Managing Risks in the Adoption of Cybersecurity Technology in Manufacturing Enterprises: Identification and Assessment

Le Vinh Quang[*,†]
[1] Eastern International University, Binh Duong New City, VIETNAM
Industrial University Ho Chi Minh City, Ho Chi Minh City, VIETNAM

Tran Huu Đuc[‡], Narayan Chandra Debnath[§]
Eastern International University, Binh Duong New City, VIETNAM

Nguyen Ngoc Long[†]
Industrial University Ho Chi Minh City, Ho Chi Minh City, VIETNAM

Abstract

The adoption of cyber security technology has become an urgent challenge, particularly in the context where manufacturing enterprises increasingly rely on connectivity technologies and digitalization processes to enhance operational efficiency. However, the adoption of cybersecurity solutions poses numerous risks that require identification and assessment. This research aims to pinpoint the risks associated with the effective adoption of cybersecurity solutions in manufacturing business operations and employs the Analytic Hierarchy Process (AHP) for risk evaluation. The analysis results provide profound insights into investment priorities for cybersecurity technology and mitigation strategies within the manufacturing industry. The study focuses on analyzing risks related to strategy, organization, technology, finance, and human factors. This research contributes to existing knowledge by addressing risks in cybersecurity adoption within the manufacturing sector. These findings offer practical guidance for manufacturing organizations seeking to enhance the effectiveness of their cybersecurity deployment, allowing them to safeguard critical assets, ensure uninterrupted production processes, and protect sensitive information.

Key Words: Cybersecurity, risk management, manufacturing industry, average analytic hierarchy process, AHP.

1 Introduction

The manufacturing industry has progressively embraced digital technologies and interconnected systems, offering huge opportunities for growth and efficiency. But this shift to digitalization also brings threats and risks, particularly concerning cybersecurity (Volberda et al., [38]). Protecting vital assets, sensitive data, and guaranteeing uninterrupted production processes are crucial considerations as industrial businesses adopt Industry 4.0 technologies and digitize their operations (Ahmed et al., [1]). Given the potential ramifications of successful attacks on the industry's infrastructure and operations, the need to protect against cyber threats has never been more critical (Gunduz & Das, [18]).

As the business environment grows more complex concerning cybersecurity, risks in the manufacturing industry also increase (Yeboah-Ofori & Islam, [43]). Attackers continually develop new techniques to circumvent defenses as new technologies emerge and current ones are improved (Zlomislić et al., [45]). Due to the dynamic nature of cyber threats, cyber security actions must be continuously monitored, updated, and adjusted (Brass & Sowell, [10]), placing pressure on resources and making it important for organizations to be on full alert.

The manufacturing industry is increasingly aware of the importance of cybersecurity (Ani et al., [6]; Wells et al., [39]). However, previous studies have often provided generalized approaches and have sometimes overlooked the complexities of securing industrial control systems, supply chains, and sensitive data within this industry (Cheung et al., [12]; Knowles et al., [23]; Raimundo & Rosário, [27]). While the body of cybersecurity literature grows, there remains a pressing need for more comprehensive research to examine the complexities and risks associated with implementing strong cybersecurity technologies. Specifically, there is a critical need to further investigate the unique risks that the manufacturing sector faces.

This research study aims to fill this important gap by analyzing the adoption of cybersecurity technologies in the manufacturing industry. To assess and prioritize risks when adopting cybersecurity technologies, the Average Analytic Hierarchy Process (AHP) method has been employed. The study analyzes over 25 sub-risks affecting the adoption of cybersecurity solutions in manufacturing firms. The findings

[*] Becamex Business School.
[†] Business Administration Faculty .Email: quang.le@eiu.edu.vn, , nguyenngoclong@iuh.edu.vn.
[‡] Administration Assistant team. Email: duc.tran@eiu.edu.vn.
[§] School of Computing and Information Technology . Email: narayan.debnath@eiu.edu.vn.

reveal that organizational risks are the most critical, followed by strategy, technology, finance, and human risks. The Average AHP methodology enables a quantitative examination of the importance and impact of each risk, providing useful information regarding priorities for cybersecurity investments and mitigation solutions.

This research makes significant contributions to the field of cyber security adoption within manufacturing enterprises. In an era where manufacturing increasingly relies on connectivity technologies and digitalization to boost operational efficiency, the pressing challenge of cybersecurity adoption looms large. To address this challenge, we aimed to pinpoint and assess the inherent risks in adopting cybersecurity solutions within the manufacturing sector, employing the Analytic Hierarchy Process (AHP) for precise risk evaluation.

The paper provides a literature review in Section 2 followed by research methodology in Section 3. A detailed explanation of the results is included in Section 4. Finally, the discussion and conclusion are presented in Section 5.

2 Literature Review

The adoption of cybersecurity technology is critical for organizations to protect their digital assets and sensitive data in an increasingly interconnected world. However, this process has challenges, as various risks can hinder its successful implementation. This literature review explores key research areas related to the identification and assessment of risks that organizations face during the adoption of cybersecurity technologies.

Several research studies have been conducted to investigate the risks that firms experience while adopting cybersecurity measures. One primary challenge is the technical complexities associated with implementing cybersecurity solutions. Research by Yan et al. [42] highlights that organizations often encounter difficulties in integrating these technologies seamlessly into their existing IT infrastructure, leading to compatibility issues and potential disruptions (Kimani et al., [22]). Financial considerations play a significant role in cybersecurity technology adoption. The financial burden includes initial implementation costs and ongoing maintenance (Argaw et al., [17]; Kabanda et al., [20]). Regulatory requirements and compliance standards can limit technology adoption. Brass & Sowell [10] discuss the challenges organizations encounter in aligning cybersecurity technologies with evolving regulatory frameworks, emphasizing the need for continuous monitoring and adaptation. A shortage of skilled cybersecurity professionals can hinder technology adoption efforts. Ghobakhloo et al. [17] highlight the importance of addressing the skills gap and ensuring organizations have the expertise required for effective technology deployment. The literature highlights a range of challenges and risks organizations encounter during the adoption of cybersecurity technologies. Understanding and addressing these risks is essential for successful technology implementation and improved cybersecurity posture.

Despite some existing research on risk assessment in the adoption of cybersecurity technology, there is a need for a comprehensive study that identifies and evaluates the full spectrum of key risks and sub-risks, transcending beyond the realms of finance, technology, or human factors. As a result, the purpose of this study is to identify and thoroughly analyze these risks using the research methodology presented by Kabra et al. [21], originally used to highlight challenges in the implementation of digital technologies.

The Analytical Hierarchy Process (AHP) is a well-known decision-making process that offers a systematic strategy for evaluating difficult situations with various criteria (Albayrak & Erensal, [4]). In the context of the risks associated with implementing cybersecurity technology in the manufacturing business, AHP provides a useful framework for quantitatively measuring the relative relevance of various risks. Discussing with experts and using AHP enables developing a prioritized list of risks, helping manufacturers allocate resources to the most critical issues. AHP is especially useful for evaluating problems in Information and Communication Technology (ICT) applications because it gives you a structured way to figure out how important these problems are based on several criteria (Kabra et al., [21]). However, a scarcity of research utilizing the Analytical Hierarchy Process (AHP) method for the analysis of cybersecurity implementation issues persists.

3 Research Methodology

This study utilizes the Average Analytic Hierarchy Process (AAHP) method to evaluate and prioritize the key risks influencing cybersecurity technology adoption in manufacturing enterprises.

3.1 Risk Identification

An extensive literature review of scholarly articles was first conducted to identify an initial set of cybersecurity adoption risk factors. These were mapped to the framework proposed by Kabra et al. [21] which categorizes risks into strategic, organizational, human, financial, and technological categories. Additional relevant risks were added based on the literature.

Input from a panel of 10 subject matter experts was then gathered through interviews to validate and refine the identified risks. The experts included CEOs of IT services companies, manufacturing company IT department heads, and university professors specializing in cybersecurity and information systems. Their insights helped modify the risk framework and ensure its applicability to the manufacturing sector.

3.2 AHP and Average AHP

Analytic Hierarchy Process (AHP) is a Multi-criteria decision-making (MCDM) technique proposed by (Wind & Saaty, [41]), which involves pairwise comparisons of multiple criteria to determine their relative importance. The AHP approach applied in this research consists of the following main steps:

- AHP Model Development: a hierarchical model was developed with the overall goal of evaluating cybersecurity adoption risks at the top level. The next level consisted of the 5 main risk categories. The lowest level contained the 25 sub-risk factors identified through the literature review and expert input.
- Pairwise Comparison Matrices: A questionnaire was designed to gather expert assessments of the relative importance of risks through AHP pairwise comparisons. Utilize a scale ranging from 1 (equal importance) to 9 (significantly more important) for this purpose and gather the resulting data.
- The eigenvector method was utilized to calculate the local weights of the sub-risks from the comparison matrices (Wind & Saaty, [41]). Global weights were obtained by multiplying local weights by the weights of their parent criteria.
- Consistency Verification: The consistency ratio (CR) was calculated to verify judgment consistency. CR ratios exceeding 0.10 indicated inconsistent comparisons. Any inconsistent matrices were discarded.

These steps will enable the calculation of weights for criteria, sub-criteria, and options based on the results of pairwise comparisons. In this research, we suggested the percentage scale (from 1 to 9) for the pair-wise comparison shown in Figure 1.

AHP comparison tables are generated for each expert to compute the relative weights of criteria, which are referred to as AHP values. If there are numerous experts (n experts), each expert's assessment (AHPEi) is performed, and the average AHP value of the experts (A(AHP)) is determined using the arithmetic mean, as shown in Equation (1).

$$A(AHP) = \frac{\sum_{i=1}^{n} AHPE_i}{n} \tag{1}$$

The AAHP risk weights were analyzed to determine priorities for cybersecurity adoption. A higher weight indicates a higher priority risk factor. This AAHP methodology enables a quantitative, systematic multi-expert evaluation of the key cybersecurity adoption risks for manufacturing enterprises.

4 Results

4.1 Identifying Challenges in Cyber Security Solutions Adoption

This study created a multi-hierarchical structure of cybersecurity adoption risks based on the technological adoption challenges stated by (Kabra et al., [21]). This was strengthened by incorporating recent literature insights and input from ten experts, including IT company CEOs, manufacturing IT managers, and ICT professors. The risks associated with cyber security technology advice will be classified into two tiers, as shown in Table 1.

4.2 Prioritization of the Cybersecurity Solutions Adoption with A(AHP)

The A(AHP) questionnaire was designed for evaluating and prioritizing the five key risk factors and their related sub-factors. As previously stated, data was gathered using the A(AHP) questionnaire. The survey included the participation of ten cybersecurity experts. The experts were instructed to use numerical scales ranging from 1 to 9 while making their choices to assess the priority of implementing cybersecurity . The questionnaire, which included a decision-making process and paired comparisons, took each participant between forty and fifty minutes to complete. Table 2 shows an example of paired criterion comparisons for a specific target defined by expert No.1. Meanwhile, Figure 1 depicts the attribution of importance on a scale of 1 to 9. As transversal values, the reciprocal values of these significance ratings were employed (aij = 1/aji). According to Expert No. 1, Strategy was three times more significant than Organization, providing a transversal value of one-third. Organization, on the other hand, was deemed three times less significant than Strategy, resulting in a reciprocal ratio of aij = 1/aji.

We meticulously developed a pairwise comparison matrix for the numerous risk variables in Table 3. This matrix was generated by dividing each element within it by the total of its column values. To better demonstrate this technique, consider an individual item in the matrix, such as 0.560. This number was calculated by dividing 1 (from Table 2) by the cumulative sum of column values for that specific entry, which is the sum of 1.00, 0.33, 0.11, 0.14, and 0.20, for a total of 1.79 (from Table 2).

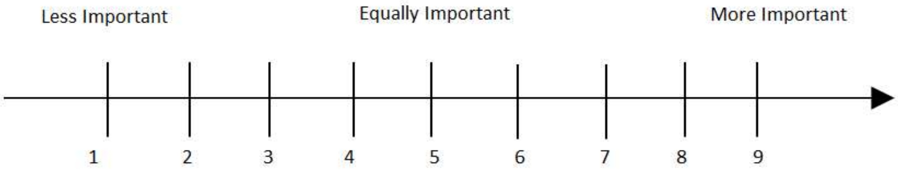

Figure 1: Shows the percentage scale (1–9) for pair-wise comparisons

Table 1: Identification of risk factors from the previous literature

Criteria	Sub-risks	Relevant studies
Main risks	Strategic risks	Gcaza & von Solms [16]
	Organizational risks	Kabanda et al. [20]
	Human risks	Bowen et al. [9]
	Financial risks	Kabanda et al. [20]
	Technological risks	De Bruijn & Janssen [13]
Strategy (S)	Lack of policies to adopt technology	Stewart & Jürjens [32]
	Inadequate policy awareness and support from the government	Kraemer et al. [24]
	Lack of management vision	Tsohou et al. [37]
	Lack of cross-organization development program	Zissis & Lekkas [44]
	Lack of supply chain understanding	Yeboah-Ofori & Islam [43]
Organization (O)	Conflicting short-term focus goal-oriented culture	Zissis & Lekkas [44]
	Not inviting end-user input	Zissis & Lekkas [44]
	Lack of cybersecurity personnel	Szczepaniuk et al. [33]
	Lack of pressure from other organizations	Singh & Alshammari [30]
	Lack of transparency in the utilization of funds	Sirisha et al. [31]
Human (H)	Lack of skills to use cybersecurity solutions	Tam et al. [34]
	Lack of education and training for the employees	Akter et al. [2]
	Lack of benchmarking about the knowledge of cybersecurity solutions	Holstein et al. [19]
	Workforce resistance to change	P. Kumar et al. [26]
	Lack of motivation to use cybersecurity solutions	Wessels et al. [40]
Finance (F)	Donor’s support	Chang & Coppe [11]
	Lack of funds for investment in technology	Fielder et al. [15]
	High Cost	Alsuwian et al. [5]
	Competition for funding	Balon & Baggili [8]
	Fundraising expenses	Eusanio & Rosenbaum [14]
Technology (T)	Lack of awareness about exact technological solutions	Alahmari & Duncan [3]
	Lack of cybersecurity solutions enabling infrastructure	A. Kumar [25]
	Lack of customization	Alahmari & Duncan [3]
	Frequent updates of technology	Tawalbeh et al. [35]
	Incompatibility in cybersecurity facilities linked with different organizations	Ani et al. [6]

Table 2: Pairwise comparison matrix of expert No. 1's decision criteria (Risk factors) with respect to the goals

Criteria	S	O	H	F	T
S	1.00	3.00	9.00	7.00	5.00
O	0.33	1.00	7.00	5.00	3.00
H	0.11	0.14	1.00	0.33	0.20
F	0.14	0.20	3.00	1.00	1.00
T	0.20	0.33	5.00	1.00	1.00

Table 3: Priorities of main risk factors

	S	O	H	F	T	Weight	Rank
S	0.560	0.642	0.360	0.488	0.490	0.508	1
O	0.187	0.214	0.280	0.349	0.294	0.265	2
H	0.062	0.031	0.040	0.023	0.020	0.035	5
F	0.080	0.043	0.120	0.070	0.098	0.082	4
T	0.112	0.071	0.200	0.070	0.098	0.110	3

After completing the matrix computation, we calculated the row averages, which are critical in calculating the Eigenvectors or relative weights of the criterion, in this case, the risk factors listed in Table 3. To illustrate, consider the relative importance of a strategic problem. This weight was determined by adding the numbers in each row, namely 0.560, 0.642, 0.360, 0.488, and 0.490, and then dividing the total number of challenge elements or criteria, which in this case is 6. As a consequence, a strategic challenge's relative weight was judged to be 0.508. In this manner, we meticulously established a framework for assessing the significance and relative importance of various risk factors, providing a valuable tool for decision-makers and experts in the field to prioritize and address these factors effectively.

We employed Saaty [29] criteria to evaluate the consistency of the comparison matrix, and in doing so, we determined both the Consistency Index (C.I.) and the Consistency Ratio (C.R.). The C.I. was computed using the formula C.I. = (max - n) / (n - 1), where 'max' represents the largest eigenvalue of the pairwise comparison matrix, and 'n' is the number of criteria being compared. This was a crucial step in ensuring the validity of our assessment. Furthermore, the C.R. was determined by dividing the C.I. by the Random Consistency Index (R.I.), which is a pre-established value. For a five-by-five matrix, the appropriate R.I. value is set at 1.12, as indicated in Table 4 for reference. In our evaluation, it was imperative to consider that an assessment is deemed satisfactory if the C.R. does not exceed the threshold of 0.10 (10 percent), as stipulated by Saaty [29]. With these procedures in mind, we meticulously calculated the C.R. using the prescribed technique, and the resulting C.R. was found to be 0.072348987. This value did not surpass the 0.10 (10 percent) criterion. Consequently, we can conclude that the judgments provided by the experts were relatively consistent, instilling confidence in the appropriateness of these criteria for making informed decisions.

Ten experts utilized the A(AHP) approach to assess each of the adoption risks in Table 1 to itself. The average score was used to establish the priority of each adoption risk level, as indicated in Table 5. The arithmetic mean of the experts' A(AHP) values was used to get the AAHP value. To show, the average AHP of the strategic risk in the table was determined by adding the rows (0.508+ 0.508+ 0.529+ 0.264 + 0.035 + 0.070 + 0.508 + 0.260 + 0.278 + 0.236), providing a result of 0.320 and placing second. Table 6 highlights the findings of all risk factors' priority, including major and sub-risks.

5 Discussion

The primary objective of this study was to identify and assess the key risks influencing the adoption of cybersecurity technology. After conducting an extensive review of the literature on cybersecurity adoption risks, a total of 25 risk factors were identified. Subsequently, a survey was designed to gather input from professionals regarding the impact of these risks. An Analytic Hierarchy Process (AHP) model was constructed to analyze the data.

The AHP analysis revealed that among the main criteria, organizational risks emerged as the most significant challenges in the adoption of cybersecurity solutions. Within organizational risks, the absence of pressure from external organizations mandating the use of cybersecurity is a high-ranked risk factor that can delay this process. This outcome suggests that the lack of external pressure may lead to a reduced sense of urgency in adopting cybersecurity solutions. Additionally, insufficient motivation from peer organizations can undermine the prioritization and importance of cybersecurity implementation. These findings align with the research by Kabanda et al. [20], who highlight that external factors play a reinforcing role in the limited adoption of cybersecurity practices.

Table 4: Average random consistency index (R.I.)

n	1	2	3	4	5	6	7	8	9	10
R.I	0.00	0.00	0.58	0.90	1.12	1.24	1.32	1.41	1.45	1.49
n	11	12	13	14	15					
R.I	1.51	1.48	1.56	1.57	1.58					

Table 5: Average of the AHP values of the experts for major risks

	Criteria weights											
	RES 1	**RES 2**	**RES 3**	**RES 4**	**RES 5**	**RES 6**	**RES 7**	**RES 8**	**RES 9**	**RES 10**	**Average**	**Rank**
SR	0.508	0.508	0.529	0.264	0.035	0.070	0.508	0.260	0.278	0.236	0.335	2
OR	0.265	0.264	0.185	0.505	0.503	0.502	0.264	0.503	0.410	0.448	0.374	1
HR	0.035	0.070	0.038	0.137	0.068	0.039	0.070	0.035	0.064	0.069	0.061	5
FR	0.082	0.038	0.077	0.045	0.134	0.223	0.038	0.068	0.098	0.101	0.088	4
TR	0.110	0.120	0.170	0.049	0.260	0.166	0.120	0.134	0.150	0.147	0.141	3

Table 6: Average of the AHP values of the experts for major risks

Criteria	Weights	Ranks
Main Factors		
Strategic Risk	0.320	2
Organizational Risk	0.385	1
Human Risk	0.062	5
Financial Risk	0.090	4
Technological Risk	0.143	3
Sub-Challenge Factors (Strategic)		
Lack of policies to adopt technology	0.162	4
Inadequate policy awareness and support from government	0.095	5
Lack of management vision	0.208	3
Lack of cross-organization development program	0.285	1
Lack of supply chain understanding	0.249	2
Sub-Challenge Factors (Organizational)		
Conflicting short-term focus goal-oriented culture	0.218	2
Not inviting end-user input	0.153	5
Lack of cybersecurity personnel	0.205	3
Lack of pressure from other organizations	0.224	1
Lack of transparency in the utilization of funds	0.200	4
Sub-Challenge Factors (Human)		
Lack of skills to use cybersecurity	0.257	2
Lack of education and training to the employees	0.169	4
Lack of benchmarking about the knowledge of cybersecurity	0.179	3
Workforce resistance to change	0.273	1
Lack of motivation to use cybersecurity	0.122	5
Sub-Challenge Factors (Financial)		
Donors support	0.205	2
Lack of funds for investment in technology	0.345	1
High Cost	0.115	5
Competition for funding	0.150	4
Fundraising expenses	0.185	3
Sub-Challenge Factors (Technological)		
Lack of awareness about exact technological solutions	0.226	2
Lack of cybersecurity enabling infrastructure	0.178	4
Lack of customization	0.145	5
Frequent updates of technology	0.261	1
Incompatibility in cybersecurity facilities linked with different organizations	0.190	3

In contrast to research focused on technology usage in manufacturing, one of the significant implementation barriers is related to financial or strategic risks (Kabra et al., [21]). Nonetheless, the current investigation indicates that financial challenges are ranked as only the fourth most significant. This suggests that the market provides a wide range of cybersecurity solutions, indicating that financial limitations may not serve as a major impediment for businesses when it comes to adopting these solutions. Most surprisingly, risks associated with human factors are considered the least prioritized which contradicts the findings of (Triplett, [36]), who highlighted humans as the weakest link in data security. Triplett identified specific careless and unintentional behaviors that were made worse by the lack of awareness among both leaders and employees.

In terms of technical risks, the findings of this study closely reflect previous studies undertaken in developing-country small and medium-sized firms (SMEs). Frequent updates of technology are ranked as the number one criterion in assessing technological risks. SMEs generally use simpler systems and infrequently update software and technology, which may make it difficult to implement rigorous protections (Rawindaran et al., [28]).

6 Conclusions, Limitations and Future Work

In conclusion, this study has shed light on the critical risks influencing the adoption of cybersecurity technology in organizations. Through an extensive literature review and a comprehensive survey, we identified 25 key risk factors and employed the AAHP to analyze their significance. Our findings highlight that organizational risks specifically the lack of external pressure mandating cybersecurity and the absence of motivation from peer organizations, pose significant challenges in the adoption of cybersecurity solutions. These results underscore the importance of external influences in shaping cybersecurity practices within organizations.

While this study provides useful insights into cybersecurity adoption risks, some limitations exist. Firstly, the sample of experts consulted was small at only 10 participants. A larger and more diverse expert panel could validate the results further. Secondly, the study focused solely on the manufacturing industry. Expanding the research across other sectors could reveal additional risks and challenges. Finally, the AHP technique has some shortcomings in terms of potential inconsistencies. Utilizing other multi-criteria decision-making methods like ANP could strengthen the analysis.

According to the findings, the pressure from external organizations is insufficient to persuade manufacturing enterprises to embrace cybersecurity solutions. Future investigations should further examine the role of external pressures from organizations and stakeholders in driving the urgency of implementing cybersecurity solutions. Furthermore, a shortage of funds for technological investment is viewed as a risk factor impacting this process. As a result, the recommendation for future study is to concentrate on solutions that may have a greater impact on focused companies and to give financing assistance to manufacturing organizations to improve cybersecurity in the present digital environment. Additionally, investigating differences in risk priorities across company sizes and developing vs. developed countries could provide more nuanced insights. Lastly, strategies for fostering collaboration among peer organizations to collectively elevate the importance of cybersecurity implementation and facilitate the sharing of best practices should be considered.

Acknowledgments

This research is financially supported by Eastern International University, Binh Duong Province, Vietnam.

References

[1] S. F. Ahmed, M. S. Bin Alam, M. Hoque, A. Lameesa, S. Afrin, T. Farah, M. Kabir, G. M Shafiullah,.and S. M. Muyeen, "Industrial Internet of Things Enabled Technologies, Challenges, and Future Directions, " *Computers and Electrical Engineering*, 110:16 pp., July 2023, https://doi.org/10.1016/j.compeleceng.2023.108847.

[2] S. Akter, M. R. Uddin, S. Sajib, W. J. T. Lee, K. Michael, and M. A. Hossain,. "Reconceptualizing Cybersecurity Awareness Capability in the Data-Driven Digital Economy," *Annals of Operations Research*. https://doi.org/10.1007/s10479-022-04844-8, 2022.

[3] A. Alahmari and B. Duncan, "Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence," *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, Cyber SA 2020*, *March 2021*. https://doi.org/10.1109/CyberSA49311.2020.9139638.

[4] E. Albayrak and Y. C. Erensal, "Using Analytic Hierarchy Process (AHP) to Improve Human Performance: An Application of Multiple Criteria Decision Making Problem," *Journal of Intelligent Manufacturing*, 15(4):491-503, 2004, https://doi.org/10.1023/B:JIMS.0000034112.00652.4c.

[5] T. Alsuwian, A. Shahid Butt, and A. A. Amin, "Smart Grid Cyber Security Enhancement: Challenges and Solutions—A Review," *Sustainability (Switzerland)*, 14(21):1-21, 2022, https://doi.org/10.3390/su142114226.

[6] U. P. D. Ani, H. (Mary) He, and A. Tiwari, "Review of Cybersecurity Issues in Industrial Critical Infrastructure: Manufacturing in Perspective," *Journal of Cyber Security Technology*, 1(1):32-74, 2017, https://doi.org/10.1080/23742917.2016.1252211.

[7] S. T. Argaw, J. R. Troncoso-Pastoriza, D. Lacey, M. V. Florin, F. Calcavecchia, D. Anderson, W Burleson,. J. M. Vogel, C. O'Leary, B. Eshaya-Chauvin, and A. Flahault, "Cybersecurity of Hospitals: Discussing the Challenges and Working Towards Mitigating the Risks," *BMC Medical Informatics and Decision Making*, 20(1):1-10, 2020, https://doi.org/10.1186/s12911-020-01161-7.

[8] T. Balon and I. Baggili, "Cybercompetitions: A Survey of Competitions, Tools, and Systems to Support Cybersecurity Education," *Education and Information Technologies*, pp. 1-33, 2023.

[9] B. M. Bowen, R. Devarajan and S. Stolfo, "Measuring the Human Factor of Cyber Security," *2011 IEEE International Conference on Technologies for Homeland Security, HST 2011*, pp. 230-235, 2011. https://doi.org/10.1109/THS.2011.6107876.

[10] I. Brass and J. H. Sowell, "Adaptive governance for the Internet of Things: Coping with emerging security risks," *Regulation and Governance*, 15(4):1092-1110, 2021. https://doi.org/10.1111/rego.12343.

[11] L. Y. C. Chang and N. Coppel, "Building Cybersecurity Awareness in a Developing Country: Lessons from Myanmar," *Computers & Security*, 97:101959, 2020.

[12] K. F. Cheung, M. G. H. Bell and J. Bhattacharjya, "Cybersecurity in Logistics and Supply Chain Management: An Overview and Future Research Directions," *Transportation Research Part E: Logistics and Transportation Review*, *146*, July 2020, 102217. https://doi.org/10.1016/j.tre.2020.102217.

[13] H. de Bruijn and M. Janssen, "Building Cybersecurity Awareness: The Need for Evidence-Based Framing Strategies," *Government Information Quarterly*, 34(1):1-7, 2017, https://doi.org/10.1016/j.giq.2017.02.007.

[14] J. M. Eusanio and D. J. Rosenbaum, "Technology

Considerations for Not-for-Profit Organizations," *The CPA Journal*, 89(4):13-15, 2019.

[15] A. Fielder, E. Panaousis, P. Malacaria, C. Hankin, and F. Smeraldi, "Decision Support Approaches for Cyber Security Investment," *Decision Support Systems*, 86:13-23, 2016, https://doi.org/10.1016/j.dss.2016.02.012.

[16] N. Gcaza and R. von Solms, "A Strategy for a Cybersecurity Culture: A South African Perspective," *Electronic Journal of Information Systems in Developing Countries*, 80(1):1-17, 2017, https://doi.org/10.1002/j.1681-4835.2017.tb00590.x.

[17] M. Ghobakhloo, M. Iranmanesh, M. Vilkas, A. Grybauskas and A. Amran, "Drivers and Barriers of Industry 4.0 Technology Adoption Among Manufacturing SMEs: a Systematic Review and Transformation Roadmap," *Journal of Manufacturing Technology Management*, 33(6):1029-1058, 2022, https://doi.org/10.1108/JMTM-12-2021-0505.

[18] M. Z. Gunduz and R. Das, "Cyber-Security on Smart Grid: Threats and Potential Solutions," *Computer Networks*, 169, 2020, 107094. https://doi.org/10.1016/j.comnet.2019.107094.

[19] D. Holstein, T. W. Cease and M. G. Seewald, "Application and Management of Cybersecurity Measures for Protection and Control," *2015 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*, pp. 76-83, 2015.

[20] S. Kabanda, M. Tanner and C. Kent, "Exploring SME Cybersecurity Practices in Developing Countries," *Journal of Organizational Computing and Electronic Commerce*, *28*(3):269-282, 2018. https://doi.org/10.1080/10919392. 2018.1484598.

[21] G. Kabra, A. Ramesh, V. Jain, and P. Akhtar, "Barriers to Information and Digital Technology Adoption in Humanitarian Supply Chain Management: A Fuzzy AHP Approach," *Journal of Enterprise Information Management*, 36(2):505-527, 2023, https://doi.org/10.1108/JEIM-10-2021-0456.

[22] K. Kimani, V. Oduol, and K. Langat, "Cyber Security Challenges for IoT-based Smart Grid Networks," *International Journal of Critical Infrastructure Protection*, 25:36-49, 2019, https://doi.org/10.1016/j.ijcip.2019.01.001.

[23] W. Knowles, D. Prince, D. Hutchison, J. F. P. Disso, and K. Jones, "A Survey of Cyber Security Management in Industrial Control Systems," *International Journal of Critical Infrastructure Protection*, 9:52-80, 2015, https://doi.org/10.1016/j.ijcip.2015.02.002.

[24] S. Kraemer, P. Carayon, and J. Clem, "Human and Organizational Factors in computer and information security: Pathways to vulnerabilities," *Computers and Security*, *28*(7):509-520, 2009, https://doi.org/10.1016/j.cose.2009.04.006.

[25] A. Kumar,. "Cyber Physical Systems (CPSs) – Opportunities and Challenges for Improving Cyber Security," *International Journal of Computer Applications*, 137(14):19-27, 2016, https://doi.org/10.5120/ijca2016908877.

[26] P. Kumar, J. Bhamu, and K. S. Sangwan, "Analysis of Barriers to Industry 4.0 Adoption in Manufacturing Organizations: An ISM Approach," *Procedia CIRP*, *98*: 85–90, March 2021, https://doi.org/10.1016/j.procir.2021.01.010.

[27] R. J. Raimundo and A. T. Rosário, "Cybersecurity in the Internet of Things in Industrial Management," *Applied Sciences (Switzerland)*, 12(3):19 pp., 2022, https://doi.org/10.3390/app12031598.

[28] N. Rawindaran, A. Jayal, E Prakash, and C. Hewage, "Perspective of Small and Medium Enterprise (SME's) and their Relationship with Government in Overcoming Cybersecurity Challenges and Barriers in Wales," *International Journal of Information Management Data Insights*, *3*(2):100191, 2023, https://doi.org/10.1016/j.jjimei.2023.100191.

[29] T. L. Saaty, "Decision Making — the Analytic Hierarchy and Network Processes (AHP/ANP)," *Journal of Systems Science and Systems Engineering*, 13(1):1-35, 2004, https://doi.org/10.1007/s11518-006-0151-5.

[30] H. P. Singh and T. S. Alshammari, "An Institutional Theory Perspective on Developing a Cyber Security Legal Framework: A Case of Saudi Arabia," *Beijing Law Review*, 11(03):637-650, 2020, https://doi.org/10.4236/blr.2020.113039.

[31] N. S. Sirisha, T. Agarwal, R. Monde, R. Yadav, and R. Hande, "Proposed Solution for Trackable Donations using Blockchain," *2019 International Conference on Nascent Technologies in Engineering, ICNTE 2019 - Proceedings*, *Icnte*, pp. 1-5, 2019, https://doi.org/10.1109/ICNTE44896.2019.8946019.

[32] H. Stewart and J. Jürjens, "Information Security Management and the Human Aspect in Organizations," *Information and Computer Security*, 25(5):494-534, 2017, https://doi.org/10.1108/ICS-07-2016-0054.

[33] E. K. Szczepaniuk, H. Szczepaniuk, T. Rokicki, and B. Klepacki, "Information Security Assessment in Public Administration," *Computers and Security*, 90:11 pp. (2020). https://doi.org/10.1016/j.cose.2019.101709.

[34] T. Tam, A. Rao, and J. Hall, "The Good, the Bad and the Missing: A Narrative Review of Cyber-Security Implications for Australian Small Businesses," *Computers and Security*, 109:1-56, 2021, https://doi.org/10.1016/j.cose.2021.102385.

[35] L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "Applied Sciences IoT Privacy and Security : Challenges and Solutions," *Mdpi*, pp. 1-17, 2020.

[36] W. J. Triplett, "Addressing Human Factors in Cybersecurity Leadership," *Journal of Cybersecurity and Privacy*, 2(3):573–586, 2022. https://doi.org/10.3390/jcp2030029.

[37] A. Tsohou, M. Karyda, S. Kokolakis, and E. Kiountouzis, "Managing the Introduction of Information Security Awareness Programmes in Organizations," *European*

Journal of Information Systems, 24(1):38-58, 2015, https://doi.org/10.1057/ejis.2013.27.

[38] H. W. Volberda, S. Khanagha, C. Baden-Fuller, O. R. Mihalache, and J. Birkinshaw, "Strategizing in a Digital World: Overcoming Cognitive Barriers, Reconfiguring Routines and Introducing New Organizational Forms," *Long Range Planning*, 54(5):102110, 2021, https://doi.org/10.1016/j.lrp.2021.102110.

[39] L. J. Wells, J. A. Camelio, C. B. Williams, and J. White, "Cyber-Physical Security Challenges in Manufacturing Systems," *Manufacturing Letters*, 2(2):74-77, 2014, https://doi.org/10.1016/j.mfglet.2014.01.005.

[40] M. Wessels, P. van den Brink, T. Verburgh, B. Cadet, and T. van Ruijven, "Understanding Incentives for Cybersecurity Investments: Development and Application of a Typology," *Digital Business*, 1(2):100014, 2021, https://doi.org/10.1016/j.digbus.2021.100014.

[41] Y. Wind and T. L. Saaty, "8002_Marketing_Applications_of_the_Analytic.pdf," *Management Science*, 26(7):641-658, 1980.

[42] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A Survey on Cyber Security for Smart Grid Communications," *IEEE Communications Surveys and Tutorials*, 14(4):998-1010, 2012, https://doi.org/10.1109/SURV.2012.010912.00035.

[43] A. Yeboah-Ofori and S. Islam, "Cyber Security Threat Modeling for Supply Chain Organizational Environments," *Future Internet*, 11(3):25 pp. 2019, https://doi.org/10.3390/fi11030063.

[44] D. Zissis,and D. Lekkas, "Addressing Cloud Computing Security Issues," *Future Generation Computer Systems*, *28*(3):583-592, 2012, https://doi.org/10.1016/j.future.2010.12.006.

[45] V. Zlomislić, K. Fertalj, and V. Sruk, "Denial of service attacks, defences and research challenges," *Cluster Computing*, 20(1):661–671, 2017, https://doi.org/10.1007/s10586-017-0730-x.

Le Vinh Quang (photo not available) is a senior lecturer at Becamex Business School, Eastern International University. He obtained his master degree in Business specializing in Technology Management, from Western Sydney University and is currently pursuing a Ph.D in Faculty of Business Administration at Industrial University of Ho Chi Minh City. His research interests encompass supply chain management, technology management, and enterprise risk management.

Tran Huu Duc (photo not available) is working as an Assistant to the University Council and Board of Presidents at Eastern International University in Vietnam. He graduated with a bachelor's degree in Supply Chain Management from Eastern International University. Currently, he focuses on research related to facilities management and technology adoption.

Narayan C. Debnath (photo not available) is currently the Founding Dean of the School of Computing and Information Technology at Eastern International University, Vietnam. He is also serving as the Head of the Department of Software Engineering at Eastern International University, Vietnam. Formerly, Dr. Debnath served as a Full Professor of Computer Science at Winona State University, Minnesota, USA for 28 years, and the elected Chairperson of the Computer Science Department at Winona State University for 7 years. Dr. Debnath has been the Director of the International Society for Computers and their Applications (ISCA), USA since 2014. Professor Debnath made significant contributions in teaching, research, and services across the academic and professional communities. He has made original research contributions in software engineering, artificial intelligence and applications, and information science; technology, and engineering. He is an author or co-author of over 500 research paper publications in numerous refereed journals and conference proceedings in Computer Science, Information Science, Information Technology, System Sciences, Mathematics, and Electrical Engineering. He is also an author of over 15 books published by well-known international publishers including Elsevier, CRC, Wiley, Bentham Science, River Publishing, and Springer. Dr. Debnath has made numerous teaching, research, and invited keynote presentations at various international conferences, industries, and teaching and research institutions in Africa, Asia, Australia, Europe, North America, and South America. He has been a visiting professor at universities in Argentina, China, India, Sudan, and Taiwan. He has been maintaining an active research and professional collaborations with many universities, faculty, scholars, professionals, and practitioners across the globe. Dr. Debnath is an active member of the IEEE, IEEE Computer Society, and a Senior Member of the International Society for Computers and their Applications (ISCA), USA.

Nguyen Ngoc Long (photo not available) is currently serving as the Vice Dean of the Faculty of Business Administration at the Industrial University of Ho Chi Minh City. He earned his doctorate degree from Hunan University in China in 2017. His research interests encompass behavior, leadership, and risk management.