Journal of Theoretical and Applied Information Technology
30th April 2024. Vol.102. No 8

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

STRUCTURED CLASSIFICATION OF CRUCIAL RESOURCES AND ECONOMIC IMPACTS IN INDUSTRY 4.0 CYBERSECURITY

WAHYU SARDJONO[1] , GUNTUR SALIM[2]

[1]Information Systems Management Department, BINUS Graduate Program - Master of Information Systems Management, Bina Nusantara University, Jakarta, INDONESIA – 11480
[1]wahyu.s@binus.ac.id

[2]Post Graduate Program, Faculty of Economic Science, University of Trisakti
Jl. Kyai Tapa No. 1 Grogol, Jakarta 11440, Indonesia
[2]guntursalim1979@trisakti.ac.id

*Corresponding author: wahyu.s@binus.ac.id

ABSTRACT

Gained popularity throughout the Industrial Revolution, where manufacturing processes are deeply interconnected through smart devices, the threat landscape of cyber-attacks has expanded significantly. This research addresses the complex repercussions of cybersecurity incidents within the context of Industry 4.0 and introduces a systematic four-step methodology for evaluating the magnitude of business impacts resulting from such breaches. The study begins by examining the increasing range of types and sizes of the operational aspects of enterprises that can be significantly impacted by cyberattacks in the context of Industry 4.0. This environment can result in financial losses, harm to reputation, instances of safety breaches and conservation laws, and even pose life-threatening situations to workers. The resultant four-step methodology empowers companies to assess the financial and operational consequences of cybersecurity breaches effectively. Practical insights and guidance are offered to companies to facilitate the identification of critical manufacturing data, prioritize cybersecurity initiatives, and estimate the costs and scale of business impacts resulting from cybersecurity breaches. In conclusion, as Industry 4.0 continues to transform manufacturing, the effective management of cybersecurity becomes paramount. This study equips organizations with a structured approach to assess and mitigate the business impacts of cybersecurity breaches, emphasizing the necessity for proactive cybersecurity strategies and securing top management support to make cybersecurity both a strategic and operational priority.

Keywords: *Industrial Revolution 4.0, Industry 4.0, Cybersecurity, Cyberattacks, Business Impacts*

1. INTRODUCTION

The scope and complexity of cyberattacks considerably increased during the Industrial Revolution 4.0 when machines are intimately connected by intelligent gadgets. It is commonly understood that cybersecurity breaches can hurt corporate performance in today's highly interconnected manufacturing sector. According to research performed by the Engineering Employers' Federation (EEF) on cybersecurity, nearly half (48%) of manufacturers who reported being harmed by cyber-attacks had significant financial and operational losses. Cyberattacks targeting manufacturing systems can yield a diverse array of adverse business ramifications. These consequences include (i) intentional sabotage of critical infrastructure and vital machinery and components, (ii) network and computer system service disruptions, (iii) The unauthorized acquisition of significant concept of commercial confidential data and their associated ownership, (iv) violations safety and environmental regulations, and (v) situations that could endanger workers' lives. Companies grappling with such circumstances face substantial economic hardships as they strive to restore normal operations, resulting in reduced productivity and a gradual decrease edge in the market. This is supported by a plethora of recent market analysis surveys and reports published by cybersecurity solutions providers. For instance, as depicted in Figure

1, IBM Security revealed that the cybersecurity threat landscape for the critical manufacturing sector has reached an unprecedented level, leading manufacturing to become the most heavily targeted industry in 2021, representing 23.2% of all cyberattacks [1].

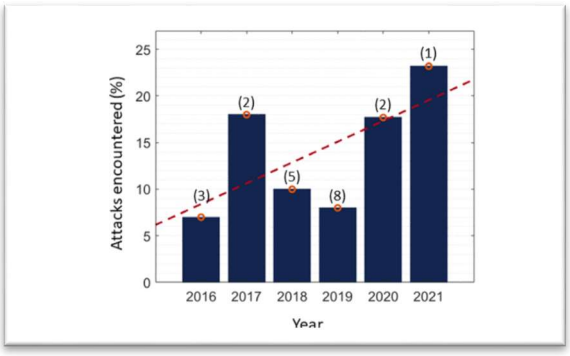

Figure 1. Percentage Of Cyberattacks Encountered By The Manufacturing Industry According To IBM Security [2].

Cascading effects can also be exploited by malicious individuals to instigate significant power disruptions. The robust interconnection between the cyberinfrastructure and the physical components within power grids allows detrimental signals to inflict damage on critical physical apparatus. Upon unauthorized entry to an unprotected network, these individuals can effectively disseminate false information via the specified protocols. Furthermore, smaller operators are particularly vulnerable to such assaults, given their potential lack of resources to strengthen their systems, yet they still retain the capability to influence the power grid's frequency. Typically, cyberattacks are classified based on their distinct attributes. For instance, adversaries can manipulate sensor readings by gaining access to configuration data, constituting a type of attack known as False Data Injection Attacks. Moreover, it is imperative that cybersecurity strategies seamlessly integrate to enhance the overall performance of the industrial value chain by harmonizing organizational and information technology strategies. Nevertheless, a Deloitte poll done in 2018 found that 64% of organizational leaders thought cybersecurity and technology-related risks were being handled insufficiently and needed to be improved.

These solutions must also be modified to fit the particular industrial setting. Despite the availability of numerous methodological solutions for cybersecurity management in the context of Industry 4.0, there hasn't been much focus on the assessment of crucial assets that need to be protected and the evaluation of their related economic implications. In response to Presidential Executive Order 13636, the National Institute of Standards and Technology (NIST) announced its Framework for Improving Critical Infrastructure Cybersecurity, to improve critical infrastructure cybersecurity. The best practices for organizations operating in the critical infrastructure industries are outlined in this framework [3].

2. LITERATURE REVIEW

This section undertakes an analysis of the prevailing cybersecurity goals within the framework of Industry 4.0. This essay will primarily focus on the essential standards, norms, and systematic approaches that are crucial for efficiently addressing cybersecurity concerns in industrial settings. The adoption of Industry 4.0 by organizations introduces a notable problem in the form of cybersecurity. The notion of Industry 4.0 refers to the integration of physical systems (CPS) which are sentient and linked together to automate various aspects of program processes, including creation, production, handling of supply chains, and hospitality support [4].

The advancements associated with the fourth industrial revolution, often known as Industry 4.0, can deliver substantial benefits to enterprises. These advantages predominantly manifest as significant improvements in operational efficiency, estimated to range from 15 to 20 percent. The major the benefits of industry purpose is to increase operational efficiency by maximizing asset utilization, automating manual operations, lowering inventory costs, and increasing service and product quality through real-time data analysis given by machinery. The importance of Industrial Control Systems (ICS) as critical cybersecurity assets in the context of Industry 4.0 was highlighted in a research done [5]. In addition to Industrial Control Systems (ICS), the fundamental asset hierarchy includes industrial internet of things gateways, and sensors. The aforementioned factors are of paramount importance in the oversight and administration of a wide range of corporate operations. The ecosystem under examination covers both supervisory control and data collection systems as well as distributed management systems [6].

Fundamental constituents of Industrial Control Systems encompass critical elements such as Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), Intelligent Electronic Devices (IEDs), and the corresponding interface technologies. In the realm of the fourth industrial revolution, commonly referred to as Industry 4.0, the significance of establishing cybersecurity standards and crafting advice documents cannot be overstated assume a

central role as indispensable assets that assist organizations in cultivating a collective comprehension of security measures pertinent to their particular industry [7]. Additionally, these resources offer methodologies for evaluating the effectiveness and efficiency of these controls. API Standard 1164 exemplifies this situation by providing essential information to the proprietors of oil and gasoline transportation systems as well as anyone interested in enhancing the cybersecurity of Supervisory Control and Data Acquisition (SCADA) systems. In response to rising concerns about intrusions on SCADA systems, this standard was developed. It is crucial to recognize that the utilization of this criterion is beyond the realm of pipelines. This study offers a thorough analysis of the inherent vulnerabilities that exist within the system, which the opportunity for unregistered organizations to exploit the mechanism for their purpose exists. Moreover, this article delineates the requisite protocols that must be incorporated inside a business organization to successfully attain an elevated level of cybersecurity.

Furthermore, this book includes a wide range of strategies for improving system architecture, backed up by specific examples of industry-approved methodologies. With the overarching goal of improving the management of cybersecurity risks spanning various components, including information technology, industrial control systems, cyber-physical systems, and, on a larger scale, interconnected devices, these methodological solutions are specifically created to strengthen cybersecurity within the context of Industry 4.0. The Framework consists of five fundamental tasks, specifically identity, protection, detection, reaction, and recovery. These activities are enabled by an assortment of protection measures [8]. The primary purpose is to support organizations by offering uniform guidelines for comprehending, managing, and conveying security hazards to stakeholders within and outside the organization to acquire a better understanding, consider the critical function that industrial control systems play in enabling the automated operation of technical industrial facilities.

3. METHODOLOGY

The matter of cybersecurity within the framework of Industry 4.0 has been addressed through a wide range of methodological methods. Nonetheless, there is a conspicuous lack of emphasis on detailed asset assessment as a strategic strategy to mitigating cyberattacks and the resulting commercial consequences. Within the overall structure of established connections industrial, these inspections serve as a tactical tool for organizations to determine the allocation of security resources to specific industrial assets. This comprises assessing the value of assets and determining the appropriate level of security. This study primarily aims to assess the negative business implications that arise because of cybersecurity breaches in networked manufacturing machines. The primary aim is to aid company management in effectively tackling cybersecurity concerns.

The review of the current state of knowledge has revealed a noteworthy absence of a complete impact assessment approach that is specifically geared to deeply comprehend and quantify the value of impacts in the context of Industry 4.0. The examination of extant scholarly works has also brought to light particular domains necessitating more investigation and a void that necessitates resolution. The appendices contained within NIST SP 800-53 provide additional resources that include general references, definitions, explanations of acronyms, a categorization of security controls based on different levels of security requirements, a comprehensive inventory of security controls, and information that establishes connections between these controls and other standards and sets of controls. This procedure may involve the use of results derived from a mission or business impact analysis to ascertain probable threat occurrences that result in these consequences [9].

In addition, ethnography was chosen as the research methodology to ensure the practical applicability of this study in the industrial sector. Ethnography is the methodical compilation of field notes, facilitating researchers in acquiring tangible facts and important insights pertinent to the specific context under investigation. The current investigation involves taking detailed field notes while carefully investigating the functioning of production-consumed equipment. The main emphasis was placed on understanding the information traffic generated by the devices, recognizing pertinent safety concerns and evaluating the technology used. Following that, the field notes were subjected to a systematic procedure involving reading, coding, and analysis, by the objectives of the study [10].

Methodological Solution	Industrial asset involved
NIST Framework for Improving Critical Infrastructure Cybersecurity	Information Technology (IT), Industrial Control Systems (ICS), Cyber-Physical Systems (CPS) and any other connected devices
Cybersecurity and resilience framework	Software-defined networking-based manufacturing applications
DevOps approach	Cyber-Physical System (CPS), industrial automation and control systems IACS
Attack tree approach	Industrial Control System (ICS)
Hierarchical model for risk assessment	Industrial Control System (ICS)
Impact assessment model	Internet of Things (IoT) devices
Vulnerability assessment methodology	Supervisory Control and Data Acquisition (SCADA) system

Figure 2. Cybersecurity Methodological Solutions In Industry 4.0 [11]

In brief, this study has systematically developed a comprehensive framework for categorizing essential assets that require safeguarding against cyber threats, utilizing a combination of scholarly sources, NIST guidelines, and the ethnographic research approach. Furthermore, it has furnished a thorough comprehension of the corresponding business ramifications. Furthermore, the research has provided a comprehensive understanding of the complex connection between essential resources and the resulting consequences for businesses, while also elucidating the approaches utilized for evaluating the effects.

The ethnographic context outlined in this research is representative of conditions pertinent to Industry 4.0. As with other manufacturing industries that employ sophisticated the internet of things, statistical analysis of large amounts of data, and digital intelligent systems gadgets are just a few of the emerging technical developments, commercial airline manufacturing sector is facing an increasingly complex array of cybersecurity challenges. The given context, it is plausible for malevolent entities to assume command over industrial operations, thereby exerting influence over the manufacturing processes or potentially modifying the quality of the produced goods. In addition, the firm may face substantial financial repercussions due to the potential compromise of confidential manufacturing process data. Therefore, it is crucial to prioritize the protection of data flows related to aeronautical manufacturing equipment in order to provide resilience against potential cybersecurity vulnerabilities.

4. RESULT AND DISCUSSION

The study successfully categorized crucial resources and identified their corresponding operational impacts, with a particular focus on interconnected industrial devices within the context of industry 4.0. In order to establish a definitive connection between a particular vital asset that has been compromised as a result of a cyberattack and its subsequent business implications, a comprehensive impact matrix has been implemented. Furthermore, the research extensively examines the approaches utilized in assessing the business consequences and presents a range of recommended indicators for evaluation.

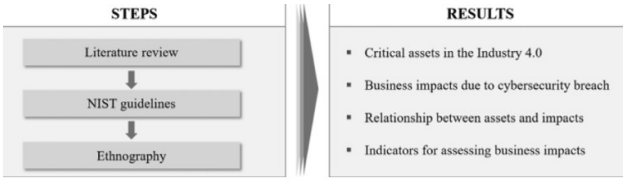

Figure 3. Search Pattern [12]

Critical Assets Analysis

In evaluating the influence of cyber hazards on company performance, it is crucial to prioritize the identification and classification of the critical assets that necessitate safeguarding. The literature study undertaken on cybersecurity challenges within the framework of Industry reveals and industrial control systems are the primary industrial investment that are intertwined with cybersecurity concerns. Possible vulnerabilities could potentially be present inside these systems, particularly at the interfaces that enable the transfer of information between different components. An illustration of potential vulnerabilities can be found within the context of Supervisory Control and Data Acquisition systems. When examining the field of Industrial Control Systems, it is crucial to carefully analyze the many components involved. The components described above consist of the networking structures and protocol stacks, the application server, the database server, the human-machine interfaces, the programmable code buttons, and the remote terminal units [13]. In the domain of modern Operational Technologies, vulnerabilities can be correlated with diverse characteristics of internet-connected industrial machinery. Among these, operating systems and firmware, recognized as fundamental components that enable the core operations of a machine, are notable. The presence of vulnerabilities in these systems has the potential to significantly impact the functionality of the equipment. [14].

Application software can be classified into a wide-ranging category encompassing diverse forms of software, including Computer-Aided Design (CAD), Computer-Aided Manufacturing (CAM), and Computer-Aided Engineering (CAE) software. Furthermore, it includes machine control software and other software with flexible, general-purpose characteristics. These software solutions make it easier to implement machine work cycles in compliance with design, production, and technical specifications [15]. To facilitate the efficient digital transfer of data between different machine components, particularly sensors. Smart devices, which comprise sensors and moving part integrated into equipment, play a significant role in monitoring the flow of data, whether it occurs over wired or wireless networks.

Data Categories Identification

Within the Industry 4.0 paradigm, the protection of data against cyberattacks stands as a matter of utmost importance due to its classification as a vital asset. Contemporary computer numerical control (CNC) machines house a substantial amount of data and are equipped with sophisticated tools that facilitate continuous monitoring of machine performance throughout the entirety of the production process. Differing from this, the data produced by the machine comprises a range of elements, which encompasses various factors such as the operating parameters of the machine, the state of the components involved, and the qualities of the workpiece.

The transmission of this data is facilitated by the utilization of intelligent sensors that have been seamlessly incorporated into the machinery, afterward relaying the information to a centralized control system, such as a Supervisory Control and Data Acquisition system. The control system is responsible for transmitting instructions to the controller installed on the machine to modify its settings. The secure transmission of information across linked systems of production for input and output capabilities equipment is of paramount importance due to its strategic relevance, necessitating protection against potential cybersecurity hazards.

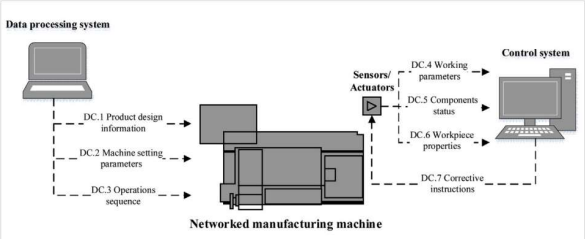

Figure 4. Flow Of Input And Output [16]

Analysis of Business Consequences

The detrimental consequences of a cybersecurity incident can be elucidated by the breach or reduction of any of the following factors pertaining to data security: confidentiality, integrity, and availability. The demand for secrecy is largely concerned with protecting information from unauthorized access or exposure. Within the framework of Industry 4.0, the unauthorized disclosure of confidential manufacturing information might result in adverse business ramifications, particularly the relinquishment of valuable knowledge and intellectual assets. In the present scenario, the loss of significant insights pertaining to processes or products leads to a forfeiture of one's competitive advantage, hence conferring an advantage upon competitors. Damage to image and reputation has a detrimental effect on the attitudes of stakeholders, encompassing consumers, suppliers or contractors, investors, and prospective employees. Ultimately, the requirement for availability ensures that data may be readily accessible and utilized as required. In the context of Industry 4.0, the failure to meet this security criterion can result in the disruption of network services, system devices, or any other computing resources associated with the manufacturing environment.

Violation of data confidentiality

The breach of confidentiality across different data categories might result in diverse consequences for businesses:

1. The compromise of confidentiality about product design information can diminish the competitive edge of a company since it allows competitors to acquire exclusive insights into products and their associated manufacturing procedures. Additionally, there is the possibility for detrimental effects on the company's image and reputation, which may result in a loss of trust from consumers and subsequent supplier substitution.
2. Potential consequences of breaching confidentiality in equipment's the configuration variables or timing of device actions are not anticipated to have substantial ramifications for business operations when examined in isolation.
3. Breach of confidentiality in machine functioning parameters or deterioration of its parts could be detrimental to the business's brand and standing among consumers by revealing information about the overall health of the production system. The potential outcome of this situation is the attrition of both consumers and investors due to the weakened reliability of the organization.
4. A breach of confidence regarding work piece attributes that indicate product quality may result in a competitive disadvantage since competitors can exploit product flaws to achieve a larger market share.

5. Individual violations of confidentiality regarding remedial instructions for machine configuration parameters are not expected to have substantial commercial consequences.
6. The nature of the released data and its possible repercussions on the company's competitive advantage, image, reputation, stakeholder relationships, and financial commitments all have different business implications.

Loss of data integrity

Unauthorized alterations to product design information might potentially result in adverse outcomes regarding product quality and breaches of contractual obligations with customers according to product standards. As a result, in the first scenario, there may be an increase in manufacturing waste alongside a decrease in sales. In the other case, the maker may face potential financial penalties. Similarly, the compromise of data integrity about machine configuration parameters can result in a decline in the quality of products and breaches of safety and environmental regulations, hence posing possible risks to the welfare of employees. Additionally, it could lead to violations of contractual obligations with consumers regarding product requirements.

Consequently, this scenario has the potential to lead to an increase in production waste, a decline in sales, and the imposition of further financial penalties due to failure to adhere to safety, environmental, or commercial standards. Furthermore, the scenario aligns with those previously mentioned in terms of data integrity loss associated with corrective directives for parameters, carrying significant potential consequences for business operations such as product quality degradation, non-compliance with safety and environmental regulations, and violations of commercial pacts with customers. As a result, producers may have challenges in managing increased levels of production waste and experiencing decreased sales due to a decline in product quality.

Loss of data availability

The lack of various types of machine input data can be classified into different groups, including manufacturing knowledge about machine setup criteria, and process sequences, which can lead to a decrease in productive time. These data are essential for launching and sustaining the manufacturing process. Additionally, this situation may lead to a violation of contractual obligations with clients in terms of adhering to product delivery timelines, as well as a decline in the caliber of workpieces due to disturbances in the production procedure. As a result, the restoration of system operation and the management of heightened levels of raw materials inventory awaiting processing would necessitate substantial resources and time allocation. This particular situation has the potential to incur financial losses as a consequence of missed sales caused by disruptions in manufacturing operations, potential financial penalties arising from breaches of contractual agreements, and an increase in waste output due to the deterioration of workpiece quality. In a similar vein, the absence of machine output data, encompassing machine operational parameters, machine component status, workpiece characteristics, and machine correction instructions, might result in production downtime caused by unexpected machine disruptions. Consequently, this could lead to potential violations of contractual obligations with clients about the timely supply of goods or services.

Business impact level assessment

The preceding section has provided a comprehensive and practical analysis of assets and their effects. These findings can serve as a good serve as an invaluable guide and function as a starting point for additional research in different domains of technologically advanced contexts, regardless of their similarity or dissimilarity to the manufacturing cell that was examined. Each of these phases might be utilized as a method to evaluate the extent of business damage, aiding organizations in comprehending which crucial assets necessitate their defensive endeavors. To commence, we propose analyzing pivotal assets within the industrial domain of cybersecurity. Undoubtedly, the compromise of these assets through cybersecurity breaches, which exploit system weaknesses, can significantly negatively impact corporate performance.

Simultaneously, a further phase may entail the characterization of the business ramifications linked to every compromised security prerequisite, encompassing the confidentiality, integrity, and availability of manufacturing data and systems. In the third phase, it is recommended to develop linkages between critical resources and cyber risks that have the potential to result in specific operational consequences for the organization. The violation of security requirements can lead to the manifestation of business repercussions, which can be analyzed and represented through the establishment of an impact matrix. In the interest of comprehensively outlining the essential data categories and business implications examined, it is imperative to involve key informants from the organization in focus groups during the initial and subsequent stages.

The user's text does not contain any information to rewrite academically. To facilitate the third phase, it is advisable to administer an online survey aimed at

including important informants inside the organization. This approach can effectively align crucial data with the potential commercial ramifications arising from cybersecurity breaches.

Data Category: Machine Operations Sequence Business Impacts Summary Report		
Business Impacts due to Loss of Data Availability		
	BI.3.1 - Loss of productive time.	IC.5. Restoring the system functionalities: 37k€ IC.6. Higher inventory levels for raw materials: 19k€ IC.3. Lost sales: 125k€
	BI.3.2 - Violation of the commercial agreements with customers on delivery time.	IC.4. Financial penalties: 140k€
	BI.3.3 - Quality degradation of the workpieces.	IC.2. Higher production waste: 7.5k€
Business Impacts due to Loss of Data Integrity		
	BI.2.1 - Damages to working machines.	IC.1. Repairing the physical systems: 10.5 k€
	BI.2.3 - Violation of standard and regulations in the field of safety and pollution. BI.2.5 - Life-threatening situations for workers.	IC.4. Financial penalties: 140k€

Figure 5. Summary Report On The Organizational Impacts Of Machine Activities Series [17]

During the fourth stage, conducting semi-structured interviews with company specialists becomes a realistic approach to assessing costs and the severity of business ramifications using the metrics proposed. It is crucial to emphasize that the extent of influence differs based on the particular data type. In a general sense, the degree of effect can be categorized as "minimal," "moderate," or "substantial." The delineations of the three major impact categories are outlined in the NIST Risk Management Guide for Information Technology Systems :

1. High impact level: When a vulnerability is exploited, it may result in the extremely costly loss of significant tangible assets or resources, severe violations, damage, or disruption of an organization's mission, reputation, or interests, or even lead to human fatalities or serious injuries.
2. Medium impact level: When a vulnerability is exploited, it can lead to the costly loss of tangible assets or resources, moderately violate, harm, or impede an organization's mission, reputation, or interests, or cause human injuries.
3. Low impact level: When a vulnerability is exploited, it may result in the loss of some tangible assets or resources, or it may noticeably affect an organization's mission, reputation, or interests.

The term "exercise of vulnerability" pertains to the situation where a few privacy concerns, such as confidentiality, integrity, or availability, associated with a particular data category, have been violated. Knowledge of product and manufacturing process specifics, IT system features, inventory levels, sales strategies from a supply chain management perspective, and an examination of legislative, system, and security-related documentation within the organization should all be acquired during the process of gathering information to determine impact costs through semi-structured interviews.

Anticipation of gathering pertinent data for assessing the extent of impact is recommended to be done by both technical and industry members of the management team. The management team has a comprehensive understanding of the sensitive information held by the organization. If this information were to be shared with external parties such as suppliers, customers, or competitors, it might potentially result in a decline in effectiveness edge or damage to the company's reputation and public perception. As a result, this study provides valuable insights that can enable companies to obtain various advantages. These include the identification of crucial manufacturing data that should be protected against cyber-attacks, the determination of business impacts that should be given priority in the event of cybersecurity breaches, the specification of business impacts resulting from the compromise of specific data categories, and the estimation of the costs and magnitude associated with these business impacts. Direction of harnessing these benefits, it is essential to establish and implement suitable procedures for application and analysis, as previously described.

5. CONCLUSION

Cybersecurity is a significant challenge for organizations embracing the Industry 4.0 framework in the contemporary context, as they strive to maintain their competitive edge. In recent times, there has been a notable effort by both European and worldwide standardization organizations to establish clear standards and generate informative guide manuals. 1Despite a significant amount of research offering methodological solutions to address cybersecurity issues within Industry 4.0, it is important to note that none of these approaches focus on security concerns by establishing a link between protecting critical assets from cyber threats and the resulting impacts on business operations, all while quantifying these impacts. This gap involves the absence of a hierarchical risk model.

This proposed technique is a significant resource for enterprises dealing with cybersecurity difficulties in the context of Industry 4.0, allowing them to assess cyber threats with the help of NIST's assets. The technique described relies on the examination of crucial assets that require safeguarding from cyber threats. It involves identifying the negative economic consequences of security breaches and establishing the relationship between these two factors. Furthermore, because

present research predominantly centers around computer numerical control, or CNC, manufacturing infrastructure, employing a factory technique contexts utilizing varied production technologies may result in divergent conclusions in terms of business effect assessment. Ultimately, the successful implementation of this system requires active participation from key employees inside the organization.

Participation in focus groups, completion of online questionnaires, and participation in semi-structured interviews are all examples of how you might be involved. The establishment of a significant response rate and the maintenance of consistent outcomes necessitate substantial support from upper-level management. In essence, cybersecurity problem resolution should become a strategic and operational priority for the organization.

REFERENCES

[1] M. H. Rahman, "Manufacturing cybersecurity threat attributes and countermeasures:," *Journal of Manufacturing Systems,* vol. 68, pp. 196-208, 2023.

[2] IBM SECURITY X, "Force Threat Intelligence Index," IBM, USA, 2022.

[3] J. A. Bullock, G. D. Haddow and D. P. Coppola, Introduction to Homeland Security - Chapter 8 Cybersecurity and critical infrastructure protection, Elsevier, 2021.

[4] M. P. Lambán, P. Morella, J. Royo and J. C. Sánchez, "Using industry 4.0 to face the challenges of predictive maintenance: A key performance indicators development in a cyber-physical system," *Computers & Industrial Engineering,* vol. 171, p. 137, 2022.

[5] M. Macas, C. Wu and W. Fuertes, "A survey on deep learning for cybersecurity: Progress, challenges, and opportunities," *Computer Networks,* vol. 212, 2022.

[6] H. Boyes, B. Hallaq, J. Cunningham and T. Watson, "The industrial internet of things (IIoT): An analysis framework," *Computers in Industry,* vol. 101, pp. 1-12, 2018.

[7] M. H. Rais, R. A. Awad and J. L. Jr, "Memory forensic analysis of a programmable logic controller in industrial control systems," *Forensic Science International: Digital Investigation,* vol. 40, 2022.

[8] R. Kaur, D. Gabrijelčič and T. Klobučar, "Artificial intelligence for cybersecurity: Literature review and future research directions," *Information Fusion,* vol. 93, 2023.

[9] L. Johnson, Security Controls Evaluation, Testing, and Assessment Handbook (Second Edition), Academic Press, 2020.

[10] V. Bolbot, K. Kulkarni, P. Brunou and O. V. Banda, "Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis," *International Journal of Critical Infrastructure Protection,* vol. 39, pp. 2-8, 2022.

[11] C. Jansen and S. Jeschke, "Mitigating risks of digitalization through managed industrial security services," *AI & SOCIETY,* vol. 33, p. 163–173, 2018.

[12] S. Raj, J. S. Pann, S. L. Fernandes and A. Ramanathan, "Attacking NIST biometric image software using nonlinear optimization," *Pattern Recognition Letters,* vol. 131, pp. 79-84, 2020.

[13] G. Corbò, C. Foglietta and S. Panzieri, "Smart Behavioural Filter for Industrial Internet of Things," *Mobile Networks and Applications,* vol. 23, p. 809–816, 2018.

[14] D. Wu, A. Ren, W. Zhang and J. Terpenny, "Cybersecurity for digital manufacturing," *Journal of Manufacturing Systems,* vol. 48, no. C, pp. 3-12, 2018.

[15] L. Xu and E. Tomai, "A survey on security analysis of machine learning-oriented hardware and software intellectual property," *High-Confidence Computing,* vol. 3, no. 2, 2023.

[16] A. Corallo and M. Lezzi, "Cybersecurity in the context of industry 4.0," *Computers in Industry,* vol. 114, 2019.

[17] S. F. Ahamed and A. Vijayasankar, "Machine learning models for forecasting and estimation of business operations," *The Journal of High Technology Management Research,* vol. 34, no. 1, 2023.