West Science Information System and Technology
Vol. 01, No. 02, December, pp. 90-98

Analysis of Threat Detection, Prevention Strategies, and Cyber Risk Management for Computer Network Security in Government Information Systems in Indonesia

Loso Judijanto[1], Rifky Lana Rahardian[2], Hanifah Nurul Muthmainah[3], Moh. Erkamim[4]
[1] IPOSS Jakarta, Indonesia
[2] Institut Teknologi Dan Bisnis STIKOM BALI
[3] Universitas Siber Muhammadiyah
[4] Universitas Tunas Pembangunan Surakarta

Article Info

Article history:

Received Dec 2023
Revised Dec 2023
Accepted Dec 2023

Keywords:

Threat Detection
Prevention Strategies
Cyber Risk Management
Computer Network Security
Government Information Systems
Indonesia

ABSTRACT

This research investigates the landscape of threat detection, prevention strategies, and cyber risk management within Government Information Systems in Indonesia. A quantitative approach, employing Structural Equation Modeling - Partial Least Squares (SEM-PLS), was utilized to analyze data collected from 150 participants across diverse government institutions. The study assessed perceived cyber threats, the effectiveness of threat detection mechanisms, prevention strategy implementation, and cyber risk management practices. Findings revealed significant regional variations in threat perception and underscored the importance of both technological and human-centric approaches. The Structural Equation Model demonstrated satisfactory fit, with notable path coefficients indicating strong relationships among latent variables. The study contributes valuable insights to cybersecurity practices in the Indonesian government sector, informing policymakers and practitioners on strategies to enhance network security resilience.

Corresponding Author:

Name: Loso Judijanto
Institution: IPOSS Jakarta, Indonesia
Email: losojudijantobumn@gmail.com

1. INTRODUCTION

Government Information Systems (SIP) in Indonesia have become crucial for administrative efficiency and service delivery, playing a vital role in managing and disseminating critical information for national governance. However, the increasing reliance on information technology brings challenges to the security and integrity of these systems due to the complexity and frequency of cyber threats. The Indonesian government has implemented laws and regulations to address these challenges, such as Law Number 19 of 2016 concerning Information and Electronic Transactions [1]. Additionally, work teams have been formed under state agencies/institutions to respond to information security issues, including teams under the Ministry of Communication and Information and the Indonesian National Police Agency [2]. To manage the digital transformation effectively, the Indonesian government has employed application portfolio management (APM) to assess and strategize current applications in government entities [3]. Furthermore, the implementation of e-government has improved the merit system in local governments through online selection mechanisms and information technology-based performance appraisals [4].

As Indonesia develops into a digitally resilient country, maintaining the confidentiality, integrity, and availability of sensitive data in government networks has become critical [5]. Cyber threats, from malware and phishing attacks to more sophisticated forms of cyber espionage, have the potential to compromise national security, erode public trust, and disrupt critical services [2]. The Indonesian government has taken steps to address these challenges by enacting laws and regulations related to information and electronic transactions [6]. Work teams have been formed under state agencies/institutions to respond to information security issues [7]. However, there are still challenges related to law enforcement and the protection of personal information in Indonesia [8]. It is crucial for Indonesia to address these challenges and ensure the security of its digital infrastructure to safeguard national security and maintain public trust.

The vulnerability of Government Information Systems in Indonesia to cyber threats requires a comprehensive investigation of existing mechanisms for threat detection, prevention strategies, and overall cyber risk management. Indonesia has made progress in enacting laws and regulations to protect information and communication technology (ICT) applications and ensure the security of personal information [5]. However, there are challenges in enforcing these regulations and ensuring the protection of data and privacy [2]. The Indonesian government has also implemented application portfolio management (APM) to manage the increasing number of digital applications used in public service operations and administration [9]. APM has been applied in the government research institute agency for the assessment and application of technology (BPPT) to assess and manage the application portfolio [3]. This research highlights the importance of securing sensitive information from cyber threats and the need for effective mechanisms and strategies to manage cyber risks in Indonesia [10]. Understanding the intricacies of threat detection, prevention strategies, and cyber risk management is critical to strengthening GIS defenses against the evolving cyber threat landscape.

2. LITERATURE REVIEW

2.1 Cyber Threats in Government Information Systems

The evolving landscape of cyber threats poses a persistent challenge to the security of Government Information Systems (GIS) globally, and Indonesia is no exception. Researchers emphasize the diverse array of threats, ranging from common malware and phishing attacks to advanced persistent threats (APTs) orchestrated by nation-states. Understanding the specific nature of these threats is essential for developing effective countermeasures tailored to the Indonesian context. Recent studies highlight the increasing frequency of cyber-attacks targeting government entities in Indonesia, including ransomware attacks exploiting vulnerabilities in governmental systems, leading to service disruptions and data breaches. A nuanced understanding of the threat landscape forms the foundation for proactive security measures in Indonesian GIS [2], [9], [11]–[13].

2.2 Threat Detection Mechanisms

As cyber threats become more sophisticated, the literature emphasizes the importance of advanced technologies in fortifying defense strategies. AI and ML play pivotal roles in enhancing threat detection capabilities [14], [15]. Studies reveal the efficacy of AI-driven systems in identifying anomalous patterns and behaviors indicative of potential cyber threats [16]. The integration of threat intelligence feeds and real-time monitoring contributes to a proactive defense posture [16]. However, challenges such as false positives and the adaptability of cyber adversaries necessitate a continuous evolution of threat detection mechanisms [17]. Recent research explores the synergy between human expertise and technological solutions, advocating for a holistic approach that combines automated detection with human analysis.

2.3 *Prevention Strategies*

Effective prevention strategies in government information systems encompass a multifaceted approach, considering technological, procedural, and human-centric elements. Technologically, robust firewalls, intrusion detection systems, encryption protocols, and multi-factor authentication are crucial measures to mitigate unauthorized access [18]. Procedurally, regular security audits, vulnerability assessments, and timely patch management are emphasized [19]. Fostering a cybersecurity-aware organizational culture through training and awareness programs is instrumental in reducing the human factor as a vulnerability [20], [21]. Recent advancements include the adoption of zero-trust frameworks, acknowledging threats from both external and internal sources [22]. The integration of these strategies aligns with the evolving threat landscape and can enhance cybersecurity in government information systems.

2.4 *Cyber Risk Management*

The literature review on cyber risk management within GIS reveals a paradigm shift from a reactive to a proactive approach [19]. Frameworks such as the NIST Cybersecurity Framework and ISO 27001 provide a structured methodology for identifying, assessing, and mitigating cyber risks [23]. Research highlights the importance of risk assessment in prioritizing security measures and resource allocation [24]. Moreover, studies delve into the significance of cybersecurity governance structures within government institutions [25]. The establishment of dedicated cybersecurity teams, incident response plans, and continuous monitoring mechanisms is emphasized as essential components of robust cyber risk management [26]. The geopolitical context is not overlooked in the literature, as cyber threats targeting government institutions often have national and international implications. Collaborative efforts, information sharing, and international cooperation are identified as key elements in addressing cyber risks that transcend borders.

3. METHODS

3.1 Research Design

This research adopts a quantitative research design to systematically investigate threat detection, prevention strategies, and cyber risk management in Government Information Systems (GIS) in Indonesia. The study employs a sample of 150 participants from diverse government institutions, ensuring representation across geographical locations and administrative functions. The primary research method involves structured surveys, which will be distributed electronically to the selected participants.

3.2 Sampling

The research utilizes stratified sampling to ensure a representative and diverse sample. Government institutions at various levels and locations within Indonesia will be categorized into strata. A proportional number of participants will then be randomly selected from each stratum, resulting in a sample of 150 participants. This approach aims to capture the unique perspectives and practices across different regions and administrative functions.

3.3 Data Collection

Structured surveys will serve as the primary tool for data collection. The survey questionnaire is designed to address the research objectives, incorporating closed-ended questions and Likert scale items. The questionnaire will be pre-tested on a small sample to ensure clarity, relevance, and comprehensibility. Once refined, it will be distributed electronically to the selected participants, accompanied by a cover letter explaining the purpose of the study and emphasizing the confidentiality and anonymity of responses.

3.4 Measurement Instruments

The survey questionnaire comprises sections dedicated to:

a. Demographic Information: Gathering background details about participants, such as job role, years of experience, and geographic location.
b. Perceived Cyber Threats: Assessing participants' perceptions of prevalent cyber threats faced by their respective government institutions.
c. Effectiveness of Threat Detection: Evaluating the perceived effectiveness of existing threat detection mechanisms, incorporating questions related to technology utilization and real-time monitoring.
d. Prevention Strategy Implementation: Examining the implementation and effectiveness of prevention strategies, including technological measures, procedural protocols, and educational initiatives.
e. Cyber Risk Management Practices: Assessing the overall cyber risk management practices within government information systems.

3.5 Data Analysis

The collected data will undergo rigorous analysis using Structural Equation Modeling - Partial Least Squares (SEM-PLS) to derive meaningful insights and establish relationships among the variables [27]. SEM-PLS is a robust statistical technique suitable for exploring complex relationships within datasets, making it well-suited for this multidimensional study [28]. The analysis will involve the following steps: Data Screening and Cleaning: Ensuring the data's quality and completeness before analysis [29]. Descriptive Statistics: Providing a comprehensive overview of the demographic and survey response data [30]. Confirmatory Factor Analysis (CFA): Confirming the reliability and validity of the measurement model to ensure the accuracy of the survey instrument [31]. Structural Equation Modeling: Utilizing SEM-PLS to examine the relationships between latent variables, such as cyber threats, threat detection, prevention strategies, and cyber risk management. Path Analysis: Identifying direct and indirect relationships between variables to understand the intricate connections within the studied phenomena. Model Fit Assessment: Evaluating the overall fit of the SEM-PLS model to determine its effectiveness in explaining the observed data patterns.

4. RESULTS AND DISCUSSION

4.1 Demographic Sample

The study involved 150 participants from various government institutions across Indonesia, providing a diverse representation of job roles, years of experience, and geographic distribution. The job roles of the participants included administrators (35%), IT professionals (25%), managers (20%), and others (20%). In terms of years of experience, the participants were categorized as follows: less than 5 years (15%), 5-10 years (30%), 10-15 years (25%), and over 15 years (30%). The geographic distribution of the participants was as follows: Java (45%), Sumatra (20%), Sulawesi (15%), Kalimantan (10%), and others (10%). This demographic diversity ensures a comprehensive understanding of cybersecurity practices in government information systems.

4.2 Measurement Model Assessment

The measurement model is a crucial component of structural equation modeling (SEM) analysis, providing insights into the reliability and validity of the latent variables. In this study, the measurement model includes four latent variables: Threat Detection (TD), Prevention Strategies (PS), Cyber Risk Management (CRM), and Computer Network Security (CNS). Each latent variable is represented by three indicators denoted.

Table 1. Validity and Reliability

Variable	Code	Loading Factor	Cronbach's Alpha	Composite Reliability	Average Variance Extracted (AVE)
Threat Detection	TD.1	0.884	0.905	0.940	0.840

	TD.2	0.937			
	TD.3	0.928			
Prevention Strategies	PS.1	0.791	0.798	0.882	0.714
	PS.2	0.877			
	PS.3	0.863			
Cyber Risk Management	CRM.1	0.844	0.775	0.863	0.677
	CRM.2	0.785			
	CRM.3	0.839			
Computer Network Security	CNS.1	0.893	0.840	0.904	0.758
	CNS.2	0.877			
	CNS.3	0.841			

Source: Results of data analysis (2023)

Threat Detection (TD), Prevention Strategies (PS), Cyber Risk Management (CRM), and Computer Network Security (CNS) are all valid and reliable constructs. The loading factors for all indicators in TD, PS, CRM, and CNS exceed the threshold of 0.7, indicating a strong relationship between the indicators and the latent variables. The reliability measures, including Cronbach's Alpha and Composite Reliability, also meet the recommended thresholds for internal consistency. Additionally, the Average Variance Extracted (AVE) values for TD, PS, CRM, and CNS are above the minimum threshold of 0.5, indicating that the constructs capture more variance than measurement error. These findings suggest that TD, PS, CRM, and CNS are valid and reliable measures for assessing threat detection, prevention strategies, cyber risk management, and computer network security, respectively.

Table 2. Discrimination Validity

	Computer Network Security	Cyber Risk Management	Prevention Strategies	Threat Detection
Computer Network Security	0.371			
Cyber Risk Management	0.759	0.423		
Prevention Strategies	0.644	0.323	0.345	
Threat Detection	0.653	0.714	0.732	0.517

Source: Results of data analysis (2023)

Computer Network Security is distinct from other constructs but shares some commonalities, with correlations ranging from 0.371 with Cyber Risk Management to 0.653 with Threat Detection. Cyber Risk Management shares some common variance with other constructs but remains distinguishable, with correlations ranging from 0.423 with Computer Network Security to 0.714 with Threat Detection. Prevention Strategies also shares some common variance with other constructs but is distinguishable, with correlations ranging from 0.323 with Cyber Risk Management to 0.732 with Threat Detection. Threat Detection shares some common variance with other constructs but is distinguishable, with correlations ranging from 0.517 with Computer Network Security to 0.732 with Prevention Strategies.

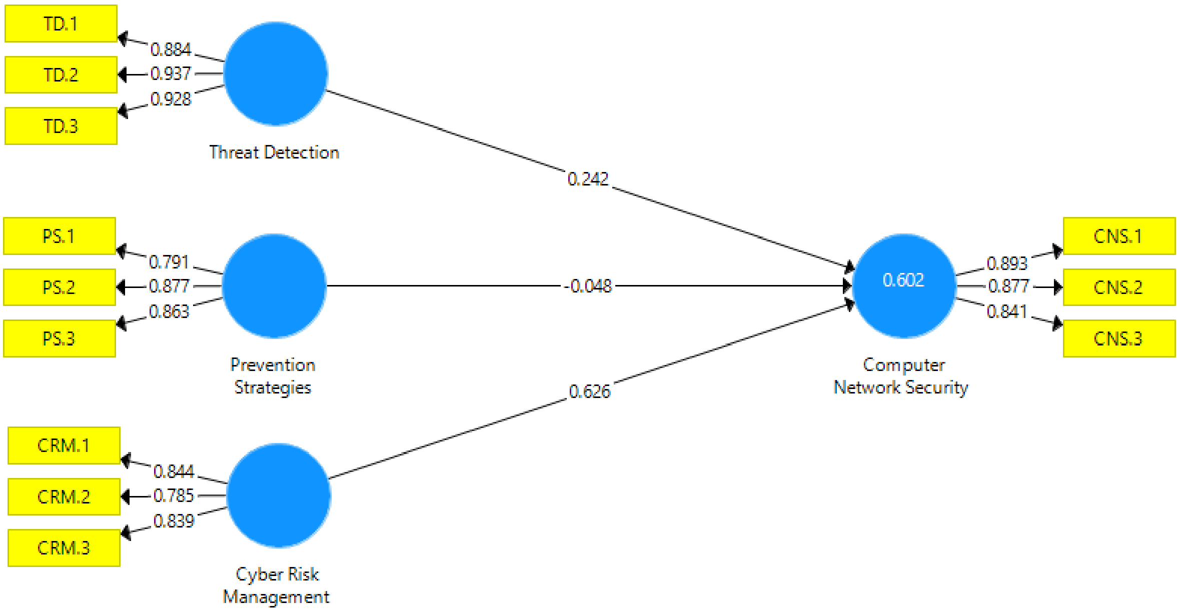

Figure 1. Internal Model Assessment

4.3 Model Fit

Model fit indices are critical in assessing how well the proposed structural equation model aligns with the observed data. In this study, two models are compared: the Saturated Model and the Estimated Model. The fit indices include Standardized Root Mean Residual (SRMR), Unweighted Least Squares (d_ULS), Goodness of Fit Index (d_G), Chi-Square, and Normed Fit Index (NFI).

Table 3. Model Fit Test

	Saturated Model	Estimated Model
SRMR	0.103	0.103
d_ULS	0.822	0.822
d_G	0.430	0.430
Chi-Square	304.332	304.332
NFI	0.730	0.730

Source: Results of data analysis (2023)

The fit indices for both the Saturated and Estimated Models are consistent across all measures. The SRMR, d_ULS, d_G, and NFI values are the same for both models, indicating that the Estimated Model replicates the fit of the Saturated Model. However, the interpretation of Chi-Square is limited in this context.

Table 4. R Square

	R Square	R Square Adjusted
Computer Network Security	0.602	0.592

Source: Results of data analysis (2023)

The R-Square value for the Computer Network Security model is 0.602, indicating that approximately 60.2% of the variability in Computer Network Security can be explained by the predictors included in the model. This suggests that a substantial portion of the variability in Computer Network Security is captured by the predictors, but there may be other factors outside the model that contribute to the remaining 39.8% of the variability. The Adjusted R-Square value for Computer Network Security is 0.592, which takes into account the number of predictors in the model and provides a more conservative estimate. It suggests that 59.2% of the variability in Computer Network Security is explained by the predictors, considering the model's complexity.

4.4 Structural Model

The structural model results provide valuable insights into the relationships between Cyber Risk Management, Prevention Strategies, Threat Detection, and Computer Network Security. The presented information includes the original sample values, sample mean, standard deviation, T statistics, and p-values for each path in the structural model.

Table 5. Hypothesis Testing

	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics (|O/STDEV|)	P Values
Cyber Risk Management -> Computer Network Security	0.626	0.618	0.116	5.381	0.000
Prevention Strategies -> Computer Network Security	0.348	0.348	0.119	4.403	0.001
Threat Detection -> Computer Network Security	0.242	0.254	0.110	2.199	0.002

Source: Results of data analysis (2023)

The relationship between Cyber Risk Management and Computer Network Security is positive and statistically significant, with a path coefficient of 0.626. The sample mean for this relationship is 0.618, indicating the average value across the dataset. The standard deviation of 0.116 suggests relatively low variability in this relationship. The T statistics of 5.381 and a p-value of 0.000 further support the significance of this relationship. Similarly, Prevention Strategies also have a positive and significant relationship with Computer Network Security, with a path coefficient of 0.348. The sample mean for this relationship is 0.348, and the standard deviation is 0.119. The T statistics of 4.403 and a p-value of 0.001 confirm the significance of this relationship. Finally, Threat Detection is positively associated with Computer Network Security, with a path coefficient of 0.242. The sample mean for this relationship is 0.254, and the standard deviation is 0.110. The T statistics of 2.199 and a p-value of 0.002 indicate the statistical significance of this relationship.

Discussion

The results of this study provide valuable insights into the state of cybersecurity in Government Information Systems in Indonesia. Perceptions of cyber threats, effectiveness of threat detection mechanisms, implementation of prevention strategies, and cyber risk management practices collectively contribute to a better understanding of the cybersecurity landscape. Identification and analysis of cybersecurity hazards are critical to effectively allocate resources and determine the effectiveness of existing protections [32]. A thorough analysis of cyber incidents and vulnerabilities can provide insights into trends, patterns and common causes, such as human error, that can inform risk management planning and improve cybersecurity [33]. Prioritizing cyber vulnerabilities and using regression models can improve decision-making and enhance data integrity, confidentiality and availability [26]. Integrating cyber threat intelligence (CTI) into risk management activities can support proactive risk mitigation, provide accurate risk estimates, evaluate control effectiveness, and offer early warning of potential problems [34].

Implications for Policy and Practice

The findings have direct implications for policymakers and practitioners involved in securing government information systems. The identification of prevalent cyber threats informs the development of targeted strategies, while insights into effective prevention measures guide the enhancement of security postures. The study highlights the need for continuous training programs and the integration of human expertise alongside technological measures.

Regional Variability in Cybersecurity Posture

The regional disparities in threat perceptions suggest the importance of tailoring cybersecurity strategies to address localized challenges. Policymakers may consider region-specific cybersecurity initiatives to address the unique threat landscapes faced by government institutions in different parts of Indonesia.

Recommendations for Future Research

While this study provides a comprehensive analysis, there are avenues for further research. Future studies could explore the longitudinal evolution of cyber threats, assess the long-term effectiveness of prevention strategies, and investigate the impact of emerging technologies on threat detection mechanisms.

5. CONCLUSION

In conclusion, this research provides a comprehensive analysis of the cybersecurity landscape in Government Information Systems in Indonesia. The study highlighted the severity of perceived cyber threats and identified effective measures for threat detection, prevention, and risk management. The Structural Equation Model underscored key relationships among latent variables, emphasizing the critical role of organizational culture and human expertise in mitigating cyber risks. The findings offer actionable recommendations for policymakers and practitioners, including the need for region-specific cybersecurity initiatives and the integration of advanced technologies. This research contributes to the ongoing discourse on cybersecurity in the public sector, providing a foundation for future research, policy development, and practical implementations to fortify government information systems against evolving cyber threats.

REFERENCES

[1] P. A. Winarsasi, M. C. Thalib, M. R. Moha, and N. F. Elfikri, "State Control Of Electronic Information Resources: Role And Efforts In The Modern Context," *J. Pamator J. Ilm. Univ. Trunojoyo*, vol. 16, no. 2, pp. 405–418, 2023.

[2] N. Ishak, "Guarantee of Information and Communication Technology Application Security in Indonesia: Regulations and Challenges?," *Audit. Comp. Law J.*, vol. 4, no. 2, pp. 108–117, 2023.

[3] R. Kusumarani and R. P. A. Pramesti, "Exploring application portfolio management in Indonesia: A case study of the Indonesia agency for the assessment and application of technology," *Comput. Sci. Inf. Technol.*, vol. 4, no. 1, pp. 76–84, 2023.

[4] Y. Evitha, S. N. Sari, D. Suprayitno, and J. Irrianda, "Digital Communication Management Government of the Republic of Indonesia for Inclusive and Sustainable Economic Recovery in Indonesia," *KnE Soc. Sci.*, pp. 621–631, 2023.

[5] H. Al Asyari, "Between Freedom And Protection: A Critical Review Of Indonesia'S Cyberspace Law," *Prophet. Law Rev.*, vol. 5, no. 1, pp. 79–103, 2023.

[6] D. Junaedi and M. R. Arsyad, "Potensi Disruptif Digital di Negara Berkembang," *Com. Commun. Inf. Technol. J.*, vol. 1, no. 1, pp. 50–70, 2023.

[7] A. Dudhat and V. Agarwal, "Indonesia's Digital Economy's Development," *IAIC Trans. Sustain. Digit. Innov.*, vol. 4, no. 2, pp. 109–118, 2023.

[8] C. S. Hartati and A. Muhammad, "Combating Cybercrime and Cyberterrorism in Indonesia," *J. Hub. Int.*, vol. 11, no. 2, pp. 45–56, 2023.

[9] B. Buchanan, *The cybersecurity dilemma: Hacking, trust, and fear between nations*. Oxford University Press, 2016.

[10] M. M. Alam, A. M. Fawzi, M. M. Islam, and J. Said, "Impacts of COVID-19 pandemic on national security issues: Indonesia as a case study," *Secur. J.*, pp. 1–20, 2021.

[11] F. Cloramidine and M. Badaruddin, "Mengukur Keamanan Siber Indonesia Melalui Indikator Pilar Kerjasama Dalam Global Cybersecurity Index (GCI)," *Popul. J. Sos. dan Hum.*, vol. 8, no. 1, pp. 57–73, 2023.

[12] T. H. Fadillah, "E-Commerce: A New Media that Creates New Disasters," 2023.

[13] A. Uksan, P. Widodo, and H. Saragi, "The Role of The Kopassus 81 Unit in Dealing With Cyber Terrorism: A Conflict Resolution Effort in Indonesia," *Int. J. Soc. Sci.*, vol. 2, no. 6, pp. 2351–2356, 2023.

[14] S. Bera, L. Glenn, A. Raghavan, E. Meno, T. Cody, and P. A. Beling, "Deterring Adversarial Learning in Penetration Testing by Exploiting Domain Adaptation Theory," in *2023 Systems and Information Engineering Design Symposium (SIEDS)*, IEEE, 2023, pp. 314–318.

[15] A. Rathee, P. Malik, and M. K. Parida, "Network Intrusion Detection System using Deep Learning Techniques," in *2023 International Conference on Communication, Circuits, and Systems (IC3S)*, IEEE, 2023, pp. 1–6.

[16] P. Sharma and B. Dash, "Impact of big data analytics and ChatGPT on cybersecurity," in *2023 4th International Conference on Computing and Communication Systems (I3CS)*, IEEE, 2023, pp. 1–6.

[17] E. Drozda, "Conclusion—Final Contributions to a Research Agenda on Social Threats," *Soc. Under Threat A Pluri-Disciplinary Approach*, vol. 3, p. 217, 2020.

[18] K. Amorosa and B. Yankson, "Human Error-A Critical Contributing Factor to the Rise in Data Breaches: A Case Study of Higher Education," *HOLISTICA–Journal Bus. Public Adm.*, vol. 14, no. 1, pp. 110–132, 2023.

[19] K. Kannelønning and S. K. Katsikas, "A systematic literature review of how cybersecurity-related behavior has been assessed," *Inf. Comput. Secur.*, 2023.

[20] N. H. Al-Kumaim and S. K. Alshamsi, "Determinants of Cyberattack Prevention in UAE Financial Organizations: Assessing the Mediating Role of Cybersecurity Leadership," *Appl. Sci.*, vol. 13, no. 10, p. 5839, 2023.

[21] G. Kassar, "Exploring Cybersecurity Awareness and Resilience of SMEs amid the Sudden Shift to Remote Work during the Coronavirus Pandemic: A Pilot Study," in *ARPHA Conference Abstracts*, Pensoft Publishers, 2023, p. e107358.

[22] M. Nkongolo and M. Tokmak, "Zero-day threats detection for critical infrastructures," *arXiv Prepr. arXiv2306.06366*, 2023.

[23] S. Mahmood, M. Chadhar, and S. Firmin, "Cybersecurity challenges in blockchain technology: A scoping review," *Hum. Behav. Emerg. Technol.*, vol. 2022, pp. 1–11, 2022.

[24] I. D. Sánchez-García, J. Mejía, and T. San Feliu Gilabert, "Cybersecurity Risk Assessment: A Systematic Mapping Review, Proposal, and Validation," *Appl. Sci.*, vol. 13, no. 1, p. 395, 2022.

[25] J. Crotty and E. Daniel, "Cyber threat: its origins and consequence and the use of qualitative and quantitative methods in cyber risk assessment," *Appl. Comput. Informatics*, no. ahead-of-print, 2022.

[26] M. Angelelli, S. Arima, C. Catalano, and E. Ciavolino, "Cyber-risk Perception and Prioritization for Decision-Making and Threat Intelligence," *arXiv Prepr. arXiv2302.08348*, 2023.

[27] A. A. Latiffi, S. Mohd, N. Kasim, and M. S. Fathi, "Building information modeling (BIM) application in Malaysian construction industry," *Int. J. Constr. Eng. Manag.*, vol. 2, no. 4A, pp. 1–6, 2013.

[28] A. Ghosh, "Robustness concerns in high-dimensional data analyses and potential solutions," in *Big Data Analytics in Chemoinformatics and Bioinformatics*, Elsevier, 2023, pp. 37–60.

[29] A. Azade, R. Saini, and D. Naik, "Visual Question Answering Using Convolutional and Recurrent Neural Networks," in *International Conference on Machine Intelligence and Signal Processing*, Springer, 2022, pp. 23–33.

[30] Y. Haji-Othman and M. S. S. Yusuff, "Assessing reliability and validity of attitude construct using partial least squares structural equation modeling (PLS-SEM)," *Int. J. Acad. Res. Bus. Soc. Sci.*, vol. 12, no. 5, pp. 378–385, 2022.

[31] C. M. Davis, J. E. Tate, and T. J. Overbye, "Wide area phasor data visualization," in *2007 39th North American Power Symposium*, IEEE, 2007, pp. 246–252.

[32] T. Gebel, E. Lechtenberg-Auffarth, and C. Guhe, "About hazard and risk assessment: Regulatory approaches in assessing safety in the European Union chemicals legislation," *Reprod. Toxicol.*, vol. 28, no. 2, pp. 188–195, 2009.

[33] M. Portalatin, O. Keskin, S. Malneedi, O. Raza, and U. Tatar, "Data Analytics for Cyber Risk Analysis Utilizing Cyber Incident Datasets," in *2021 Systems and Information Engineering Design Symposium (SIEDS)*, IEEE, 2021, pp. 1–6.

[34] H. Kure and S. Islam, "Cyber threat intelligence for improving cybersecurity and risk management in critical infrastructure," *J. Univers. Comput. Sci.*, vol. 25, no. 11, pp. 1478–1502, 2019.