Providing a Cybersecurity Evaluation Model for Small and Medium Enterprises (SME) (Case Study: Hamoon Nayzeh Pipe Manufacturing Company)

Meysam Halvaei Hosnaroudi [1], Safiyeh Mehri Nejad* [2],Abdollah AminMousavi[3]

1.Department of Technology Management, Central Tehran Branch, Islamic Azad University, Tehran, Iran.
2.Department of Financial Management, Central Tehran Branch, Islamic Azad University, Tehran, Iran (Corresponding author).
3.Department of Technology Management, Central Tehran Branch, Islamic Azad University, Tehran, Iran.

*** Corresponding author email address**: s.mehrenejad@gmail.com

Received: 2024-07-17 **Reviewed:** 2024-08-03 **Revised:** 2024-08-28 **Accepted:** 2024-09-18 **Published:** 2024-12-30

Abstract

In this study, an effort has been made to design and present a comprehensive and systematic framework for evaluating cybersecurity in small and medium enterprises (SMEs) based on the meta-synthesis approach. This research aims to identify existing models and provide solutions for assessing and improving the cybersecurity status in such companies. The present study is qualitative and utilizes the meta-synthesis approach to analyze and integrate the results of previous research. In this research, all articles published in reputable scientific journals (ISI), books, theses, and internal and external scientific reports related to cybersecurity in SMEs, especially in areas such as cyber threats, data protection, risk management, and security solutions, from 2015 to 2024 were collected and analyzed. After coding and analysis, key factors effective in evaluating the cybersecurity of SMEs were identified. The results from the data analysis indicate that cybersecurity evaluation in SMEs requires a multidimensional approach that, in addition to addressing cyber threats, also considers cultural and organizational aspects. The proposed framework includes various components such as cyber risk assessment, vulnerability identification, evaluating training needs and employee awareness, analyzing cyber threats and attacks, and developing comprehensive security policies. Moreover, the proposed model emphasizes the importance of establishing resilient security infrastructures against threats and utilizing advanced technological tools such as Intrusion Detection Systems (IDS), firewalls, and data encryption.

Keywords: *security, cybersecurity, small and medium enterprises (SME), cybersecurity evaluation, meta-synthesis*

How to cite this article:

Halvaei Hosnaroudi M , Mehri Nejad S, Amin Mousavi A. (2024). Providing a Cybersecurity Evaluation Model for Small and Medium Enterprises (SME) (Case Study: Hamoon Nayzeh Pipe Manufacturing Company). Management Strategies and Engineering Sciences, 6(5), 36-42.

1. Introduction

Over time and with the advancement of science and technology, the evolution of cybersecurity has undergone changes and transformations. Since the invention of the first computer and storage equipment, the concern for data preservation and the security of these devices has always existed. Although this concern has taken on a different form with the passage of time and resulting advancements, it has continued to carry considerations [1]. With the emergence of the digital age and the production of new equipment, maintaining the security of these devices has remained highly important and worthy of attention. In the digital information era, the need for governments and companies for information technology in order to optimize operations, streamline business processes, and provide remote services has increased. Consequently, information technology and information and cybersecurity have also gained a special position in the digital arena. Today, the ability to penetrate the cyber space is considered one of the most important sources of power in the 21st century. Therefore, governmental and non-governmental actors utilize this power in the cyber space or the physical space to achieve military, ideological, and social objectives [2, 3].

Researchers state that information security means the protection of information and information systems and platforms from unauthorized activities. Today, if an organization's confidential information or that of its customers is hacked, it is just as important (or even more so) that the organization's systems are hacked and its service delivery is halted [4, 5]. Given what has been stated so far, it can be concluded that if cybersecurity is compromised, it not only threatens the occurrence of irreparable material damages (communication and information systems) to organizations but also makes its non-material damages (information and customer privacy) unavoidable [6, 7]. This issue has become so important that reputable companies and organizations have taken steps to establish an educational institution in the cyber domain to train capable personnel and plan for their future in cybersecurity. Therefore, while monitoring and measuring the organization's cybersecurity status, an enhancement program must also be considered (Kumar & Gupta, 2023). This program must be aligned and planned in accordance with the organization's strategic objectives. Consequently, alongside organizational maturity, there must also be consideration for the maturity of the organization's information and cybersecurity. Based on the above explanations and considering that assessing and measuring the cybersecurity maturity level of SMEs to evaluate and understand their cybersecurity strengths and weaknesses is a very difficult and complex issue, there is a need for research and the provision of a cybersecurity evaluation model [8, 9]. The cybersecurity maturity evaluation model is an approach that can be used to measure the organization's existing security status and, by comparing this status with the desired state, perform a gap analysis and outline the path for the organization to achieve the desired status. Various theorists have defined the concept of information security and cybersecurity. According to Whitman, information security includes the confidentiality, integrity, and availability of data during storage, processing, and transmission, where disruption in any of these components can have serious impacts on the performance of governments, companies, and society (Whitman, 2013). Cybercrimes are a growing industry, with their costs estimated to range between $375 billion and $575 billion for the global economy [1, 10]. To prevent these cybercrimes, it is necessary to protect companies and service-providing organizations from cyber attack risks by using extensive and up-to-date cybersecurity measures [11-14]. Cybersecurity and information security share many common points, but they are distinct from each other. According to the ISO 27032 standard, information security focuses on data protection, while cybersecurity focuses on preventing or stopping cyber attacks by enhancing application security, network security, and internet security. In another definition, cybersecurity is a set of tools, policies, security concepts, guidelines, risk management approaches, actions, training, best practices, assurances, and technologies that can be used to protect the cyber environment and the assets of companies and users [15, 16].

This research appears necessary because, if not conducted, issues such as the need for companies to understand their cybersecurity deployment points and current status, creating a shared understanding of cybersecurity among higher institutions, and enabling the planning and targeted implementation of cybersecurity projects by relevant sectors in order to achieve important goals such as sustainability, business continuity, and privacy protection would arise.

Accordingly, providing a cybersecurity evaluation model for the country’s small and medium enterprises has been considered the main objective of the study. Additionally, identifying the factors (dimensions, components, and indicators) effective in designing the cybersecurity evaluation model from the perspective of the cybersecurity maturity evaluation model has been defined as secondary research objectives. For this purpose, this dissertation seeks to present a cybersecurity evaluation model for small and medium enterprises with a focus on cybersecurity management standards, examining cybersecurity maturity models, and utilizing expert opinions by specifying the components of the cybersecurity maturity model. The resulting model can lead to increased cybersecurity for these companies and assist national managers in implementing the cybersecurity maturity model at the national level, in line with revising and evaluating the country's cybersecurity status.

2. Methodology

The present research is qualitative and, using the meta-synthesis method, systematically reviews previous models and frameworks related to the development of cybersecurity evaluation. Since the concept of developing a cybersecurity evaluation is a relatively new concept and, on the other hand, most articles in this area are qualitative studies lacking quantitative data, the current research employs the meta-synthesis method as a suitable approach for comprehensively integrating the concepts of developing a cybersecurity evaluation model for small and medium enterprises (SMEs), based on the translation and interpretation of limited qualitative studies. In this way, past research (both empirical and review) in the area of developing cybersecurity evaluation was examined using the meta-synthesis method.

3. Findings

To perform the meta-synthesis, the seven-step method of Sandelowski and Barroso (2007) was utilized, with each step described below.

Step One: Formulating Research Questions

To formulate and pose the research questions, various factors such as necessity, temporal context, and methodology of the study population were utilized. The research questions were posed based on the SEIP model as follows:

1. What are the contexts and backgrounds for evaluating cybersecurity in small and medium enterprises (SMEs)?
2. What are the inputs or internal data for evaluating cybersecurity in small and medium enterprises (SMEs)?
3. What is the cybersecurity evaluation process for small and medium enterprises (SMEs)?
4. What are the outputs or external data for evaluating cybersecurity in small and medium enterprises (SMEs)?

The main question of this study is to identify the cybersecurity evaluation for small and medium enterprises (SMEs). The examined population consists of related articles in English found in databases such as Google Scholar, Science Direct, IEEE Explorer, Scopus, and Emerald Insight between the years 2015 to 2021. The method used is document analysis.

Step Two: Systematic Review of Literature

The purpose of the literature search and data collection was achieved using the library method. The statistical universe of this study includes all articles published in ISI journals, books, internal and external theses related to the topic of developing a cybersecurity evaluation for small and medium enterprises (SMEs) within the time period of 2015 to 2021. Keywords related to the concept of developing a cybersecurity evaluation and related models in their titles, abstracts, or keywords were searched in internal databases such as Normex, Siyavlia Mag Iran, Elm Net, and external databases like Science Direct, Emerald, Scopus, ProQuest, Springer, Wiley, InterScience, Taylor & Francis, as well as the specialized database Google Scholar.

Step Three: Detailed Evaluation of Studies and Selection of Appropriate Texts

In the third step, the suitability of the found articles with the research questions was examined. Thus, the selected set of studies was reviewed several times. In each review iteration, a number of articles were rejected and removed from the meta-synthesis process. After the review, the suitability of the articles with the considered factors and the methodological quality of the studies were evaluated. The "Critical Appraisal Skills Programme" (CASP) tool was used to assess the quality of primary qualitative studies. This tool consists of 10 questions that help define the concept of qualitative research and determine the accuracy, validity, and importance of qualitative studies.

Step Four: Extracting Information from Texts

In this stage of the meta-synthesis process, the selected articles from step three were repeatedly reviewed and studied to obtain the components of the strategic development of the branding process. Information related to each of the 77 articles, including cybersecurity components for small and medium enterprises (SMEs), authors, and publication year, were extracted and the results were entered into a table.

Step Five: Analyzing and Integrating Qualitative Findings

In the present study, first, all components related to cybersecurity for small and medium enterprises (SMEs) were identified, which are presented in Table 1.

Table 1. Summary of Findings

Row	Model Name	Developed Indices	Defined Levels / Stages	Year of Publication / Last Edition	Creators
1	ISFAM	1) Risk Management 2) Policy Development 3) Information Security Organization 4) Human Resources Security 5) Access and Identity Management Compliance 6) Software Security Development 7) Incident Management 8) Business Continuity Management 9) Change Management 10) Physical and Environmental Security 11) Asset Management 12) Architecture	Stage One: Design Stage Two: Implementation Stage Three: Operational Effectiveness Stage Four: Monitoring	January 2014	Marco Spruit and Martijn Röling
2	ISMM	1) System Monitoring 2) Policies and Procedures 3) Compliance Security 4) Security Incidents 5) Security Architecture 6) Preventive and Corrective Controls	Level One: Non-acceptance Level Two: Initial Acceptance Level Three: Secondary Acceptance Level Four: Acceptable Level Five: Full Acceptance	January 2024	Miller, K., & Thompson
3	E-Government ISMM	1) Information Security Objectives 2) Environmental Security 3) Security Policies and Procedures 4) Risk Reduction Processes 5) Awareness	Level One: Undefined Level Two: Partially Defined Level Three: Managed Capacity Level Four: Under Supervision Level Five: Optimized	August 2011	Geoffrey Karokola and Others
4	5S21S	1) Security Policies 2) Information Security Organization 3) Asset Management 4) Human Resources Security 5) Physical Security 6) Operations and Communications Management 7) Access Control 8) Maintenance and Development 9) Information Systems Management 10) Information Security Incidents 11) Business Continuity Management 12) Compliance	Level One: Commitment Level Two: Principles Level Three: Supervision	January 2024	Alan Gillies, Roberts, M., & Green
5	GAIA-MLIS	1) Policies and Procedures 2) Security Event Awareness 3) Access and Identity Management 4) Access Control 5) Physical Security 6) Network Management 7) Data Encryption 8) Classification	Level Zero: No Assurance Level One: Initial Assurance Level Two: Sustained Assurance Level Three: Safety Level Four: Complete Assurance	January 2014	Roger W. Coelho and Others
6	Cybersecurity Maturity Model for National Critical Infrastructures	1) Protection of Storage Systems 2) Information Sharing 3) Server Protection 4) Physical Security 5) Portable Equipment Security 6) Communication and System Protection 7) Communications and Operations Management 8) Network Security 9) Configuration Management 10) Secure Software Development 11) Network Management 12) Network Security Architecture 13) Workforce Training and Awareness 14) Workforce Management 15) Security Management 16) Security Compliance 17) Information Security Improvement Objectives 18) Application Security 19) Organizational Information Security 20) Human Resources Security 21) Data Classification 22) Cyber Programs Management 23) Use of Indigenous Products 24) Business Continuity Management 25) Security Policies and Procedures 26) Workforce Planning 27) Governance Structure 28) Policy Scope 29) Auditing and Accountability 30) Risk Reduction Processes 31) Risk Management 32) Secondary Company Risk Management 33) Vulnerability and Threat Management 34) Security Incident Management 35) Incident and Event Response and Operations Continuity 36) Recovery 37) Threat Tracking 38) System Monitoring 39) End-User Controls 40) Access Control 41) Environmental Security Risk 42) Data Encryption 43) Situational Awareness 44) Assessment 45)	Level Zero – Level One – Level Two – Level Three – Level Four – Level Five	2023	Mohammad Okhtari and Colleagues

		Identification - Prevention and Corrective Control 46) Individual Security Compliance in Cyber Space 47) Cybersecurity Awareness 48) System Monitoring 49) Social Engineering Attack Control 50) Identification and Authentication 51) Identity and Access Management (IAM) 52) System and Information Integrity 53) Maintenance and Development 54) Information System Ownership 55) Change Management 56) Adoption of New Technology 57) Data Change Analysis / Monitoring			
7	Cybersecurity Maturity Model of the Strategic Management Center of IFTA	1) Information Security Policy in the Organization 2) Internal Organization 3) Human Resources Management 4) Financial Resources Management 5) Cyber Risk Management 6) Asset Management - Changes and Configuration 7) Security Operations Center 8) Technical Vulnerability Management 9) Workforce Management 10) Business Continuity Planning 11) Information Backup 12) Encryption 13) Digital Identity Lifecycle Management 14) Access Control 15) Remote Communications	Level One – Level Two – Level Three – Level Four	2018	Strategic Management Center of the Presidential Office of IFTA
8	CCSMM	1) Threat Identification 2) Information Sharing 3) Technology 4) Training 5) Measurement	Level One: Initial Level Two: Advanced Level Three: Self-assessment Level Four: Integration Level Five: Leading	January 2007	U.S. Department of Homeland Security
9	NICE	1) Workforce Planning 2) Business Processes 3) Risk Management 4) Governance Structures 5) Technology Activation	Level Limited Level Advancing Level Optimized	August 2017	National Security Directive by U.S. President George Bush (2018)
10	CMMC	1) Access Control 2) Personal Security 3) Asset Management 4) Physical Security 5) Auditing and Accountability 6) Recovery 7) Awareness and Training 8) Risk Management 9) Configuration Management 10) Security Management 11) Identification and Authentication 12) Situational Awareness 13) Event Response 14) Communication and System Protection 15) Maintenance 16) System Information Integrity 17) Media Protection	Level One: Basic Cyber Hygiene Level Two: Intermediate Cyber Hygiene Level Three: Good Cyber Hygiene Level Five: Advanced	October 2020	U.S. Department of Defense
11	CYSFAM	1) Server Protection 2) User Controls 3) Network Security 4) Application Security 5) Encryption 6) Portable Equipment Security 7) Vulnerability Management 8) Social Engineering Control 9) Incident Management 10) Cybersecurity 11) Awareness 12) Cyber Governance	Level One: Technical Level Two: Organizational	February 2021	Bilge Yigit Ozkan and Others
12	C2M2	1) Asset Change and Configuration Management 2) Threat and Vulnerability Management 3) Risk Management 4) Identity and Access Management 5) Situational Awareness 6) Incident and Event Response 7) Operations Continuity 8) Third-Party Risk Management 9) Workforce Management 10) Cybersecurity Architecture 11) Cybersecurity Program Management	Level One – Level Two – Level Three – Level Four	July 2021	U.S. Department of Energy

As seen in Table 1, reaching the output (consequence) of the cybersecurity process for small and medium enterprises (SMEs) is the desired research model.

Step Six: Quality Control

In this research, to examine validity, Glin's Vital Assessment tool was used. With the help of this tool, all selected studies were evaluated and selected using 10 assessment criteria. Additionally, the researcher employed the method of agreement between two coders to examine the reliability of the research. For this purpose, a sample of the selected articles was provided to another expert, and the results obtained through the Kappa index using SPSS software were calculated, which, with a Kappa coefficient of 0.635 and a significance value of 0.001, were accepted.

Step Seven: Presenting the Findings

Based on the review of previous research and the classification of extracted codes in Table 1, the cybersecurity components for small and medium enterprises (SMEs) were obtained.

4. Discussion and Conclusion

Cybersecurity for small and medium enterprises (SMEs) is a complex challenge. Unlike large companies, which typically have more financial and human resources to combat cyber threats, SMEs are unable to implement complex models and advanced security systems due to financial, temporal, and resource constraints. On the other hand, with the increase in cyber threats, these companies are particularly vulnerable and require simple and cost-effective frameworks that can protect sensitive information while adapting to their resource limitations. Based on the reviews conducted in this research, the use of frameworks such as the NIST Cybersecurity Framework and ISO/IEC 27001 is highly effective for SMEs because these frameworks provide comprehensive security protections while being adaptable to the limited resources and specific conditions of each company.

One of the key points addressed in this study is the importance of continuous employee training. Many cyber attacks occur due to human errors and lack of employee awareness. Therefore, investing in training and increasing employee awareness regarding cyber threats can significantly reduce risks and vulnerabilities. Additionally, SMEs need to conduct periodic assessments and utilize penetration tests to identify vulnerabilities in their systems and continuously update their security controls.

This research also references various cybersecurity evaluation models that should be selected based on the needs and resources of each company. In fact, for SMEs, it is more advisable to use models that offer easier implementation, lower costs, and gradual improvement. Models such as CIS Controls and the NIST Cybersecurity Framework are highly suitable for SMEs due to their step-by-step and transparent approaches.

Since cybersecurity poses a serious threat to many SMEs, implementing a comprehensive and effective security evaluation model is of great importance. Utilizing standard cybersecurity frameworks like the NIST Cybersecurity Framework and ISO/IEC 27001 can help SMEs identify and manage threats. These frameworks, in addition to providing strong security controls, can flexibly align with the limited resources of these companies.

The most important recommendation for SMEs in the field of cybersecurity is to adopt approaches that are both simple and effective. One such approach is continuous employee training, especially in areas such as phishing attack detection, internal organizational threats, and the safe use of technologies. Additionally, implementing regular risk assessment processes, conducting penetration tests, and continuously updating systems can enhance cybersecurity in these companies.

The overall conclusion of this study is that although small and medium enterprises face numerous challenges in the realm of cybersecurity, they can effectively protect themselves against cyber threats and enhance their data security by selecting appropriate models and implementing security programs that are tailored to their needs and resources. This not only helps in safeguarding sensitive information but also prevents disruptions in business activities and the potential closure of businesses.

Finally, considering the rapid advancement and complexity of cyber threats, SMEs must continually evaluate and improve their security approaches. By implementing an efficient and tailored security evaluation model, they can achieve greater success in combating cyber threats.

The limitations of this research include the evaluation and analysis of articles and studies in both Persian and English languages, the considerable time required for extensive literature review and code extraction, as well as the compilation, integration, and interpretation of codes. Additionally, there is a limitation regarding the applicability scope of the model.

Authors' Contributions

Authors equally contributed to this article.

Acknowledgments

Authors thank all participants who participate in this study.

Declaration of Interest

The authors report no conflict of interest.

Funding

According to the authors, this article has no financial support.

Ethical Considerations

All procedures performed in this study were under the ethical standards.

References

[1] A. T. Chatfield and C. G. Reddick, "A Framework for Internet of Things-Enabled Smart Government: A Case of IoT Cybersecurity Policies and Use Cases in U.S. Federal Government," *Government Information Quarterly*, vol. 36, no. 2, 2019, doi: 10.1016/j.giq.2018.09.007.

[2] F. Cremer *et al.*, "Cyber Risk and Cybersecurity: A Systematic Review of Data Availability," *The Geneva Papers on Risk and Insurance Issues and Practice,* 2022, doi: 10.1057/s41288-022-00266-6.

[3] G. Kabanda, C. T. Chipfumbu, and T. Chingoriwo, "A Cybersecurity Model for a Roblox-Based Metaverse Architecture Framework," *British Journal of Multidisciplinary and Advanced Studies,* vol. 3, no. 2, pp. 105-141, 2022, doi: 10.37745/bjmas.2022.0048.

[4] M. A. Khan and M. Malaika, "Central Bank Risk Management, Fintech, and Cybersecurity," 2021, doi: 10.2139/ssrn.4026279.

[5] N. Kshetri, "Blockchain's Roles in Strengthening Cybersecurity and Protecting Privacy," *Telecommunications Policy,* vol. 41, no. 10, pp. 1027-1038, 2017, doi: 10.1016/j.telpol.2017.09.003.

[6] S. Kumar and R. R. Mallipeddi, "Impact of cybersecurity on operations and supply chain management: Emerging trends and future research directions," *Production and Operations Management,* vol. 31, no. 12, pp. 4488-4500, 2022, doi: 10.1111/poms.13859.

[7] P. Radanliev and D. D. Roure, "Advancing the Cybersecurity of the Healthcare System With Self-Optimising and Self-Adaptative Artificial Intelligence (Part 2)," *Health and Technology,* vol. 12, no. 5, pp. 923-929, 2022, doi: 10.1007/s12553-022-00691-6.

[8] M. Salminen and K. Hossain, "Digitalisation and Human Security Dimensions in Cybersecurity: An Appraisal for the European High North," *Polar Record,* 2018, doi: 10.1017/s0032247418000268.

[9] K. Smith and G. Dhillon, "Assessing Blockchain Potential for Improving the Cybersecurity of Financial Transactions," *Managerial Finance,* 2019, doi: 10.1108/mf-06-2019-0314.

[10] M. Swan, "Anticipating the Economic Benefits of Blockchain," (in eng), *Technology Innovation Management Review,* vol. 7, no. 10, pp. 6-13, 10/2017 2017. [Online]. Available: http://doi.org/10.22215/timreview/1109.

[11] H. Alizadeh and H. Foroughi, "A Strategic SWOT Analysis of Leading Electronics Companies based on Artificial intelligence," *International Journal of Business Management and Entrepreneurship,* vol. 2, no. 3, pp. 59-74, 2023. [Online]. Available: https://mbajournal.ir/index.php/IJBME/article/view/42.

[12] H. Alizadeh and F. Rajab pour, "Investigating the impact of environmental factors on the adoption of social media among small and medium enterprises during the Covid-19 crisis," in *The 6th National Conference and the 3rd International Conference on New Patterns of Business Management in Unstable Conditions,* 2024. [Online]. Available: https://civilica.com/doc/2098684/.

[13] G. M. M. Catagua, "Information Security in the Metaverse: A Systematic and Prospective Review," *Código Científico Revista De Investigación,* vol. 4, no. 2, pp. 781-817, 2023, doi: 10.55813/gaea/ccri/v4/n2/257.

[14] G. Saridakis, V. Benson, J.-N. Ezingeard, and H. Tennakoon, "Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users," *Technological Forecasting and Social Change,* vol. 102, pp. 320-330, 2016. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0040162515002590.

[15] L. Bahrami, N. Safaie, and H. Hamidi, "Effect of motivation, opportunity and ability on human resources information security management considering the roles of Attitudinal, behavioral and organizational factors," *International Journal of Engineering, Transactions C: Aspects,* vol. 34, no. 12, pp. 2624-2635, 2021, doi: 10.5829/ije.2021.34.12c.07.

[16] O. Ganji Bidmeshk and S. A. Hosseini Seno, "Proposing and Testing the Model of Aligning the Marketing Information Security Policy with Strategic Information Systems Plan (Case Study: Ferdowsi University of Mashhad)," (in en), *New Marketing Research Journal,* vol. 5, no. 4, pp. 73-98, 2016. [Online]. Available: https://nmrj.ui.ac.ir/article_17825.html.