

Towards a Sustainable Future: Developing a Cybersecurity Framework for Manufacturing

Abstract

Purpose - This study aims to propose a cybersecurity framework that prioritizes sustainability in the manufacturing sector by identifying necessary resources and capabilities for effective cybersecurity management. The proposed framework aims to enhance resource protection and safeguard data confidentiality, integrity, and accessibility, provide proactive steps for predicting cyber threats, and highlight the importance of educating employees at all levels of the organization.

Design/methodology/approach- A thorough review of existing literature and analysis was conducted to develop the proposed cybersecurity framework. Several frameworks, including the NIST cybersecurity framework, were reviewed to identify the necessary skills and resources required to combat cyber threats and keep businesses sustainable.

Findings- The proposed framework includes proactive steps, such as predicting cyber threats, and emphasizes the importance of educating employees and raising awareness at all levels of the organization. Resilience is also emphasized, which refers to an organization's ability to recover and continue operations following a cyberattack. Implementing this framework may require a significant budget and time investment, and small organizations may face limitations in applying all aspects of the framework.

Originality/value- This study proposes a cybersecurity framework that prioritizes sustainability in the manufacturing sector, which provides added protection for organizations. The framework's key functions can be adopted partially or fully, making it suitable for organizations of varying sizes. Future research can focus on addressing the framework's limitations and shortcomings to further reduce cyber risks for sustainable manufacturing, establishing the scale of an industry based on its economy, and extending the framework to non-manufacturing businesses.

Keywords: Cybersecurity, Cyber threats, Cybersecurity framework, Manufacturing sector, Sustainability.

Paper type - Research paper

1. Introduction

Throughout history, industrial sectors have undergone multiple revolutions, such as mechanisation in the eighteenth century and the use of energy and assembly lines in the nineteenth century during the Second Industrial Revolution. In the late 1970s, the Third Industrial Revolution partially automated industries through the use of memory-programmable controllers in computers (Kamarul Bahrin *et al.*, 2016). In 2011, Industry 4.0 was introduced as a component of the German High Tech 2020 Strategy, aimed at driving digital manufacturing by connecting products, value chains, and business models (Pfeiffer, 2017). Since then, Industry 4.0 has gained popularity due to its benefits, including efficiency, sustainability, and productivity improvement (Mullet *et al.*, 2021). This revolution has transformed various sectors, such as health and safety, aviation, agriculture, manufacturing, logistics, and infrastructure. The demand for digital services and manufacturing to produce smart products has resulted in the emergence of new business models. By utilizing advanced analytics for customer and supplier data, supply chains can accurately forecast future demand (Iqbal *et al.*, 2020).

With the adoption of Industry 4.0 by more businesses to increase efficiency and sustainability, the number of internet-connected systems has increased, along with the risk of cyberattacks on data and processes. Cyberattacks have increased significantly after the Covid-19 pandemic and the Russia-Ukraine war due to vulnerabilities in the system (Jagtap *et al.*, 2022). The manufacturing industry is hesitant to invest in Industry 4.0 technologies due to the uncertainty surrounding digital improvement caused by cyber threats (Alqudhaibi *et al.*, 2022). To address this issue, security objectives, countermeasures, standards, and protocols have been established, and cybersecurity teams assess all cybersecurity risks (Cormier and Ng, 2020). Developing cyber solutions to prevent cyber threats is necessary due to the unique use of manufacturing systems, making them vulnerable to cyberattacks. Industry 4.0 may play a crucial role in improving operational efficiency, productivity, and mass customization (Borky and Bradley, 2019; Mullet *et al.*, 2021). Data security and safety are crucial for managing the increased amount of data and ensuring smooth processes (Kavallieratos *et al.*, 2020). A sustainable framework must prioritize cybersecurity by predicting cyberattack methods to address threats early on. Understanding the actual situation is essential to developing a strategy that considers cybersecurity a priority in future organization projects.

This paper aims to develop a cybersecurity framework for sustainable manufacturing by identifying necessary skills and tools and defining relevant concepts. To achieve this, the study utilizes multiple databases, including Scopus, IEEE, and Elsevier, to obtain publications and articles related to sustainability efforts in manufacturing relevant to cybersecurity management. The data undergoes a screening technique to ensure its reliability and relevance to the study objectives. The research focuses on gaining a better understanding of cybersecurity management by identifying required knowledge and techniques, establishing core principles of sustainable manufacturing, and developing a framework applicable to businesses. Table 1 provides details of the objectives, research questions, and methodology used in the study.

Objective	Paper Questions	Methodology/Task
Identify skills and tools for effective Cybersecurity management in the manufacturing sector	<ol style="list-style-type: none"> 1. Which skills are important for cybersecurity management? 2. Why these skills are very important for effective cybersecurity management? 	<ol style="list-style-type: none"> 1. Finding the literature about cyber-attacks and how it is mitigated.
Define the fundamental principles of Cybersecurity in sustainable manufacturing	<ol style="list-style-type: none"> 1. What is the process used when a cyberattack is detected? 2. What principles are used when a cyber incident takes place? 	<ol style="list-style-type: none"> 1. Principles used in NIST. 2. NIST framework for manufacturing profile.
Develop a Cybersecurity framework for sustainable manufacturing	<ol style="list-style-type: none"> 1. How does the cybersecurity framework work? 2. Cybersecurity Framework for other sectors? 	<ol style="list-style-type: none"> 1. Comparing frameworks of different profiles. 2. Finding the possible gaps through literature.

Table 1. Summary of objectives, research questions, and methodology.

The research is divided into three parts. The first part aims to identify necessary skills and tools to manage cybersecurity effectively and promote sustainability in the manufacturing sector. The goal is to anticipate threats and mitigate them using tools. The second part is to establish fundamental principles of cybersecurity in sustainable manufacturing, which will serve as the foundation for the framework. The final part involves describing the developed cybersecurity framework for sustainable manufacturing, which organizations can use to identify, protect, detect, respond to, and recover from cyberattacks based on sustainability pillars. Figure 1 shows the relationship between cybersecurity and sustainability pillars.

Fundamentally, sustainability is about managing resources in a way that prevents resource depletion, strategically satisfies current demands, and anticipates future needs. For instance, environmental sustainability attempts to preserve natural resources like water, forests, and productive land so that future generations can prosper. Similar to this, cybersecurity sustainability is spending time, effort, and money in a way that reduces risk, lowers expenses, and increases effectiveness both immediately and over time. Consider how sustainability looks across the social, economic, and environmental pillars to implement these ideas.

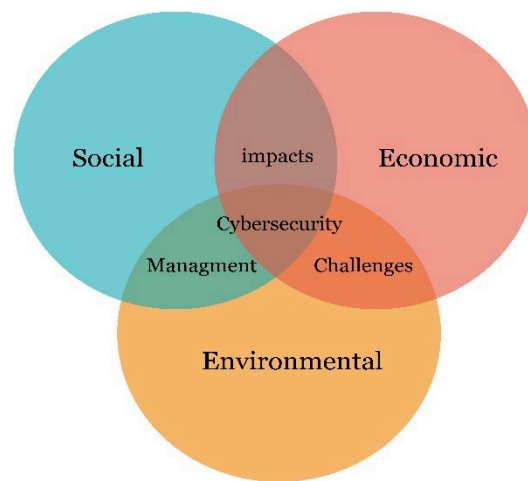


Fig 1. Sustainability pillars.

2. Literature Review

This section introduces the concepts of cybersecurity and Industry 4.0. It also identifies definitions and methods used in the literature for sustainable manufacturing and cybersecurity prioritization, serving as guidelines for this work (Culot *et al.*, 2019). Additionally, this section discusses the impact of cybersecurity on manufacturing and how it is relevant to manufacturing sustainability.

2.1 Cybersecurity, Sustainability and I4.0 concept

Cybersecurity is a means of defending internet-connected systems from cyber threats. The National Institute of Standards and Technology (NIST) defines cybersecurity as the prevention of damage to, protection of, and restoration of computers, electronic communications systems and services, wire communication, and electronic communication, including the information contained therein, to ensure availability, integrity, authentication, confidentiality, and non-repudiation (Barrett, 2018). In simpler terms, cybersecurity aims to prevent harm to, safeguard, and restore industrial assets while maintaining the properties of availability, integrity, authentication, and confidentiality.

Sustainable manufacturing focuses on enhancing various aspects of the manufacturing process, including staff, products, and the environment. According to (Machado *et al.*, 2020),

sustainable manufacturing involves integrating processes and systems to produce high-quality products and services while minimizing the use of unsustainable resources. Sustainable manufacturing ensures that resources are secure for customers, employees, and surrounding communities, while also reducing adverse impacts throughout the product life cycle.

Cybersecurity sustainability refers to dedicating time, funds, and effort to minimize cyber threats' risks, reduce costs, and increase short-term and long-term effectiveness (Sadik *et al.*, 2020). Sustainability in cybersecurity and the environment can occasionally overlap, particularly in manufacturing technologies (Miller *et al.*, 2021). For example, consider dealing with suppliers who adhere to environmental obligations, governance missions, and social cloud providers who use renewable energy to power their data centres (Katal *et al.*, 2022). The role of security awareness training in a sustainable framework is to enhance employees' skills and behaviour to safeguard their organization (Alshaikh *et al.*, 2019). Additionally, security specialists can educate executives to recognize and report cyber threats, such as spear-phishing campaigns.

Industry 4.0 forms the basis for various advancements. However, in recent years, industries have encountered several cyber-attacks, and the manufacturing industry is no exception, leading to the sector's need to be more confident in investing in Industry 4.0 technology. IBM reports indicate that the manufacturing industry experienced the highest number of attacks (23%) in 2021, which negatively impacted the sustainability of the global supply chain network (Rameem Zahra *et al.*, 2022). The report further highlights that 47% of the attacks on the industry were due to poor vulnerability management within organizations.

2.2 Cybersecurity characteristics

Mullet and Sonni have categorized cybersecurity characterization into two types: technical and managerial (Mullet *et al.*, 2021). Technical characterization focuses on the technical aspects of cybersecurity that IT specialists can handle, while managerial characterization focuses on the strategic aspects of cybersecurity in an organization.

2.2.1 Technical Characterisation. The technical aspects of cybersecurity characterisation concern the following essential factors:

- Critical assets to be protected - The term "cyberspace" refers to the perimeter that cybersecurity protects, and every element interacting with it is at risk and requires

protection (Li *et al.*, 2019). This includes hardware such as tools, phones, and other devices; people working within the organization; physical assets such as buildings and factories; and IT infrastructure, which involves applications, networks, processes, and data (Alqudhaibi *et al.*, 2022).

- Cyber-attacks threaten critical assets - Cyber-attacks pose a threat to these critical assets, and it is necessary to secure them against all risks, such as vulnerabilities and attacks.
- Security protection - In dealing with cyber-attacks, two approaches can be taken: short-term and immediate protection in case cybercriminals penetrate the system, and long-term prevention and protection solutions such as guidelines (Tounsi and Rais, 2018).

2.2.2 Managerial Characterisation. Mullet *et al.* state that cybersecurity management is built on three fundamental ideas, namely the strategic aspect with value generation, awareness of the need for cybersecurity, and definition of cybersecurity strategy (Mullet *et al.*, 2021).

- Strategy Definition - Defining the organization's strategy is essential to understand the importance and impact of a cyberattack (AlDaajeh *et al.*, 2022). The strategy aims to reduce the costs associated with unreliability and ensure business continuity. From a non-technical perspective, a cyberattack can result in financial loss for the finance department, reputational harm for the marketing department, or hardware downtime for the production department. Managers need to adopt a strategic approach and consider risk management and cyber resilience. The involvement needs to be from top management to shop floor employees.
- Strategy Aspect - As companies handle customer data, there are potential business opportunities for them to offer cybersecurity services such as data protection, reliable technology, and secure access. Customers are willing to pay for such services, providing an avenue for companies to benefit (Kavallieratos *et al.*, 2020).
- Awareness - Empowering people includes raising awareness that cybersecurity involves everyone. In the corporate setting, awareness is promoted through the implementation of cybersecurity strategies (Donalds and Osei-Bryson, 2020; Mullet *et al.*, 2021). It is important for companies to recognize the significance of cybersecurity to their customers, stakeholders, and other relevant parties. Implementing multiple layers of defense can improve system security, and the human resources department plays a critical role in raising awareness. This is particularly crucial in the manufacturing industry where cyber governance is often inadequate, according to Vincent (Vincent,

2022). A survey of 350 manufacturers indicated poor data governance across the manufacturing sector, as depicted in figure 2.

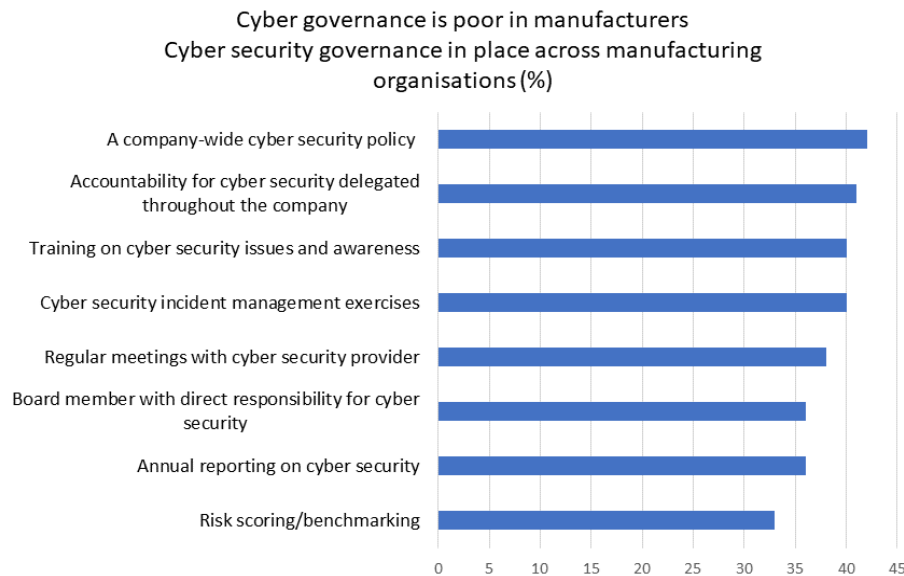


Fig 2. Cybersecurity governance across manufacturing organisations (%).

3. Cybersecurity Challenges and Analysis

The manufacturing sector is experiencing an increasing number of cybersecurity issues that require continual resolution as new problems emerge. According to Ani et al. (2017), information, communication, and operations management systems (ICSs) demand special attention because of their susceptibility to risks. People, processes, and technology are the three fundamental categories that an ICS employs to define its security anomalies and controls. These three categories serve as structural elements for all functional digital systems (Ani *et al.*, 2017). To help ICS owners comprehend and identify security issues during deployment, security concerns related to these three cooperating categories have been explored.

The issues related to people in the manufacturing sector are considered to be insecurity problems associated with the human workforce. On the other hand, the process-centric issues are the most closely related to the flaws in industrial infrastructure that could pose risks. The technology-centred issues are considered to be weaknesses in security, hardware, software, and network systems. The lack of cybersecurity infrastructure due to the organisation's lack of financial resources can also pose a problem and make it more challenging for systems to identify attacks, giving a false impression of security (Vincent, 2022). Due to poor cyber hygiene, most manufacturers are inviting attackers to access their system and spread the threat.

Cyber hygiene practices include regular data backup, training, privacy shield for screens, permission control, password changes, software updates, access control, penetration tests, and VPN use (Borky and Bradley, 2019; Alqudhaibi *et al.*, 2023).

As the manufacturing industry expands with the implementation of I4.0 and IoT, the risk of cyber threats damaging manufacturing organisations is increasing. Despite being aware of these risks, many manufacturers struggle to cope with cyber threats, as highlighted by Vincent (2022). To analyse cyber threats, various factors such as the source of the attack, attack objectives, and cyber layer must be evaluated (Mullet *et al.*, 2021). Cyber risks and threats are evaluated based on availability, integrity, and confidentiality characteristics. There are several types of cyberattacks, but the five most common ones are scamming, phishing, man-in-the-middle attacks, ransomware, and SQL injection (Shahin, Chen, Hosseinzadeh, *et al.*, 2022). These types of attacks can cause significant damage, including revenue loss, reputational harm, legal and regulatory repercussions, loss of customers, and fines, with medium-sized companies being the most targeted (Vincent, 2022). Figure 3 shows the percentage of manufacturers who believe they are well-prepared to deal with cyberattacks. However, some manufacturers neglect cybersecurity as they upgrade their systems, increasing the likelihood of cyber threats.

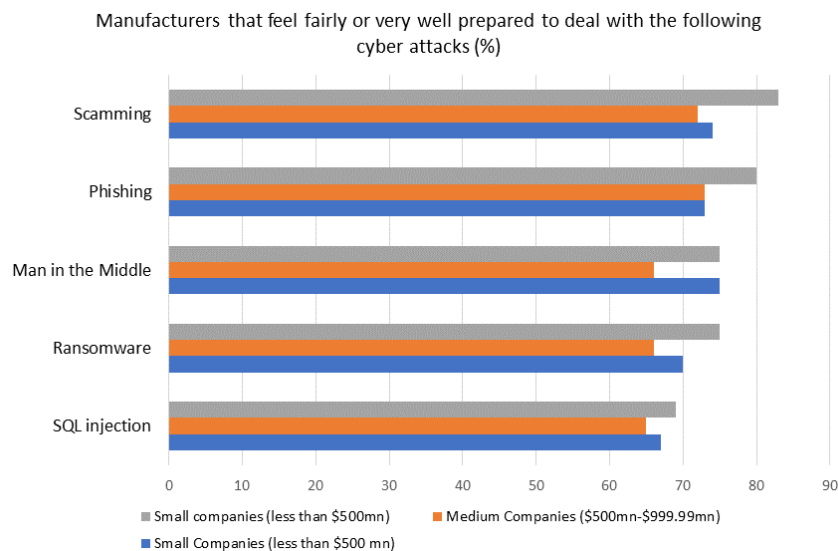


Fig 3. Manufacturers' preparedness against cyberattacks (Vincent, 2022).

4. Define the fundamental principles of cybersecurity in sustainable manufacturing

The concept of the "triad" in cybersecurity refers to the balance of data confidentiality, integrity, and availability. Confidentiality refers to keeping information private, which is important for both public and private enterprises. Access to data is closely controlled, but there are various types of attacks that can compromise confidentiality, in addition to human error. Data integrity, on the other hand, ensures that data is accurate, reliable, and trustworthy, and has not been changed in any way (Schlatt *et al.*, 2023). When data integrity is compromised, it can have a negative impact on the business and its operations. Availability means that authorized users can always access the data, and it is crucial to ensure that networks and applications are compliant with security policies to maintain availability. Business operations can be disrupted when availability is compromised (Shafae *et al.*, 2019).

To ensure sustainable manufacturing, it is crucial for businesses to maintain availability, confidentiality, and integrity through proper protocols. As per the NIST framework, the functional categories that support the mission objectives should be aligned with the organisation's mission to maintain the categories of functions shown in Table 2 (Barrett, 2018; National Institute of Standards and Technology, 2018). This helps companies focus on cybersecurity defences against risks that could directly and seriously impact their ability to carry out essential tasks. For the manufacturing industry, NIST identifies the top five business goals, which are maintaining environmental safety, human safety, production goals, product quality, and sensitive information.

Table 2. Functions & categories in the NIST framework.

Function	Function	Category	Category
Unique Identifier		Unique Identifier	
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Management
		PR.AC	Identity Management, Authentication and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data security

PR	Protect	PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Event
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communication

5. Cybersecurity framework for sustainable manufacturing design and analysis

5.1 Developing a cybersecurity framework for sustainable manufacturing

The cybersecurity framework is designed to improve the protection of organizations by establishing advanced measurement standards and technologies. NIST has developed frameworks for various profiles, including one for the manufacturing profile. This framework provides manufacturers with several benefits (Barrett, 2018), such as:

- A method to enhance their current cybersecurity position.
- An evaluation of their ability to manage risk in the control environment.
- A systematic process for creating a cybersecurity plan to maintain system security assurance.

To enhance the current cybersecurity position of manufacturing systems, the manufacturing profile is utilized as a roadmap that emphasizes cybersecurity outcomes. The profile offers a voluntary, risk-based approach to manage cybersecurity activities and minimize the cyber risk to the manufacturing system. It is designed to encourage manufacturers to adopt industry standards and current cybersecurity systems.

The guidance provided by the profile is flexible and allows for security measures to be increased as needed while maintaining a standard baseline. The profile framework uses the manufacturer's own risk management methodology to guide and prioritize cybersecurity decisions, helping to identify target conditions for cybersecurity operations and providing business justifications through ongoing risk assessments (Shahin, Chen, Bouzary, *et al.*, 2022). It also helps manufacturers prioritize security activities to meet their business goals, enabling them to establish critical tasks and set decision-making priorities. The framework is divided into three categories based on the impact on the organization, as there is no single solution that works for all methods of managing cybersecurity threats in manufacturing facilities.

In this context, Lewis *et al.* proposed a framework for information security sharing in UK small and medium-sized enterprise (SME) supply chains based on information classification (Lewis *et al.*, 2014). However, this framework may have limitations when applied to larger SMEs, given that the study was conducted with a small sample of companies in the UK. Thus, it is recommended to conduct monitoring and evaluation before applying the framework to ensure its effectiveness. Furthermore, Efthymiopoulos argues that a strategic cybersecurity framework is essential for NATO and the military industry (Efthymiopoulos, 2019). The author provides a strategic overview of past, present, and future events and concludes that NATO must remain adaptable to protect against current and potential multi-dimensional threats.

The present research aims to establish a cybersecurity framework for sustainable manufacturing. Based on the literature review and subsequent analysis, the following key findings have emerged for the development of a cybersecurity framework for the manufacturing industry.

5.2 *The proposed framework for sustainable manufacturing*

The proposed framework for cybersecurity in sustainable manufacturing is based on the key findings obtained from the literature review and is presented in Table 3.

Table 3. Proposed Framework Elements

<ul style="list-style-type: none"> • Mandatory Awareness Training • Resilience Training • Employee Activity and Behavior Monitoring 	<ul style="list-style-type: none"> • Cloud Storage for safety • Data Access Restriction based on Location • Continuous Vulnerability Management
--	--

- | | |
|--|--|
| • Cybersecurity Policy in Corporate Strategy | • Real-Time Reporting |
| • Cybersecurity and Framework Audit | • Penetrations Test and Physical Intrusion Test |
| • Cyberhealth and Cyber hygiene Monitoring | • Use of AI and ML for False Positive Detection |
| • Safe Vendor Access | • Quarterly Testing and Review with Incident Response Planning |
-

The initial recommended action is to require cybersecurity training for all employees in the organization to enhance awareness across all departments. Many organizations offer training, but it is not mandatory, and this could improve cybersecurity awareness. Moreover, monitoring employees' activities and behaviour could help detect unusual behaviour.

Manufacturing companies should follow a standard framework to develop their cybersecurity strategies. Therefore, auditing both the framework and the cybersecurity policy is critical (Sabillon *et al.*, 2018; Wong *et al.*, 2022). It is also important to assess the manufacturer's cybersecurity practices, cyber hygiene, and cyber health (Vincent, 2022). When dealing with third parties, such as external suppliers and vendors, it is crucial to protect data by reviewing their cybersecurity policies and ensuring secure asset sharing, such as data sharing and financial transactions (Mullet *et al.*, 2021). Additionally, due to the benefits of cloud storage, including security, safety, and availability (Alouffi *et al.*, 2021), it is essential to protect data access by, for example, restricting access based on location to add an extra layer of security and keep confidential data safe.

Continuously monitoring vulnerabilities is helpful in identifying weaknesses that could jeopardize the system, and as a result, strategically extending continuous vulnerability management is advantageous (Mullet *et al.*, 2021). To protect data and the system, real-time reporting should be carried out during the monitoring process (Naseer *et al.*, 2021). False positives are frequently detected by manufacturers, which results in the waste of resources. Artificial intelligence can be used to identify false positives as well as real-time cyber threats that are active worldwide. To assess the system's defences against various cyber threats, physical intrusion testing and system penetration tests should be performed (Shi *et al.*, 2019; Wong *et al.*, 2023). Figure 4 describes the cybersecurity framework's implementation, which

contains the inputs, activities, and outputs.

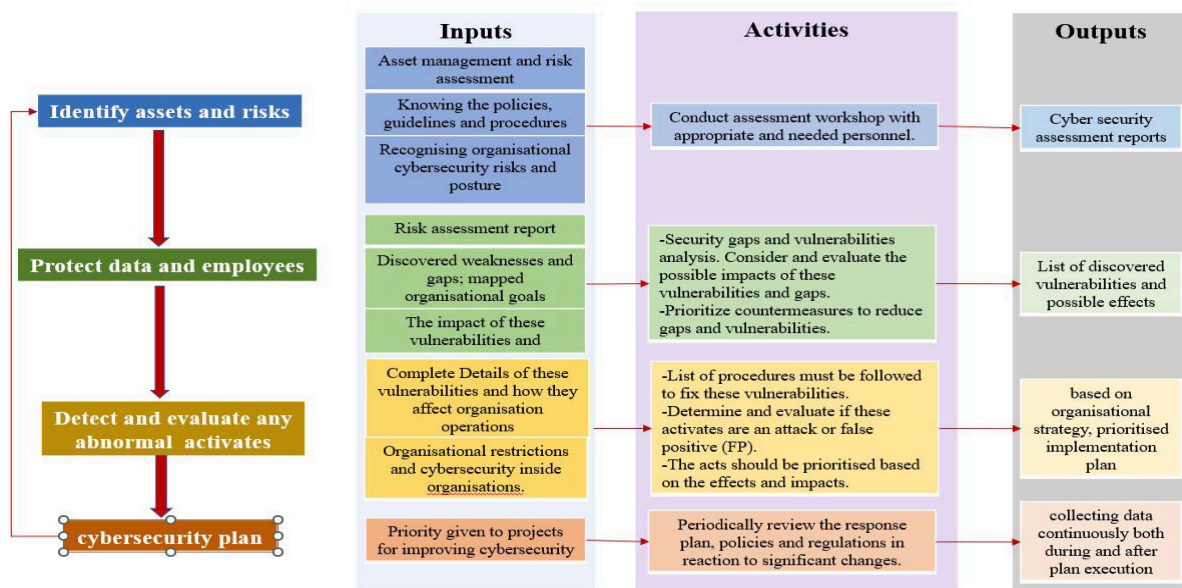


Fig 4. Cybersecurity framework implementation in the Manufacturing sector.

To enhance cybersecurity, it is important to predict and prevent cyber-attacks using reliable datasets and various algorithms. The use of Artificial Intelligence (AI) and Machine Learning (ML) technologies in predicting cyber-attacks offers multiple algorithms. Implementing this approach is crucial in outlining the necessary measures to protect against cyber-attacks. The framework's lifecycle and design are depicted in Figure 5.

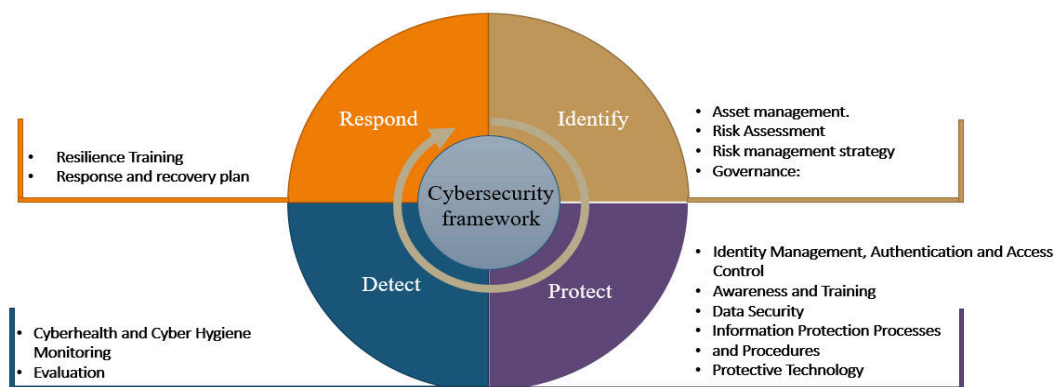


Fig 5. The framework lifecycle and pillars.

Multifactor authentication is an effective measure to enhance identity management and access control. It is also crucial to have a response plan and strategy in place, and a documented recovery plan that covers critical resources and operations. Regular testing and cyber incident response planning are recommended for improved recovery planning. Since manufacturers need to maintain operations, resilience training is necessary following cyberattack factors

(Buehler *et al.*, 2020; Hajj *et al.*, 2020). Table 4 outlines these factors for the proposed framework.

Table 4. The proposed framework factors.

Proposed Element for Framework	Pillar	Category
Cloud Storage & resources	Identify	Asset Management
Predict cyberattacks	Identify	Risk Assessment
Staff Activity and Behaviour Monitoring	Identify	Risk Assessment
Use of AI & ML for Detection of False Sensitive	Identify	Risk Assessment
Audit on Organisational Practice	Identify	Risk Management Strategy
Framework Audit	Identify	Risk Management Strategy
Third-Party Cybersecurity Review	Identify	Risk Management Strategy
Continues Vulnerability Management	Identify	Governance
Multifactor Authentication	Protect	Identity Management, Authentication and Access Control
Safe Routes for Third-Party Asset Sharing	Protect	Identity Management, Authentication and Access Control
Mandatory Awareness Training	Protect	Awareness and Training
Data Access on Location	Protect	Data Security
Penetration Tests and physical Intrusion	Protect	Data Security
Live Reporting	Protect	Information Protection Processes and Procedures
Periodic Testing and Cyber Incident Response Planning	Protect	Protective Technology
Abnormal activities	Detect	Security Continues Monitoring
Cyberhealth and Cyber Hygiene Monitoring and Evaluation	Detect	Security Continues Monitoring
Resilience Training	Respond	Response and Recovery Planning

6. Validation of the proposed cybersecurity framework

This research concentrates on identifying the skills and tools, defining the concepts, and establishing the framework for cybersecurity in the manufacturing sector to fulfil the aims of sustainable manufacturing. To establish the framework, the study's scope includes sustainability efforts in manufacturing that are relevant to cybersecurity management, Multiple

databases, provide publications and articles for the literature on information search. The data become more explicit and dependable after the screening technique, allowing it to be used in critical evaluations that contribute to the themes and topics of interest. As a result, findings that are unrelated to the study's objectives will be excluded.

This part describes how the validation process for the framework was carried out through interviews with two experts in the field. The experts were selected, and the framework was sent to them ten days in advance to allow them to review it thoroughly. Although the interview questions were specific, the researcher was able to delve deeper into other frameworks as a result of this approach. In addition, subject-specific questions were prepared for the interview, and both experts were asked the following questions:

- Do you agree with the pillars of the proposed cybersecurity framework?
- Do you agree with the elements and components of the proposed cybersecurity framework?
- Is the cybersecurity framework including everything that is necessary?
- Do you think the framework would contribute to the cultivation of the suggested culture?
- Are there any other frameworks you know you can refer to?
- Any other comments and suggestions?

The interviews were conducted through video call and the answers were sent by email from them. We intend from this interview questions to validate our framework elements and components. In addition, the most crucial thing was to get the experts' approval that the suggested framework would contribute to the manufacturing sector. Both experts agreed that the framework's four pillars should be present, and one of them elaborated by saying:

-Yes, I agree with the pillars of the proposed cybersecurity framework, especially since it starts from the stage of identifying the security threat and this is the basis on which the rest of the pillars are built. However, the proposed framework has been generalised abstractly, which may be positive on the one hand. Still, it may require more customisation to suit organisations whose activities differ from others.

The experts submitted additional thoughts when asked if they agreed with the elements and components of the presented framework. One of the experts recommends that the proposed framework remain available for improvement based on the feedback as needed. Moreover, he continued by saying:

-The proposed framework has included eighteen elements categorised into four categories, which are the framework's pillars. This consistent association between the pillars and elements gave the proposed framework rigidity and durability in preventing potential cyber-attacks. However, the scope of the proposed framework must remain available for improvement based on the feedback as needed and according to the changes in the nature of cyber threats in the future.

Regarding the suggested framework's comprehensiveness, both experts agreed that it was. One expert said that:

-In terms of theoretical foundations, the proposed framework includes the basic principles of cybersecurity related to confidentiality, integrity, and availability. Nevertheless, this depends mainly on the nature of the organisation in which such a framework is applied, as well as the rapid changes that occur in the field of cybersecurity due to the different hackers' methods and tools, especially in the future.

Additionally, the experts were pleased with the contribution the proposed change would make. Also, the experts were optimistic about how the cybersecurity framework would contribute to the organisation's protection. Expert one increased by stating:

-As long as the proposed framework includes aspects related to training, policies, and awareness, it will contribute effectively. However, feedback and continuous evaluation must be taken into consideration.

When it comes to other existing frameworks, expert one refers that:

-The Cyber Risk Management Framework (CRMF) and Cyber Security Risk Indicator (CSRI), in terms of risk management and security incident response, are related and worth to be considered 'mainly since the proposed framework focuses on aspects related to awareness, training, policies and legislation.

Both experts had a few reservations. Expert one suggested that:

-The cybersecurity framework must be applied in stages; the monitoring and modifying phase and feedback gathering are essential. Also, due to the differences between the size of organisations and their activities, it is important to take into account these factors when applying the proposed security framework to ensure the best results are achieved to protect the organisation from cyber threats and overcome potential security risks and discover vulnerabilities as soon as possible.

However, expert two suggested applying the proposed framework with a small organisation and keeping it under the monitoring and supervision of the cybersecurity practitioner. In summary, it can be concluded that the proposed framework was sufficiently validated, according to the experts' comments.

7. Conclusion and future work

This study's key findings identify the skills and resources required to combat cyber threats and keep businesses sustainable. To enhance the existing cybersecurity measures or for those who do not have any framework in place, the proposed framework can be adopted by organizations. It should be noted that the proposed framework has the same five functions as the NIST framework, but the primary objective is to strengthen the security that is already in place. The organization can choose to comply with the suggested framework in part or in full. The cybersecurity framework could be particularly useful for medium-sized companies that do not have adequate cybersecurity measures. By adopting the framework, the organization can effectively balance the triad of availability, confidentiality, and integrity. The proposed framework can help protect the system, identify potential cyber threats, and have an appropriate incident response plan to reduce the impact of such threats. Additionally, resilience training can help the organization resume regular operations following a cyberattack. However, it should be noted that the implementation of the framework may require budget and time, and small organizations may face limitations in implementing it fully.

This study discussed the important cybersecurity concepts and identified the necessary resources and capabilities for effective cybersecurity management. A key aspect of this research was the development of a cybersecurity framework for sustainable manufacturing, based on a thorough review of existing literature and analysis. The proposed framework is

intended to enhance resource protection and safeguard data confidentiality, integrity, and accessibility by providing an additional layer of security. The framework includes proactive steps, such as predicting cyber threats, and highlights the importance of educating employees and raising awareness at all levels of the organization, as well as examining the overall cyber health of the organization across all departments. Resilience is also emphasized, which refers to an organization's ability to recover and continue operations following a cyberattack. However, implementing this framework may require a significant budget and time investment, and small organizations may face limitations in applying all aspects of the framework. Nonetheless, incorporating the framework's key functions can still provide added protection for small organizations.

The manufacturing industry is a significant contributor to the global economy, and as it advances with smarter and more efficient technologies, some issues need to be addressed. It is essential for countries with industries to provide guidelines for the manufacturing sector. However, due to the industry's varying economic scale worldwide, it can be challenging for the sector to understand precisely what to follow from the framework. To make it more useful, the framework should include guidance on how to apply it in phases across an organization's departments, with measurable targets to track progress. Further studies on cybersecurity and sustainability in the future are recommended.

The cybersecurity framework proposed in this study may not be suitable for larger organizations but can be improved in certain areas. Future research can focus on addressing the framework's limitations and shortcomings to further reduce cyber risks for sustainable manufacturing. To make it easier to understand and apply the framework, the scale of an industry based on its economy can be established. Additionally, the framework should be updated regularly to include new tools and techniques for countering cyberattacks. Furthermore, the framework could be extended to non-manufacturing businesses by including implementation strategies, making it more valuable.

References

- AlDaajeh, S., Saleous, H., Alrabae, S., Barka, E., Breiting, F. and Raymond Choo, K.K. (2022), "The role of national cybersecurity strategies on the improvement of cybersecurity education", *Computers and Security*, Elsevier Ltd, Vol. 119, p. 102754, doi: 10.1016/j.cose.2022.102754.
- Alouffi, B., Hasnain, M., Alharbi, A., Alosaimi, W., Alyami, H. and Ayaz, M. (2021), "A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies", *IEEE Access*, Institute of Electrical and Electronics Engineers Inc., Vol. 9, pp. 57792–57807, doi: 10.1109/ACCESS.2021.3073203.
- Alqudhaibi, A., Albarrak, M., Aloseel, A., Jagtap, S. and Salonitis, K. (2023), "Predicting Cybersecurity Threats in Critical Infrastructure for Industry 4.0: A Proactive Approach Based on Attacker Motivations", doi: 10.3390/s23094539.
- Alqudhaibi, A., Aloseel, A., Jagtap, S. and Salonitis, K. (2022), "Identifying and Predicting Cybersecurity Threats in Industry 4.0 Based on the Motivations Towards a Critical Infrastructure", doi: 10.3233/ATDE220599.
- Alshaikh, M., Maynard, S.B. and Ahmad, A. (2019), *TOWARD SUSTAINABLE BEHAVIOUR CHANGE: AN APPROACH FOR CYBER SECURITY EDUCATION TRAINING AND AWARENESS* Information Security Strategy in Organisations View Project Information Security Management Practices in Organisations View Project.
- Ani, U.P.D., He, H. (Mary) and Tiwari, A. (2017), "Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective", *Journal of Cyber Security Technology*, Vol. 1 No. 1, pp. 32–74, doi: 10.1080/23742917.2016.1252211.
- Barrett, M. (2018), *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*, Gaithersburg, MD, doi: 10.6028/NIST.CSWP.04162018.
- Borky, J.M. and Bradley, T.H. (2019), "Protecting Information with Cybersecurity", *Effective Model-Based Systems Engineering*, Springer International Publishing, Cham, pp. 345–404, doi: 10.1007/978-3-319-95669-5_10.
- Buehler, K., Anant, V., Bailey, T., Kaplan, J., Nayfeh, M. and Richter, W. (2020), *Digital McKinsey and Global Risk Practice- Cybersecurity in a Digital Era*, McKinsey & Company.
- Cormier, A. and Ng, C. (2020), "Integrating cybersecurity in hazard and risk analyses", *Journal of Loss Prevention in the Process Industries*, Vol. 64, p. 104044, doi: 10.1016/j.jlp.2020.104044.

- Culot, G., Fattori, F., Podrecca, M. and Sartor, M. (2019), “Addressing Industry 4.0 Cybersecurity Challenges”, *IEEE Engineering Management Review*, Vol. 47 No. 3, pp. 79–86, doi: 10.1109/EMR.2019.2927559.
- Donalds, C. and Osei-Bryson, K.-M. (2020), “Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents”, *International Journal of Information Management*, Vol. 51, p. 102056, doi: 10.1016/j.ijinfomgt.2019.102056.
- Efthymiopoulos, M.P. (2019), “A cyber-security framework for development, defense and innovation at NATO”, *Journal of Innovation and Entrepreneurship*, Vol. 8 No. 1, p. 12, doi: 10.1186/s13731-019-0105-z.
- Hajj, R., Peasley, S., Hunt, J., Manolian, H. and Beckoff, D. (2020), “Cyber security for smart factories ”, *Deloitte*, available at: <https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/cybersecurity-for-smart-factories.pdf> (accessed 24 March 2023).
- Iqbal, A., Zhao, G., Suhaimi, H., He, N., Hussain, G. and Zhao, W. (2020), “Readiness of subtractive and additive manufacturing and their sustainable amalgamation from the perspective of Industry 4.0: a comprehensive review”, *The International Journal of Advanced Manufacturing Technology*, Vol. 111 No. 9–10, pp. 2475–2498, doi: 10.1007/s00170-020-06287-6.
- Jagtap, S., Trollman, H., Trollman, F., Garcia-Garcia, G., Parra-López, C., Duong, L., Martindale, W., et al. (2022), “The Russia-Ukraine Conflict: Its Implications for the Global Food Supply Chains”, *Foods*, Vol. 11 No. 14, p. 2098, doi: 10.3390/foods11142098.
- Kamarul Bahrin, M.A., Othman, M.F., Nor Azli, N.H. and Talib, M.F. (2016), “INDUSTRY 4.0: A REVIEW ON INDUSTRIAL AUTOMATION AND ROBOTIC”, *Jurnal Teknologi*, Vol. 78 No. 6–13, doi: 10.11113/jt.v78.9285.
- Katal, A., Dahiya, S. and Choudhury, T. (2022), “Energy efficiency in cloud computing data centers: a survey on software technologies”, *Cluster Computing*, Springer, doi: 10.1007/s10586-022-03713-0.
- Kavallieratos, G., Katsikas, S. and Gkioulos, V. (2020), “Cybersecurity and safety co-engineering of cyberphysical systems - A comprehensive survey”, *Future Internet*, MDPI AG, Vol. 12 No. 4, doi: 10.3390/FI12040065.
- Lewis, R., Louvieris, P., Abbott, P., Clewley, N. and Jones, K. (2014), “Cybersecurity Information Sharing: a Framework for Sustainable Information Security Management in UK SME Supply Chains”, *22nd European Conference on Information Systems, ECIS 2014*, Tel Aviv.

- Li, L., He, W., Xu, L., Ash, I., Anwar, M. and Yuan, X. (2019), "Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior", *International Journal of Information Management*, Vol. 45, pp. 13–24, doi: 10.1016/j.ijinfomgt.2018.10.017.
- Machado, C.G., Winroth, M.P. and Ribeiro da Silva, E.H.D. (2020), "Sustainable manufacturing in Industry 4.0: an emerging research agenda", *International Journal of Production Research*, Taylor & Francis, Vol. 58 No. 5, pp. 1462–1484, doi: 10.1080/00207543.2019.1652777.
- Miller, T., Staves, A., Maesschalck, S., Sturdee, M. and Green, B. (2021), "Looking back to look forward: Lessons learnt from cyber-attacks on Industrial Control Systems", *International Journal of Critical Infrastructure Protection*, Elsevier B.V., Vol. 35, doi: 10.1016/j.ijcip.2021.100464.
- Mullet, V., Sondi, P. and Ramat, E. (2021), "A Review of Cybersecurity Guidelines for Manufacturing Factories in Industry 4.0", *IEEE Access*, Vol. 9, pp. 23235–23263, doi: 10.1109/ACCESS.2021.3056650.
- Naseer, A., Naseer, H., Ahmad, A., Maynard, S.B. and Masood Siddiqui, A. (2021), "Real-time analytics, incident response process agility and enterprise cybersecurity performance: A contingent resource-based analysis", *International Journal of Information Management*, Vol. 59, p. 102334, doi: 10.1016/j.ijinfomgt.2021.102334.
- National Institute of Standards and Technology. (2018), *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*, Gaithersburg, MD, doi: 10.6028/NIST.CSWP.04162018.
- Pfeiffer, S. (2017), "The Vision of 'Industrie 4.0' in the Making—a Case of Future Told, Tamed, and Traded", *NanoEthics*, Vol. 11 No. 1, pp. 107–121, doi: 10.1007/s11569-016-0280-3.
- Rameem Zahra, S., Ahsan Chishti, M., Iqbal Baba, A. and Wu, F. (2022), "Detecting Covid-19 chaos driven phishing/malicious URL attacks by a fuzzy logic and data mining based intelligence system", *Egyptian Informatics Journal*, Vol. 23 No. 2, pp. 197–214, doi: 10.1016/j.eij.2021.12.003.
- Sabillon, R., Serra-Ruiz, J., Cavaller, V. and Cano, J. (2018), "A comprehensive cybersecurity audit model to improve cybersecurity assurance: The cybersecurity audit model (CSAM)", *Proceedings - 2017 International Conference on Information Systems and Computer Science, INCISCOS 2017*, Institute of Electrical and Electronics Engineers Inc., Vol. 2017-November, pp. 253–259, doi: 10.1109/INCISCOS.2017.20.

- Sadik, S., Ahmed, M., Sikos, L.F. and Najmul Islam, A.K.M. (2020), "Toward a sustainable cybersecurity ecosystem", *Computers*, MDPI AG, Vol. 9 No. 3, pp. 1–17, doi: 10.3390/computers9030074.
- Schlatt, V., Guggenberger, T., Schmid, J. and Urbach, N. (2023), "Attacking the trust machine: Developing an information systems research agenda for blockchain cybersecurity", *International Journal of Information Management*, Vol. 68, p. 102470, doi: 10.1016/j.ijinfomgt.2022.102470.
- Shafae, M.S., Wells, L.J. and Purdy, G.T. (2019), "Defending against product-oriented cyber-physical attacks on machining systems", *International Journal of Advanced Manufacturing Technology*, Springer, Vol. 105 No. 9, pp. 3829–3850, doi: 10.1007/s00170-019-03805-z.
- Shahin, M., Chen, F.F., Bouzary, H., Hosseinzadeh, A. and Rashidifar, R. (2022), "A novel fully convolutional neural network approach for detection and classification of attacks on industrial IoT devices in smart manufacturing systems", *International Journal of Advanced Manufacturing Technology*, Springer Science and Business Media Deutschland GmbH, doi: 10.1007/s00170-022-10259-3.
- Shahin, M., Chen, F.F., Hosseinzadeh, A., Bouzary, H. and Rashidifar, R. (2022), "A deep hybrid learning model for detection of cyber attacks in industrial IoT devices", *International Journal of Advanced Manufacturing Technology*, Springer Science and Business Media Deutschland GmbH, doi: 10.1007/s00170-022-10329-6.
- Shi, P., Qin, F., Cheng, R. and Zhu, K. (2019), "The penetration testing framework for large-scale network based on network fingerprint", *Proceedings - 2019 International Conference on Communications, Information System, and Computer Engineering, CISCE 2019*, Institute of Electrical and Electronics Engineers Inc., pp. 378–381, doi: 10.1109/CISCE.2019.00089.
- Tounsi, W. and Rais, H. (2018), "A survey on technical threat intelligence in the age of sophisticated cyber attacks", *Computers and Security*, Elsevier Ltd, 1 January, doi: 10.1016/j.cose.2017.09.001.
- Vincent, M. (2022), "In charts: Industry leaders gain 'false sense of cyber security'", *Financial Times*, 1 June.
- Wong, L.-W., Lee, V.-H., Tan, G.W.-H., Ooi, K.-B. and Sohal, A. (2022), "The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities", *International Journal of Information Management*, Vol. 66, p. 102520, doi: 10.1016/j.ijinfomgt.2022.102520.

Wong, L.-W., Tan, G.W.-H., Ooi, K.-B. and Dwivedi, Y. (2023), “The role of institutional and self in the formation of trust in artificial intelligence technologies”, *Internet Research*, doi: 10.1108/INTR-07-2021-0446.



DSPACE

<https://dspace.org/>

Towards a sustainable future: developing a cybersecurity framework for manufacturing

Alqudhaibi, Adel; Deshpande, Sourav; Jagtap, Sandeep; Salonitis, Konstantinos

2023-10-30

Emerald

<https://doi.org/10.1108/TECHS-05-2023-0022>

Alqudhaibi A, Deshpande S, Jagtap S, Salonitis K (2023) Towards a sustainable future: developing a cybersecurity framework for manufacturing. Technological Sustainability, Volume 2, Issue 4, October 2023, pp. 372-387