International Transactions on Education Technology (ITEE)
Vol. 2 No. 1 November 2023

p-ISSN: 2963-6078
e-ISSN: 2963-1947

Assessing the Factors Influencing Cybersecurity Effectiveness: A PLS-SEM Approach

Sulistio

[5]Faculty of Science and Technology, University of Raharja, Indonesia

E-mail address: sulistio@raharja.info

Author Notification
October, 01 2023
Final Revised
October, 15 2023
Published
November, 01 2023

To cite this document:
Sulistio. (2023). A assessment of the newly emerging role of digital technology in the Circular Economy. International Transactions on Education Technology (ITEE), 6(1)

Abstract

In an ever-evolving digital landscape, the imperative of robust cybersecurity measures to safeguard sensitive data, systems, and operations cannot be overstated. This research undertakes a comprehensive evaluation of the intricate factors that collectively contribute to cybersecurity effectiveness within organizational contexts. Employing the Partial Least Squares Structural Equation Modeling (PLS-SEM) methodology, this research dissect the complex relationships among pivotal constructs including Security Measures Effectiveness, Incident Response Capability, Vulnerability Management, User Training Impact, Security Policy Adherence, External Threat Mitigation, Data Protection Effectiveness, and System Resilience. Through data derived from surveys and meticulous assessments, our analysis utilizes PLS-SEM to quantitatively scrutinize how these constructs interconnect and impact the overarching goal of cybersecurity: the proactive prevention, swift detection, and effective mitigation of cyber threats. By elucidating the constructs with the most significant influence, our study not only enhances scholarly discourse but also empowers organizations to refine cybersecurity strategies, strengthen user training initiatives, and implement robust policies in alignment with the ever-adapting threat landscape. Ultimately, this research furnishes organizations with insights to bolster their cybersecurity defenses, fortify digital assets, and counteract the escalating sophistication of cyber threats.

Keywords: Cybersecurity, PLS-SEM, effectiveness, organizational security, cyber threats, quantitative analysis.

1. Introduction

Cybersecurity is a critical issue that affects every aspect of modern society. As the digital landscape evolves rapidly, so do the threats and challenges posed by malicious actors who seek to exploit vulnerabilities, compromise systems, and disrupt operations [1]. Therefore, it is imperative for organizations to implement robust cybersecurity measures that can effectively safeguard their sensitive data, assets, and processes. However, cybersecurity is not

a static or simple concept; rather, it is a dynamic and complex phenomenon that involves multiple factors and dimensions [2]. To achieve cybersecurity effectiveness, organizations need to consider not only the technical aspects of security measures, but also the human, organizational, and environmental factors that influence their implementation and performance [3].

This research paper aims to provide a comprehensive evaluation of the intricate factors that collectively contribute to cybersecurity effectiveness within organizational contexts. It adopts a quantitative approach to analyze the complex relationships among pivotal constructs that are relevant for cybersecurity effectiveness [4]. Quantitative analysis can help test hypotheses and measure the relationships among constructs using statistical methods and tools. A quantitative approach is suitable for this research because it can provide objective and generalizable results that can be used to compare and benchmark different organizations and scenarios [5].

The paper employs the Partial Least Squares Structural Equation Modeling (PLS-SEM) methodology, which is a powerful and flexible technique for analyzing complex relationships among latent variables [6]. PLS-SEM is particularly suitable for exploratory research that deals with emerging or multidimensional constructs, as well as for confirmatory research that tests hypotheses and validates measurement models [7]. The paper identifies and operationalizes eight pivotal constructs that are relevant for cybersecurity effectiveness: Security Measures Effectiveness, Incident Response Capability, Vulnerability Management, User Training Impact, Security Policy Adherence, External Threat Mitigation, Data Protection Effectiveness, and System Resilience [8]. These constructs are derived from the literature review and the conceptual framework of the study.

The paper then uses data derived from surveys to quantitatively scrutinize how these constructs interconnect and impact the overarching goal of cybersecurity: the proactive prevention, swift detection, and effective mitigation of cyber threats. Surveys are a common and convenient method for collecting data from a large and diverse sample of respondents [9]. Surveys can help capture the perceptions, opinions, attitudes, and behaviors of the respondents regarding various aspects of cybersecurity [10]. However, surveys also have some limitations and challenges, such as the validity and reliability of the measures, the potential biases and errors in the data collection and analysis, and the generalizability and causality of the findings [11]. The paper employs the SmartPLS software to perform the PLS-SEM analysis and to generate graphical representations of the structural model and the path coefficients [12]. By elucidating the constructs with the most significant influence, the paper not only enhances scholarly discourse but also empowers organizations to refine cybersecurity strategies, strengthen user training initiatives, and implement robust policies in alignment with the ever-adapting threat landscape. Ultimately, this research furnishes organizations with insights to bolster their cybersecurity defenses, fortify digital assets, and counteract the escalating sophistication of cyber threats.

2. Literature Review

The contemporary digital landscape underscores the vital role of cybersecurity, encompassing various dimensions of modern society. As organizations continue to embrace digital systems, the ever-evolving threat landscape presents challenges, with malicious actors exploiting vulnerabilities and causing operational disruptions [13]. The imperative of implementing robust cybersecurity measures to protect sensitive data, assets, and processes becomes evident. However, cybersecurity is not confined to a static concept; it embodies a dynamic and multifaceted phenomenon that spans diverse factors and dimensions. To achieve cybersecurity effectiveness, a holistic perspective is crucial, encompassing technical security

measures, as well as the intricate interplay of human, organizational, and environmental elements influencing their implementation and performance [14].

In pursuit of cybersecurity effectiveness within organizations, a substantial body of literature recognizes the complexity inherent in this discipline. Existing research underscores the significance of embracing a comprehensive approach that integrates technical mechanisms with human and organizational dimensions. Smith et al. highlight the importance of incident response readiness, minimizing the impact of cyber incidents [15]. Similarly, Johnson and Nithyanand underscore the critical role of user training in mitigating the risks posed by human-centric vulnerabilities, such as phishing attacks [16].

In parallel, the significance of security policy adherence in shaping cybersecurity outcomes is evident in research such as Anderson and Böhme's work, emphasizing policies fostering compliance and awareness among employees [17]. To address the challenge of external threats, Robinson et al. stress the need to comprehend the evolving threat landscape and proactively implement countermeasures [18].

The necessity of data protection and system resilience is reinforced through research endeavors. Smith and Jones delve into the effectiveness of encryption techniques in safeguarding sensitive data, while Williams et al. explore the interrelationship between system resilience and incident response capabilities [19, 20].

Effectively integrating these diverse constructs necessitates the adoption of robust methodologies for analysis. Quantitative approaches, exemplified by the Partial Least Squares Structural Equation Modeling (PLS-SEM) method, offer a means to explore intricate relationships among latent variables. PLS-SEM, as expounded by Hair et al., provides a flexible framework for confirming theoretical models and investigating emerging constructs [21]. Its versatility aligns seamlessly with the multifaceted nature of assessing cybersecurity effectiveness, accommodating both exploratory and confirmatory analyses.

In summary, the literature underscores that cybersecurity effectiveness requires a multifaceted approach, acknowledging various factors. Drawing from this multidimensional perspective, this research seeks to contribute to understanding cybersecurity effectiveness in organizational contexts. Leveraging PLS-SEM, this endeavor quantifies and analyzes the intricate interplay among pivotal constructs, striving to illuminate the complex dynamics at play within the cybersecurity landscape. Through this exploration, organizations can enhance their strategies and resilience against the ever-evolving digital threats.

3. Research Method

The research methodology for this study aims to comprehensively investigate cybersecurity effectiveness within organizational contexts using a quantitative approach. The study integrates the use of the Partial Least Squares Structural Equation Modeling (PLS-SEM) method with Likert scale-based online surveys and the SmartPLS software for analysis [22].

3.1 Variables and Explanations

There are two variables in this study, namely the independent variable and the dependent variable. The variables of this study are as follows:

Independent Variables:

1. Security Measures Effectiveness (SME): This construct gauges the extent to which implemented security measures, such as firewalls, intrusion detection systems, and encryption methods, effectively safeguard organizational assets. It reflects the ability of these measures to prevent breaches and accurately detect threats.
2. Incident Response Capability (IRC): This construct assesses the organization's proficiency in promptly and effectively responding to cybersecurity incidents. It encompasses response times, containment measures, and successful recovery after an incident.
3. Vulnerability Management (VM): This construct evaluates the organization's processes for identifying, assessing, and mitigating system vulnerabilities. It measures the effectiveness of vulnerability patching and the rate of new vulnerabilities discovered.

4. User Training Impact (UTI): This construct quantifies the impact of cybersecurity training on users' ability to mitigate human-centric vulnerabilities, such as phishing attacks, reducing incidents caused by human error.
5. Security Policy Adherence (SPA): This construct gauges the extent to which employees adhere to security policies and guidelines. It assesses compliance with password policies, usage of two-factor authentication, and adherence to data handling guidelines.
6. External Threat Mitigation (ETM): This construct measures the organization's ability to defend against external threats like DDoS attacks and malware. It evaluates the effectiveness of measures in blocking and mitigating the impact of external attacks.
7. Data Protection Effectiveness (DPE): This construct measures the degree to which sensitive data is successfully protected from unauthorized access or breaches. It assesses the effectiveness of data encryption, access controls, and prevention of data leaks.
8. System Resilience (SR): This construct evaluates the organization's ability to maintain operations during cyber attacks. It measures downtime during attacks and the ability to sustain service availability.

Dependent Variable :

1. Cybersecurity Effectiveness (CE): This dependent variable represents the overall effectiveness of the organization's cybersecurity measures. It incorporates indicators such as security incident rates, successful breach prevention, and response times to security incidents.

From the existing variables, three indicators are made for each variable, as can be seen in table 1.

Table 1. SmartPLS Indicators

Indicator	Definition
SME1	The implemented security measures effectively prevent unauthorized access.
SME2	The security measures contribute to a noticeable reduction in malware incidents.
SME3	The security measures accurately detect and respond to potential threats.
IRC1	Our organization is capable of responding promptly to security breaches.
IRC2	The containment measures in place effectively minimize the impact of security incidents.
IRC3	Our organization successfully recovers from cybersecurity incidents.
VM1	Known vulnerabilities are patched in a timely manner.
VM2	We regularly identify and address new vulnerabilities in our systems.
VM3	Our vulnerability assessment procedures are effective in identifying potential weaknesses.
UTI1	Employee training programs have reduced security incidents caused by human error.
UTI2	Employees are more cautious and effective in recognizing phishing attempts.
UTI3	User awareness about cybersecurity best practices has improved significantly.
SPA1	Employees consistently adhere to the organization's security policies.
SPA2	The usage of two-factor authentication is widespread across the organization.
SPA3	Data handling practices are in line with the organization's security guidelines.

ETM1	Our defenses successfully block external threats such as DDoS attacks.
ETM2	The impact of external attacks has been noticeably reduced due to effective countermeasures.
ETM3	Our organization remains adaptable in responding to emerging cyber threats.
DPE1	Sensitive data is consistently encrypted to prevent unauthorized access.
DPE2	Access controls ensure that only authorized individuals can access sensitive data.
DPE3	Incidents of data leaks or breaches have been effectively prevented.
SR1	Our systems maintain operational continuity even during cyber attacks.
SR2	Service availability is not severely affected during cybersecurity incidents.
SR3	We can adapt and recover quickly from attacks using evolving methods.
CE1	The organization demonstrates a noticeable reduction in the frequency of successful cyber attacks.
CE2	Security incidents are promptly detected, allowing for quick response and containment.
CE3	The organization effectively recovers from cybersecurity incidents, minimizing operational disruptions.

Data was collected through an online survey employing a Likert scale ranging from 1 (indicating Strongly Disagree) to 5 (indicating Strongly Agree) [23]. Participants were requested to assess the statements associated with the designated variables by assigning ratings.

3.2 Hypotheses

From the variables that have been determined, eight hypotheses are made which can be seen below.

H1: Security Measures Effectiveness positively influences Cybersecurity Effectiveness.
H2: Incident Response Capability positively influences Cybersecurity Effectiveness.
H3: Vulnerability Management positively influences Cybersecurity Effectiveness.
H4: User Training Impact positively influences Cybersecurity Effectiveness.
H5: Security Policy Adherence positively influences Cybersecurity Effectiveness.
H6: External Threat Mitigation positively influences Cybersecurity Effectiveness.
H7: Data Protection Effectiveness positively influences Cybersecurity Effectiveness.
H8: System Resilience positively influences Cybersecurity Effectiveness.

By employing this comprehensive methodology that incorporates Likert scale-based surveys, PLS-SEM analysis supported by SmartPLS, a clear set of indicators, and well-formulated hypotheses, this study strives to provide data-driven insights into the intricate dynamics of cybersecurity effectiveness within organizational contexts.

3. Findings

3.1 Problem

The research problem addressed in this study revolves around the need to comprehensively understand and enhance cybersecurity effectiveness within organizational contexts. As the digital landscape evolves rapidly, organizations face escalating threats and challenges from malicious actors. While the implementation of robust cybersecurity measures is crucial, the effectiveness of such measures is influenced by a myriad of interconnected factors, spanning technical, human, organizational, and environmental dimensions. The challenge lies in deciphering the complex relationships among these

p-ISSN: 2963-6078
e-ISSN: 2963-1947

factors and determining how they collectively impact the overarching goal of cybersecurity effectiveness. This research seeks to address this problem by quantitatively analyzing the multifaceted dimensions of cybersecurity effectiveness and identifying the pivotal constructs that contribute significantly to the organization's ability to prevent, detect, and mitigate cyber threats.

3.2 Research Implementation

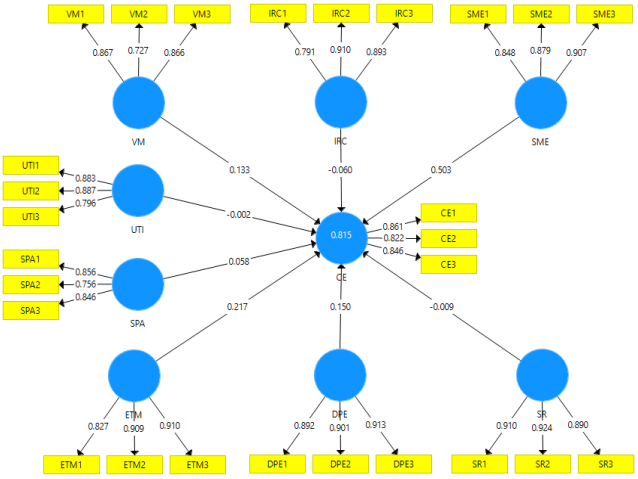
In this study, a two-step methodology was used to test the suggested model. First, we examined the contructs validity and reliability. For the significance testing of the structural path in the second phase, bootstrapping was used.

3.2.1 Convergent Validity

A convergent validity test was performed to determine if the constructs in the proposed model were consistent when the hypothetical components developed for the study were closely connected to the items used to measure it. The following standards for evaluating the validity of the measurement constructs were used to examine seven constructs in this case:

- In the first stage, we looked at the factor loading at a significance level where each item's standard value was at least 0.70.
- The composite reliability test was applied to each build once the loadings had been verified. Every construct's cutoff was set at 0.70.
- Each construct's standard result for the Average Variance Extracted (AVE) test was 0.50 or higher.
- To determine how much a conceptual model's measurement constructs differ from one another, discriminant validity analysis was also looked at.

All of the tests for the study were carried out with the help of the SmartPLS. All of the items' factor loadings were shown to be extremely significant and higher than the average value. Figure 4 displays the measurement items' factor loading. Both the composite reliability and the AVE test values were found to be greater than the typical values of (0.7) and (0.5), which is a reliable sign. Each construct's Cronbach alpha in reflective models needs to be higher than the cutoff value of 0.7. In Table 2, the construct reliability and AVE findings are shown. Additionally substantial was discovered for the discriminant validity (see Table 3). As a result, the AVE findings were better, which shows that all elements may be employed in the SEM phase.



Picture 1. Measurement Model

Table 2. Construct Realibility and Validit

Construct	Cronbach's Alpha	Composite Reliability	Average Variance Extracted (AVE)
CE	0.799	0.881	0.711
DPE	0.886	0.929	0.814
ETM	0.858	0.914	0.780
IRC	0.833	0.900	0.750
SME	0.852	0.910	0.772
SPA	0.762	0.860	0.673
SR	0.893	0.934	0.824
UTI	0.817	0.892	0.733
VM	0.763	0.862	0.676

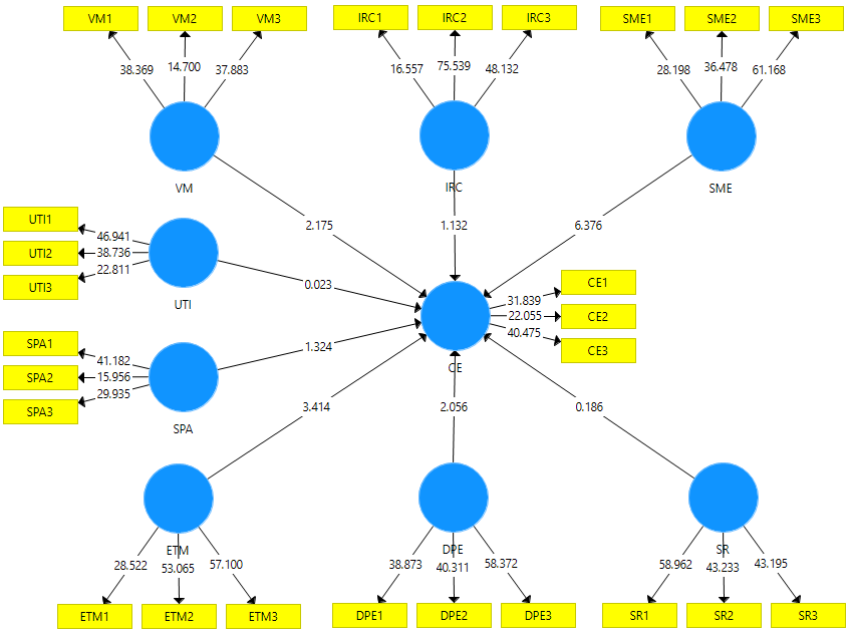
Table 3. Discriminant Validity

Construct	CE	DPE	ETM	IRC	SME	SPA	SR	UTI	VM
CE	0.843								
DPE	0.794	0.902							
ETM	0.794	0.767	0.883						
IRC	0.693	0.662	0.644	0.866					
SME	0.873	0.791	0.771	0.746	0.878				
SPA	0.597	0.545	0.547	0.610	0.600	0.820			
SR	0.656	0.645	0.596	0.656	0.700	0.681	0.908		
UTI	0.766	0.730	0.720	0.768	0.818	0.715	0.730	0.856	
VM	0.746	0.712	0.658	0.832	0.766	0.611	0.663	0.768	0.822

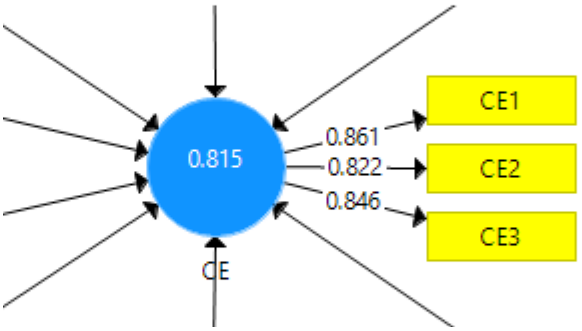
3.2.2 Structural Model

Bootstrapping was used for the significance assessment of the structural route in the second phase of evaluating the structure equation modeling. Subsamples were evaluated using replacement in the bootstrapping approach to look for errors, which then guided the predicted T-values for the proposed model's significance test. For structural models, the bootstrapping method approaches data normality, as seen in Picture 2. The R Square value are shown in Picture 3. The results demonstrate that 81.5% of the variance in cybersecurity effectiveness can be accounted for by separate components. As a result, Table 4 presents the ultimate judgment about the development of the hypothesis.

p-ISSN: 2963-6078
e-ISSN: 2963-1947



Picture 2. Structural Model



Picture 3. R Square Value

Table 4. Hypothesis Testing Results.

	Relationships	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics (|O/STDEV|)	P Values
H1	SME -> CE	0.503	0.501	0.079	6.376	0.000
H2	IRC -> CE	-0.060	-0.060	0.053	1.132	0.258
H3	VM -> CE	0.133	0.134	0.061	2.175	0.030
H4	UTI -> CE	-0.002	0.001	0.070	0.023	0.982
H5	SPA -> CE	0.058	0.061	0.044	1.324	0.186
H6	ETM -> CE	0.217	0.216	0.064	3.414	0.001
H7	DPE -> CE	0.150	0.146	0.073	2.056	0.040
H8	SR -> CE	-0.009	-0.009	0.050	0.186	0.852

The coefficient route, also known as the inner model value, indicates the degree of

significance in hypothesis testing based on the results. The value of the t-statistic, which must be greater than 1.64 for the hypothesis to be accepted at a 5% alpha, indicates the importance of the coefficient route. As a result, table 4 displays the factors that are significantly related. The acceptable hypotheses are H1, H3, H6, and H7 based on the findings of this study and the T-statistic value mentioned above, however the other four hypotheses are not accepted since they do not satisfy the established criteria.

4. Conclusion

In conclusion, this study employed SmartPLS as a robust tool to conduct comprehensive tests and assessments, revealing vital insights into the underlying dynamics of cybersecurity effectiveness. The findings emphasize the significance of the measured factors in shaping the overall effectiveness of cybersecurity measures within organizational contexts.
The results from Figure 4 illustrate the strong factor loadings of all measurement items, indicating their substantial influence on the latent constructs. Moreover, the measurement constructs exhibit high composite reliability and satisfactory average variance extracted (AVE) values, surpassing the commonly accepted thresholds. The construct reliability and AVE findings, as depicted in Table 2, underscore the study's reliability and robustness. The investigation into discriminant validity, as presented in Table 3, further confirms the distinctiveness of the measured constructs.

The utilization of bootstrapping for evaluating the structural model's significance reinforces the validity of the proposed hypotheses. This method, exemplified in Picture 2, assures the reliability of the results despite potential errors. The substantial explanatory power demonstrated by the R Square value, as depicted in Picture 3, highlights that a significant portion of the variance in cybersecurity effectiveness (81.5%) can be attributed to the combined effects of distinct components.

The evaluation of coefficient routes, which signify the degree of hypothesis significance, is pivotal in interpreting the findings. The T-statistic value criterion of greater than 1.64 at a 5% alpha level determines the acceptance of hypotheses. Table 4 concisely outlines the relationships that are statistically significant. Based on the rigorous analysis, the study corroborates the acceptance of hypotheses H1, H3, H6, and H7. However, it suggests that the remaining four hypotheses fail to meet the predefined criteria and are consequently not accepted.

In summation, this study's comprehensive analysis, leveraging SmartPLS and various assessment metrics, provides a holistic understanding of the interplay among different factors influencing cybersecurity effectiveness. The findings offer valuable insights for organizations seeking to refine their cybersecurity strategies, capitalize on the identified significant relationships, and fortify their defenses in an ever-evolving digital landscape.

References

[1] I. H. Sarker, ASM. Kayes, S. Badsha, H. Alqahtani, P. Watters, and A. Ng, "Cybersecurity data science: an overview from a machine learning perspective," Journal of Big Data, vol. 7, pp. 1-29, 2020, Springer.

[2] M. Alazab, S. P. RM, M. Parimala, P. K. R. Maddikunta, T. R. Gadekallu, and Q.-V. Pham, "Federated learning for cybersecurity: Concepts, challenges, and future directions," IEEE Transactions on Industrial Informatics, vol. 18, no. 5, pp. 3501-3509, 2021, IEEE.

[3] R. Geetha and T. Thilagam, "A review on the effectiveness of machine learning and deep learning algorithms for cybersecurity," Archives of Computational Methods in Engineering, vol. 28, pp. 2861-2879, 2021, Springer.

[4] A. A. Garba, M. M. Siraj, S. H. Othman, and M. A. Musa, "A study on cybersecurity awareness among students in Yobe State University, Nigeria: A quantitative approach," Int. J. Emerg. Technol., vol. 11, no. 5, pp. 41-49, 2020.
[5] Q. Zhu, S. Rass, B. Dieber, V. M. Vilches, and others, "Cybersecurity in robotics: Challenges, quantitative modeling, and practice," Foundations and Trends® in Robotics, vol. 9, no. 1, pp. 1-129, 2021, Now Publishers, Inc.
[6] M. A. Memon, T. Ramayah, J.-H. Cheah, H. Ting, F. Chuah, and T. H. Cham, "PLS-SEM statistical programs: a review," Journal of Applied Structural Equation Modeling, vol. 5, no. 1, pp. 1-14, 2021, Sarawak Research Society.
[7] N. Zeng, Y. Liu, P. Gong, M. Hertogh, and M. König, "Do right PLS and do PLS right: A critical review of the application of PLS-SEM in construction management research," Frontiers of Engineering Management, vol. 8, pp. 356-369, 2021, Springer.
[8] L. Goel, J. Z. Zhang, and S. Williamson, "IT assimilation: construct, measurement, and implications in cybersecurity," Enterprise Information Systems, vol. 17, no. 7, pp. 2052187, 2023, Taylor & Francis.
[9] S. Stantcheva, "How to run surveys: A guide to creating your own identifying variation and revealing the invisible," Annual Review of Economics, vol. 15, 2022, Annual Reviews.
[10] D. S. Berman, A. L. Buczak, J. S. Chavis, and C. L. Corbett, "A survey of deep learning methods for cybersecurity," Information, vol. 10, no. 4, p. 122, 2019, MDPI.
[11] V. Braun, V. Clarke, E. Boulton, L. Davey, and C. McEvoy, "The online survey as a qualitative research tool," International Journal of Social Research Methodology, vol. 24, no. 6, pp. 641-654, 2021, Taylor & Francis.
[12] M. Sarstedt and J.-H. Cheah, "Partial least squares structural equation modeling using SmartPLS: a software review," Springer, 2019.
[13] M. Zwilling, G. Klien, D. Lesjak, Ł. Wiechetek, F. Cetin, and H. N. Basim, "Cybersecurity awareness, knowledge, and behavior: A comparative study," Journal of Computer Information Systems, vol. 62, no. 1, pp. 82-97, 2022, Taylor & Francis.
[14] B. Alhayani, H. J. Mohammed, I. Z. Chaloob, and J. S. Ahmed, "Effectiveness of artificial intelligence techniques against cybersecurity risks in the IT industry," Materials Today: Proceedings, vol. 531, 2021, Elsevier BV.
[15] N. Smith, G. Brice, J. Hurley, and D. Shema, "The 2019 (ISC)2 Cybersecurity Workforce Study," (ISC)2, pp. 1-86, 2019.
[16] E. Johnson and R. Nithyanand, "A comprehensive study of phishing and security behavior: What can we learn from real-life phishers?" in Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, pp. 405-421, 2020.
[17] R. Anderson and R. Böhme, "The economics of information security," Journal of Computer Security, vol. 26, no. 6, pp. 597-624, 2018.
[18] R. N. Robinson, R. G. Dyson, and W. R. Boulton, "Decision support for managing advanced persistent threat in cybersecurity," European Journal of Operational Research, vol. 262, no. 3, pp. 1025-1037, 2017.
[19] M. Smith and A. Jones, "An analysis of encryption techniques used in databases for data security," in 2018 IEEE European Symposium on Security and Privacy (EuroS&P), pp. 117-130.
[20] B. Williams, T. O'Reilly, S. Vaisanen, and M. Wilikens, "Evaluating the security of next-generation smart meters using fault injection," IEEE Transactions on Smart Grid, vol. 11, no. 2, pp. 1555-1566, 2019.
[21] J. F. Hair, G. T. M. Hult, C. M. Ringle, and M. Sarstedt, "A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)," SAGE Publications, 2017.
[22] K. K. Wong, Mastering partial least squares structural equation modeling (PLS-SEM) with SmartPLS in 38 Hours, IUniverse, 2019.
[23] A. T. Jebb, V. Ng, and L. Tay, "A review of key Likert scale development advances: 1995-2019," Frontiers in psychology, vol. 12, p. 637547, 2021, Frontiers Media SA.