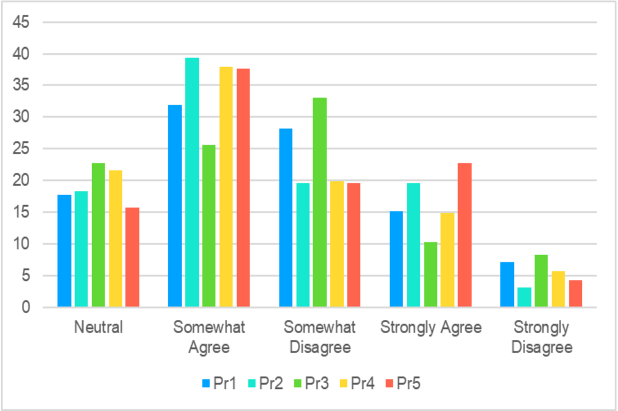


Fig. 7. Correlation analysis of personal resources (Pr1), (Pr2), (Pr3), (Pr4) and (Pr5).

Furthermore, participants were questioned about their personal information safety. The responses showcased a mixture of perspectives. Many participants tended to express a somewhat agreeable or disagreeable viewpoint, indicating that they may not have a strong confidence in the security of their personal information.

The analysis of these personal resource responses highlights a significant knowledge gap or lack of familiarity with cybersecurity practices among the participants. While a minority group demonstrated competence in handling cybersecurity matters, most appear to possess limited understanding or capability in this domain. This emphasizes the importance of raising awareness and providing education and resources to enhance individuals' personal cybersecurity skills and knowledge. We can collectively strengthen our overall cybersecurity posture by empowering individuals to protect their personal information better and effectively respond to cybersecurity threats.

E. *Implementation of Cyber Controls and Precautions (Icsc)*

To gain insight into the organizational setup, the researchers gathered information from the participants regarding the number of cybersecurity controls implemented by their SMEs and the extent to which their security policies covered various aspects. Upon analyzing the responses, the researchers observed a higher frequency of participants, indicating a lack of knowledge about these aspects. This suggests that many participants were unsure or unaware of the specific controls in place within their organizations. However, it is worth noting that the second and third most common responses indicated that their businesses had implemented between 1 and 5 controls and 10 or more controls, a positive indication of proactive security measures being taken. Fig. 8 displays the descriptive statistics of Implementing Cyber Controls and Precautions (Icsc1). Nevertheless, the fourth highest response rate was recorded for the option "none," implying that there may be certain aspects of cybersecurity that were overlooked or not adequately covered by our survey questions. This signifies a potential gap in assessing the participants' understanding of their organization's cybersecurity practices.

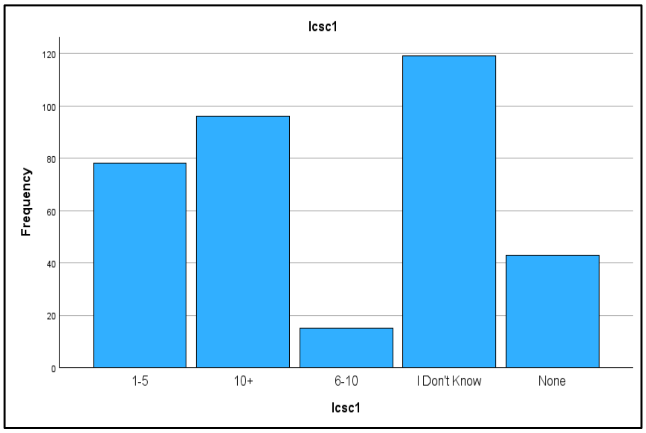


Fig. 8. Descriptive statistics of implementation of cyber controls and precautions (Icsc1).

It is crucial for the researchers to address this limitation and explore additional areas of concern that might have been missed in the initial survey design. Another significant finding is that most participants expressed a lack of awareness regarding their business's actions pertaining to cybersecurity. This highlights a concerning lack of knowledge or visibility among participants regarding the specific measures and initiatives their organizations undertake to mitigate cybersecurity risks. Fig. 9 shows the descriptive statistics of Implementing Cyber Controls and Precautions (Icsc2).

These findings underscore the importance of enhancing communication and awareness within organizations regarding cybersecurity practices. Providing employees with comprehensive information about the implemented controls is crucial, and ensuring they understand their roles and responsibilities in maintaining a secure environment is crucial.

Additionally, conducting more comprehensive assessments and addressing the areas of uncertainty can help organizations identify and rectify potential gaps in their cybersecurity strategies.

F. *Reflective Measurement Model*

In this research paper, the researchers analyzed several factors representing underlying factors presented in Table II. These factors include "Importance of Cybersecurity," "Social Resources," "Organizational Resources," "Personal Resources," and "Implementation of Cybersecurity Controls." The researchers also have a formative construct called "Cyber Situational Awareness."

To evaluate the reflective constructs, we examined the item loadings of their indicators. Item loadings indicate the strength of the relationship between each indicator and its respective factor.

Most of the item loadings were slightly below the recommended threshold of 0.708. (Hair Jr et al., 2021) suggested a relatively strong association between the indicators and their factors. However, five items, specifically Or2, Or3, Or4, Pr2, and Pr5, had item loadings below the threshold.

The researchers also assessed the internal consistency reliability of the reflective factors using composite reliability and Cronbach's alpha. Composite reliability values measure the reliability of the items in capturing the factors, while Cronbach's alpha estimates the internal consistency of the item set. Although most composite reliability values were below the satisfactory threshold of 0.70, none were problematically high (above 0.95) [27].

The researchers examined the average variance extracted (AVE) for each factor to evaluate convergent validity. AVE represents the proportion of variance in the items explained by the factor. Three factors had AVE values above the acceptable threshold of 0.50, indicating that they explain significant variance in the items [28]. However, "Organizational Resources" and "Personal Resources" had AVE values below 0.50, suggesting that they explain a relatively smaller proportion of variance in their items.

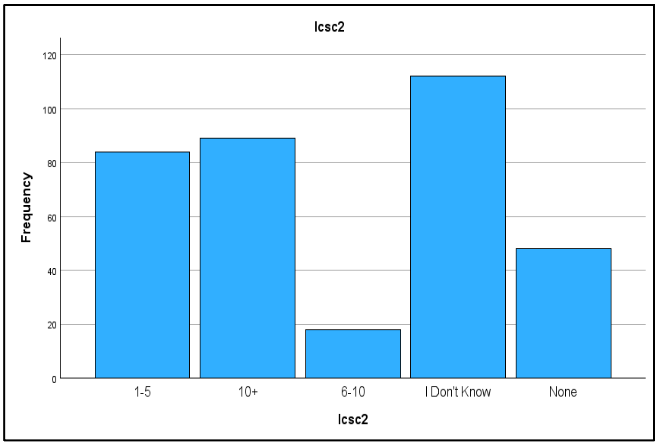


Fig. 9. Descriptive statistics of implementation of cyber controls and precautions (Icsc2).

TABLE II. RESULT SUMMARY FOR REFLECTIVE MEASUREMENT MODEL

Factor	Items	Loadings	Indicator reliability	AVE	Composite reliability	Cronbach's alpha	Discriminant validity
Importance of Cybersecurity	Ics1	.829	.702	.6408	0.69576	.415	Yes
	Ics2	.771	.731				
Social resources	Sr1	.718	.706	.5430	0.659471	.324	Yes
	Sr2	.765	.692				
	Sr3	.727	.694				
Organizational resources	Or1	.756	.694	.4608	0.611686	.299	Yes
	Or2	.648	.699				
	Or3	.680	.692				
	Or4	.624	.699				
Personal resources	Pr1	.719	.699	.4783	0.68684	.354	Yes
	Pr2	.669	.693				
	Pr3	.736	.706				
	Pr4	.748	.696				
	Pr5	.571	.690				
Implementation of cyber security controls	Icsc1	.898	.725	.8227	0.884216	.542	Yes
	Icsc2	.916	.724				

G. Result for Formative Construct Significance Testing

Table III displayed the results of a statistical analysis conducted on a formative factor named Cyber situational awareness "Csa category." This factor comprises four formative items: Csa1, Csa2, Csa3, and Csa4. Examining the outer weights column, it was observed that the relative importance of each item in shaping the overall formative factor. Higher values indicate a more significant influence of the respective item on the factor. Notably, Csa1 possesses the highest outer weight of 0.766, signifying its prominent role in defining the factor compared to the other items. Moving on to the T-value column, the statistical significance of the relationship between each item and the formative factor was assessed. Higher T-values indicate a more substantial relationship. All items exhibit considerable T-values, with Csa1 boasting the highest at 72.801. These results suggest that all items significantly contribute to the formative factor. The P-value column enables evaluating the level of significance associated with each item. P-value lower than the chosen significance level (typically 0.05) indicates statistical significance, implying that the indicator's relationship with the factor is unlikely to occur randomly [28]. In this analysis, all items demonstrate exceptionally low P-values (0.000), confirming their statistical significance.

In the 95% BCa confidence interval column, the researchers encountered a range that estimates the true relationship between each item and the formative factor. Narrower intervals indicate higher precision in estimating these relationships. Notably, all items exhibit relatively tight confidence intervals, suggesting high precision in capturing their relationships with the factor. The "Significance" column provides a succinct indication of the statistical significance of each item. In this case, all items are marked as "Yes," signifying their significant impact on the formative factor. These findings underscore the substantial importance of all four items (Csa1, Csa2, Csa3, and Csa4) in defining the formative factor. The high outer weights, significant T-values, low P-values, and narrow confidence intervals collectively provide strong evidence of the meaningful contribution of each item. Consequently, these results significantly enhance our understanding of the investigated phenomenon.

H. Results of the Structural Model Path Co-Efficient

In Table IV the hypothesis column represents the specific hypotheses being tested in the analysis. The hypotheses are labeled as H1, H2, H3, H4, and H5, indicating different relationships between the dependent and independent variables. Where D-I column specifies the dependent and independent variables involved in each hypothesis. It indicates the direction of the relationship being examined. For example, H1: Cyber situational awareness - Importance of cyber security (Csa-Ics) indicates that the independent variable Cyber situational awareness "Csa" is hypothesized to influence the dependent variable Importance of cyber security "Ics." The path coefficients in the hypothesis table indicate the strength and direction of the relationships between variables. Positive coefficients in H1 and H2 suggest that increasing Csa positively impacts Ics and social resources (Sr), respectively. The negative coefficient in H3 indicates that an increase in Icsc is associated with decreased organizational resources (Or). However, the relationships in H4 and H5 are not statistically significant, suggesting that the coefficients may not accurately represent the true impact.

Overall, the path coefficients provide valuable insights into the relationships between variables, highlighting significant associations and the need for further investigation in non-significant cases.

T-value provides information on the statistical significance of each path coefficient. The T-values indicate the degree to which the observed path coefficients deviate from zero. For H1, the T-value of 1.999 indicates a statistically significant relationship between Csa and Ics. Similarly, H2 shows a highly significant relationship between Csa and Sr, with a T-value of 4.837. In contrast, H3 reveals a statistically significant negative relationship between Icsc and Or, as indicated by the T-value of -2.492. However, H4 does not exhibit a significant relationship between Icsc and Pr, with a T-value of -1.010.

TABLE III. RESULT SUMMARY FOR FORMATIVE CONSTRUCT SIGNIFICANCE TESTING

Formative Factor	Formative items	Outer weights	T value	P value	95%BCa confidence interval	Significance P<.05
Cyber situational awareness (Csa_category)	Csa1	.766	72.801	.000	4.231 – 4.456	Yes
	Csa2	.651	34.550	.000	2.826 – 3.154	Yes
	Csa3	.725	44.251	.000	3.336 – 3.632	Yes
	Csa4	.736	43.310	.000	3.336 – 3.641	Yes

TABLE IV. SIGNIFICANCE TESTING RESULTS OF THE STRUCTURAL MODEL PATH CO-EFFICIENT

Hypothesis	D-I	Path coefficients	T value	P value	95% confidence intervals	Significance P<.005	R square
H1	Csa-Ics	.106	1.999	.046	.003 - .353	Yes	.011
H2	Csa-Sr	.251	4.837	.000	.143 - .340	Yes	.063
H3	Icsc-Or	-.132	-2.492	.013	-.171 - -.020	Yes	.017
H4	Icsc-Pr	-.054	-1.010	.313	-.107 - .034	No	.003
H5	Icsc-Csa	.079	1.488	.138	-.023 - .163	No	.006

The P-value column complements the T-values by providing the level of significance associated with each path coefficient. In H1, the P-value of 0.046 confirms the statistically significant relationship between Csa and Ics. H2 demonstrates a highly significant relationship between Csa and Sr, indicated by the P-value of 0.000. H3 exhibits a statistically significant relationship between Icsc and Or, with a P-value of 0.013. Conversely, H4 suggests no significant relationship between Icsc and Pr, with a P-value of 0.313.

The 95% confidence intervals offer a range within which the true population parameter is likely to fall. For H1, the confidence interval of 0.003 to 0.353 reinforces the statistical significance of the relationship between Csa and Ics. Similarly, the narrow interval of 0.143 to 0.340 for H2 supports the significance of the relationship between Csa and Sr. H3's confidence interval of -0.171 to -0.020 suggesting a significant negative relationship between Icsc and Or. However, caution is necessary when interpreting H4's confidence interval of -0.107 to 0.034, as the relationship between Icsc and Pr is not statistically significant. Fig. 10 shows the results of PLS-SEM analysis.

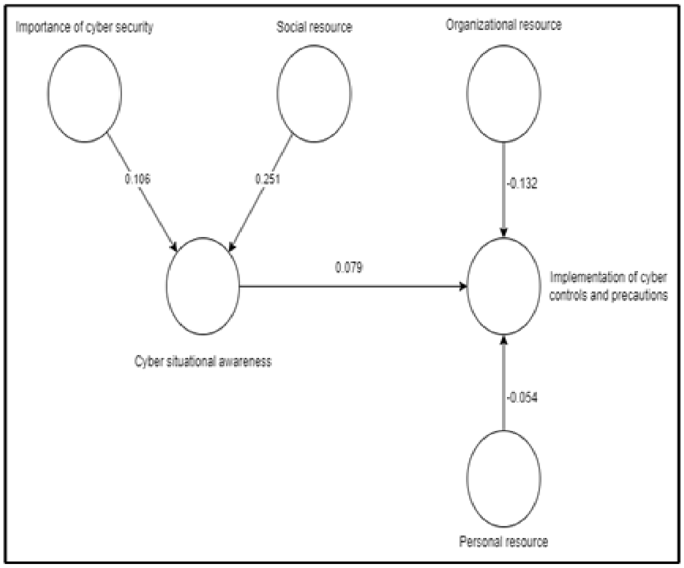

Importance of cyber security
Social resource
Organizational resource
0.106
0.251
-0.132
0.079
Implementation of cyber controls and precautions
Cyber situational awareness
-0.054
Personal resource

Fig. 10. Results of the PLS-SEM analysis.

I. *Impact of Negative Path Coefficient Values among Hypotheses*

Hypothesis H3 examines the relationship between the implementation of cyber security controls and precautions (Icsc) and organizational resources (Or), while Hypothesis H4 explores the relationship between Icsc and personal resources (Pr). Although both hypotheses have negative path coefficients, H3 (-0.132) is statistically significant, whereas H4 (-0.054) is not. Here is a detailed justification for these findings:

Hypothesis H3: The negative path coefficient (-0.132) in H3 suggests that as the implementation of cyber security controls and precautions (Icsc) increases, the availability or allocation of organizational resources (Or) decreases. Several reasons contribute to this relationship:

- Resource Reallocation: When organizations prioritize the implementation of cyber security controls and precautions, they often allocate resources, such as financial investments, personnel, and technology, to support these measures. This reallocation of resources can lead to reduced availability or allocation of resources for other organizational activities, resulting in a negative relationship between Icsc and Or.
- Trade-offs: Implementing cyber security controls and precautions often involves making trade-offs in resource allocation. Organizations may need to invest in security technologies, employee training, or hiring specialized personnel, which could lead to limited resources for other organizational needs. As a result, the negative path coefficient indicates that an increase in Icsc is associated with decreased available resources.
- Efficiency and Effectiveness: Implementing cyber security controls and precautions effectively requires utilizing resources efficiently. Organizations with limited resources may face challenges in implementing comprehensive security measures, leading to increased vulnerability and organizational risk. Consequently, the negative relationship between Icsc and or may arise from the difficulty in maintaining sufficient resources for cyber security and other organizational functions.

Hypothesis H4: Although H4 suggests a negative relationship between Icsc and personal resources (Pr), the non-significant p-value (0.313) indicates that this relationship is not statistically significant in the given sample. Several reasons may contribute to this result:

- Individual Factors: Personal resources encompass an individual's capabilities, knowledge, skills, and access to relevant information. The negative path coefficient implies that, in theory, as Icsc increases, personal resources (Pr) should decrease. However, in the context of the specific sample or survey respondents, other factors such as individual characteristics, experiences, and attitudes may overshadow the impact of Icsc on personal resources.
- Complexity of Personal Resources: Personal resources in cybersecurity could include individual knowledge, expertise, awareness, and adherence to security practices. Assessing personal resources accurately can be challenging, as it involves subjective factors and self-perception. Measurement limitations or insufficient sensitivity in capturing personal resource variations may contribute to the non-significant findings.
- Indirect Relationship: The relationship between Icsc and personal resources may be indirect, mediated by other variables not considered in the hypothesis. Factors such as organizational culture, training programs, or information-sharing practices might influence personal resources, moderating the relationship between Icsc and Pr. Not accounting for these mediating factors could result in a non-significant direct relationship between Icsc and Pr.

By considering a more extensive and diverse sample, conducting qualitative investigations, or refining the measurement instruments, researchers can better understand the relationship between Icsc and personal resources in the specific context of cyber security.

V. Conclusion and Future Work

Based on the research findings, several fruitful insights can be drawn that shed light on the relationships between cybersecurity items within organizations. The study identified a significant positive relationship between Cyber Situational Awareness (Csa) and Implementation of Cybersecurity Controls (Icsc), suggesting that enhancing awareness can contribute to better control implementation. In simple terms, Saudi Arabia should focus on raising cyber situational awareness among SMEs so that the SMEs have implementation of cyber security controls in their companies. Additionally, a significant positive relationship was found between Csa and Social Resources (Sr), emphasizing the importance of promoting awareness to enhance organizational resilience. Saudi Arabia should promote awareness among the SMEs so that the SMEs can have better organizational resilience to different cyber-attacks. Furthermore, a significant negative relationship between Icsc and Organizational Resources (Or) indicates that robust control implementation can potentially reduce organizational risk. SMEs in Saudi Arabia should implement robust cyber security mechanisms in their companies to reduce organizational risk. However, no significant relationships were found between Icsc and Personal Resources (Pr). In the context of Saudi Arabia, implementing cyber security does not rely on the personal resources of the employees of the SMEs. These findings provide valuable insights for organizations seeking to improve their cybersecurity practices.

While the study provides valuable insights, some limitations should be acknowledged. Firstly, the effect sizes observed were relatively small, suggesting that there may be other factors at play that were not considered in the analysis. Additionally, the study relied on self-reported data, which may introduce biases and inaccuracies. Data was collected from different sectors. The sample size and composition could also affect the generalizability of the findings. Furthermore, the study focused on specific variables and did not consider potential mediating or moderating factors. These limitations should be taken into account when interpreting the results.

Future work can focus on several areas to address the limitations and extend the research. Firstly, qualitative research can provide a deeper understanding of the underlying mechanisms behind the identified relationships. This qualitative exploration can help identify specific aspects of Cyber Situational Awareness and Personal Resources that impact control implementation most. Additionally, future studies can delve deeper into the dimensions of Cyber Situational Awareness, such as knowledge of threats and risk assessment capabilities, to develop targeted interventions and comprehensive training programs. Exploring additional contributors to Organizational Resources, such as human factors, supply chain vulnerabilities, and emerging technological threats, can also provide a more holistic understanding of risk management. Furthermore, investigating the role of communication strategies, organizational culture, and individual cognitive biases can assist in designing effective risk communication campaigns and tailored training programs. Integrating technical controls with organizational and behavioral aspects in comprehensive frameworks can enhance the effectiveness of cybersecurity initiatives. These future directions can further advance the understanding and practice of cybersecurity within organizations.

Acknowledgment

Thanks to the Saudi Electronic University for all support provided for this work.

References

[1] Karen Renaud and Jacques 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, pp. 24–46, 2021.

[2] F. Alharbi et al., “The impact of cybersecurity practices on cyberattack damage: The perspective of small enterprises in Saudi Arabia,” Sensors, vol. 21, no. 20, p. 6901, 2021.

[3] K. Luan, R. Halvorsrud, and C. Boletsis, “Evaluation of a Tool to Increase Cybersecurity Awareness Among Non-experts (SME Employees),” in Proceedings of the International Conference on Information Systems Security and Privacy (ICISSP), 2023, pp. 509–518.

[4] J. M. Archibald and K. Renaud, “Refining the pointer ‘human firewall’ pentesting framework,” Information & Computer Security, vol. 27, no. 4, pp. 575–600, 2019.

[5] T. Kokkonen, “Anomaly-based online intrusion detection system as a sensor for cyber security situational awareness system,” Jyväskylä studies in computing, no. 251, 2016.

[6] M. R. Endsley, Designing for situation awareness: An approach to user-centered design. CRC press, 2016.

[7] M. Husák, T. Jirsík, and S. J. Yang, “SoK: Contemporary issues and challenges to enable cyber situational awareness for network security,” in Proceedings of the 15th International Conference on Availability, Reliability and Security, 2020, pp. 1–10.

[8] G. Erdogan, R. Halvorsrud, C. Boletsis, S. Tverdal, and J. B. Pickering, “Cybersecurity Awareness and Capacities of SMEs,” 2023.

[9] N. Naik, P. Jenkins, P. Grace, and J. Song, “Comparing attack models for it systems: Lockheed martin’s cyber kill chain, mitre att&ck framework and diamond model,” in 2022 IEEE International Symposium on Systems Engineering (ISSE), IEEE, 2022, pp. 1–7.

[10] M. K. Ahn, Y. H. Kim, and J.-R. Lee, “Hierarchical multi-stage cyber attack scenario modeling based on G&E model for cyber risk simulation analysis,” Applied Sciences, vol. 10, no. 4, p. 1426, 2020.

[11] D. S. Rodriguez-Bermejo, R. D. Medenou, R. P. de Riquelme, J. M. Vidal, F. Torelli, and S. L. Sánchez, “Evaluation methodology for mission-centric cyber situational awareness capabilities,” in Proceedings of the 15th International Conference on Availability, Reliability and Security, 2020, pp. 1–9.

[12] N. Neshenko, C. Nader, E. Bou-Harb, and B. Furht, “A survey of methods supporting cyber situational awareness in the context of smart cities,” J Big Data, vol. 7, no. 1, pp. 1–41, 2020.

[13] M. N. Nafees, N. Saxena, A. Cardenas, S. Grijalva, and P. Burnap, “Smart grid cyber-physical situational awareness of complex operational technology attacks: A review,” ACM Comput Surv, vol. 55, no. 10, pp. 1–36, 2023.

[14] A. Georgiadou, S. Mouzakitis, and D. Askounis, “Assessing mitre att&ck risk using a cyber-security culture framework,” Sensors, vol. 21, no. 9, p. 3267, 2021.

[15] Small and Medium Enterprises General Authority, “Saudi SMEs official definition,” https://www.my.gov.sa.

[16] General Authority for Statistics, “Importance of small and medium enterprises (SMEs) to Saudi economy,” https://www.stats.gov.sa/en.

[17] A. Al-Tit, A. Omri, and J. Euchi, “Critical success factors of small and medium-sized enterprises in Saudi Arabia: Insights from sustainability perspective,” Adm Sci, vol. 9, no. 2, p. 32, 2019.

[18] O. M. Elhassan, “Obstacles and problems facing the financing of small and medium enterprises in KSA,” Journal of Finance and Accounting, vol. 7, no. 5, pp. 168–183, 2019.

[19] F. Alharbi et al., “on cyberattack damage: The perspective of small enterprises in Saudi Arabia,” Sensors, vol. 21, no. 20, p. 6901, 2021.

[20] V. V. Muthuswamy, “Cyber Security Challenges Faced by Employees in the Digital Workplace of Saudi Arabia’s Digital Nature Organization,” International Journal of Cyber Criminology, vol. 17, no. 1, pp. 40–53, 2023.

[21] M. , Bada and J. R. Nurse, “The social and psychological impact of cyberattacks,” Emerging cyber threats and cognitive vulnerabilities, pp. 73–92, 2020.

[22] M. S. Satar and G. Alarifi, “Factors of E-business adoption in small and medium enterprises: evidence from Saudi Arabia,” Hum Behav Emerg Technol, vol. 2022, 2022.

[23] M. Hassan, K. Saeedi, H. Almagwashi, and S. Alarifi, “Information Security Risk Awareness Survey of Non-governmental Organization in Saudi Arabia,” in The International Research & Innovation Forum, Springer, 2022, pp. 39–71.

[24] A. AbuAbid, M. Rahim, and H. Scheepers, “Experienced Benefits and Barriers of e-Business Technology Adoption by SME suppliers,” vol. 2011, p. 11, 2011, doi: 10.5171/2011.7917780.

[25] J. Pallant, SPSS survival manual: A step by step guide to data analysis using IBM SPSS. McGraw-hill education (UK), 2020.

[26] F. Ridzuan and W. M. N. W. Zainon, “A review on data cleansing methods for big data,” Procedia Comput Sci, vol. 161, pp. 731–738, 2019.

[27] A. Diamantopoulos, M. Sarstedt, C. Fuchs, P. Wilczynski, and S. Kaiser, “Guidelines for choosing between multi-item and single-item scales for construct measurement: a predictive validity perspective,” J Acad Mark Sci, vol. 40, pp. 434–449, 2012.

[28] A. Purwanto, “Partial least squares structural squation modeling (PLS-SEM) analysis for social and management research: a literature review,” Journal of Industrial Engineering & Management Research, 2021.