Securing Industry 4.0: Assessing Cybersecurity Challenges and Proposing Strategies for Manufacturing Management

Alqudhaibi, Adel; Albarrak, Majed; Jagtap, Sandeep; Williams, Nikki; Salonitis, Konstantinos

Published in:
Cyber Security and Applications

DOI:
10.1016/j.csa.2024.100067

2025

Document Version:
Publisher's PDF, also known as Version of record

Cyber Security and Applications 3 (2025) 100067

Contents lists available at ScienceDirect

Cyber Security and Applications

journal homepage: http://www.keaipublishing.com/en/journals/cyber-security-and-applications/

Securing industry 4.0: Assessing cybersecurity challenges and proposing strategies for manufacturing management

Adel Alqudhaibi[a], Majed Albarrak[b], Sandeep Jagtap[a,c,*], Nikki Williams[a], Konstantinos Salonitis[a]

[a] Sustainable Manufacturing Systems Centre, Cranfield University, Cranfield MK43 0AL, United Kingdom
[b] University of Warwick, Coventry CV4 7AL, United Kingdom
[c] Division of Engineering Logistics, Faculty of Engineering, Lund University, Lund 22643, Sweden

ARTICLE INFO

Keywords:
Cybersecurity
Manufacturing systems
Industry 4.0
Cybersecurity challenges
Cybersecurity awareness
Cybersecurity framework

ABSTRACT

Industry 4.0 represents the foundation of the fourth industrial revolution, characterised by the integration of innovative technology into the manufacturing process. This integration enhances automation, diagnostics, data analysis, and autonomous decision-making through the networking of equipment and machinery. However, the increased reliance on technology raises concerns about the implementation and maintenance of cybersecurity. This paper aims to address cybersecurity challenges in the manufacturing industry and suggest strategies to reduce risks. In particular, it examines the level of awareness and understanding of cybersecurity issues among manufacturing employees, establishes accountability for cyberattacks, and evaluates the effectiveness of existing industry practices. The current cybersecurity landscape in the manufacturing industry was thoroughly analysed. Data were gathered through surveys, interviews, and case studies to measure awareness, identify knowledge gaps, and assess existing practices. The research findings indicate a significant knowledge gap regarding cybersecurity among manufacturing employees. This vulnerability can be attributed to the lack of funding and training, especially compared to the resources provided to information technology departments and corporate employees. The study emphasises the importance of redirecting cybersecurity resources and protocols towards the manufacturing industry. This paper puts forward a series of recommendations to mitigate risks and safeguard the manufacturing industry.

1. Introduction

Contemporary manufacturing companies utilise a range of hardware and software to ensure the confidentiality, availability, and integrity of data, which are essential factors for long-term success and profitability. In line with the Industry 4.0 revolution, many companies are integrating their manufacturing systems and machinery to improve efficiency and competitiveness. However, this integration poses significant implementation challenges, especially in emerging countries where prioritising investment in shop-floor digitalisation and understanding cybersecurity requirements are crucial for successful adoption [1]. This integration is driven by the projected use of over United States dollar (USD) 12 billion internet-connected devices in manufacturing by 2022, as shown in Fig. 1, representing a 50 % increase since 2018 [2,3]. Integrating advanced technologies such as virtual manufacturing is becoming increasingly critical in this context, enabling manufacturers to design, test, and optimise their processes in a virtual environment before actual production, thus enhancing efficiency and reducing costs [5]. However, with the rise in connectivity, there has been an alarming increase in the number and severity of cyberattacks. In fact, over a third of reported cyberattacks in 2016 were targeted at connected manufacturing assets, as depicted in Fig. 2. According to information provided by NTT (May 2021), cyberattacks against the manufacturing industry have increased by 300 % compared to 2019 [6].

A report by National Institute of Standards and Technology (NIST) [7] suggests that the increase in attacks indicates that security measures for manufacturing industry systems are generally not as strong as those in corporate information technology (IT) environments. Despite the growing cyber threats, there is a significant knowledge gap among manufacturing employees when it comes to cybersecurity. This gap is worsened by a disparity in cybersecurity funding and training compared to IT departments. This paper aims to investigate whether local users of integrated, networked systems in the manufacturing sector are aware of cyber threats and whether their roles, experiences, and responsibilities are suitable for effectively managing this threat. Additionally, the study aims to bridge the existing knowledge gap by developing

Peer review under responsibility of KeAi Communications Co., Ltd.
* Corresponding author at: Division of Engineering Logistics, Faculty of Engineering, Lund University, Lund 22643, Sweden.
E-mail addresses: s.z.jagtap@cranfield.ac.uk, sandeep.jagtap@tlog.lth.se (S. Jagtap).

https://doi.org/10.1016/j.csa.2024.100067
Received 24 May 2024; Received in revised form 9 July 2024; Accepted 27 July 2024
Available online 29 July 2024

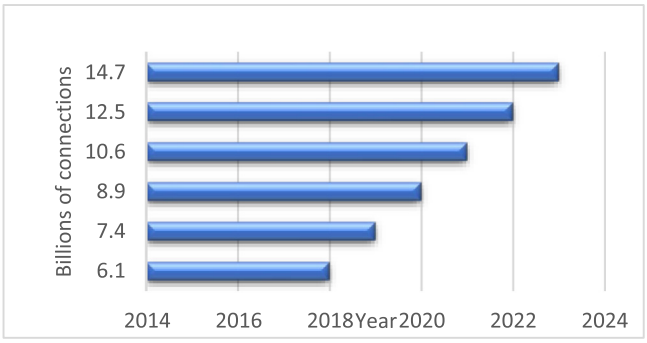

Fig. 1. Global growth of machine-to-machine connections [4].

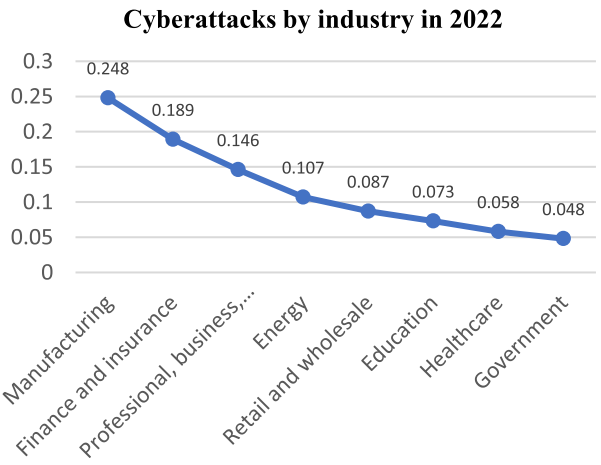

Fig. 2. Cyberattacks by industry in 2022 [7].

and implementing engaging activities to educate all stakeholders. Furthermore, the study is systematically addressed through four distinct but interrelated objectives: Firstly, it evaluates published research on cyber security in manufacturing environments to establish best practices. Secondly, it assesses current cyber security knowledge, experiences, and accountability beliefs within various manufacturing functions of an established aerospace manufacturing company, using a detailed survey. Thirdly, it analyses the data collected from this survey to determine a current representative baseline for cyber security awareness and to compare this with existing literature to identify gaps and opportunities for improvement. Finally, it proposes a future strategy aimed at either improving or maintaining a robust understanding of cyber security within manufacturing functions. These objectives collectively drive the comprehensive analysis and strategic recommendations our paper presents. As manufacturing organisations increasingly connect their equipment and assets to improve data accessibility, there is often a delay in adequately training staff who may be unaware of their roles, responsibilities, and obligations in creating and maintaining a cyber-secure environment. This paper investigates the effectiveness of current industry practices in addressing cybersecurity implementation. The following sections of this paper explore the literature review, research methodology, findings, and recommendations, offering a thorough understanding of the awareness and preparedness of manufacturing employees in addressing cybersecurity threats.

2. Literature review

2.1. Cybersecurity and its associated risks

Cybersecurity refers to the measures individuals and institutions take to mitigate cyberattack threats, protect hardware and services from theft or damage, and prevent unauthorised access to data [8]. With the widespread use of connected devices, there has been an abundance of guidance, standards, regulations, and incident management services provided by private and government cybersecurity agencies, institutes, and consultants [9]. The National Cyber Security Centre has published guidance to help board members understand cybersecurity [10,11]. Recently, the number of identified cyberattacks has reached a level where certain incidents make global news headlines, such as the US fuel pipeline attack and the WannaCry and NotPetya ransomware attacks [12]. However, these examples represent only a small portion of the actual attacks. Numerous prominent companies, including Adobe, eBay, and LinkedIn, have fallen victim to cyberattacks, resulting in data breaches and subsequent data loss over the past decade [10].

These incidents have raised awareness about the threats of cyberattacks. According to a survey conducted by Microsoft [11], 22 % of companies considered cyber threats to be the most significant risk to their business operations. Furthermore, it has been observed that cyberattacks have wide-ranging effects [13]. A study carried out by Oxford University identified five themes that encompass the concept of cyber harm: social, reputational, psychological, economic, and physical or digital harm [14]. The Microsoft survey and the Oxford University study remind us of the clear consequences of cyberattacks on businesses, such as operational disruptions, decreased stock prices, and regulatory fines. However, equal attention should be given to the less obvious effects, including loss of life, compromised consumer interactions, reduced organisational morale, and increased media scrutiny [15].

The increased awareness of cyberattacks has resulted in higher sales of business cyber insurance [16]. According to a recent report, the cyber insurance market is expected to grow at a compound annual growth rate of 21 %, reaching a value of USD 20.4 billion by 2025 [17]. The term ‘cyberattack’ refers to a deliberate attempt to undermine business operations by using programmes like viruses to breach a company’s servers [18]. On the other hand, ‘cybersecurity’ encompasses the measures taken to prevent or minimise the impact of such attacks [19]. A report by Hiscox highlights a significant increase in business spending on cybersecurity, with the average business now allocating over 20 % of its IT budget to address this threat [20].

All current approaches offered by leading consultancy firms and institutions, with regard to effective cybersecurity, revolve around five key components: identification, protection, detection, response, and recovery [21]. By identifying these five principles, firms can minimise their vulnerability to cyberattacks by outlining procedures for identifying, protecting against, detecting, responding to, and recovering from such attacks. Effective cybersecurity follows a similar structure to conventional risk management strategies: it is most effective when regularly reviewed and monitored, when staff possess a strong awareness and understanding of the security measures, when protocols are vigorously applied, and when resources and funds are efficiently utilised to mitigate, monitor, and manage the impacts of any cyberattack.

The analysis conducted in the study by Galinec et al. [22] highlights the importance of addressing issues that arise from inadequate employee education or awareness. Even a single employee who is unaware or uneducated can unintentionally undermine even the most comprehensive cybersecurity strategy. The European Union Agency for Cybersecurity [23] advocates for involving proactive employees in achieving effective cybersecurity, going beyond mere compliance with rules and policies, as these regulations may need to catch up with current cyber threats. This dual approach is further supported by the National Initiative for Cybersecurity Education framework, which recognises the need to establish a continuum of cybersecurity, its relationship with the IT department, and its crucial relationship with all work roles across the organisation [24].

2.2. Manufacturing sector systems

The term ‘manufacturing sector systems’ covers a well-established and extensively researched topic that includes two distinct areas: IT

and operation technology (OT), which are often referred to by the same name [25]. According to the dictionary of production engineering, manufacturing sector systems include the people, equipment, procedures, and organisations aimed at achieving a company's manufacturing objectives [26]. While this definition gives a broad description of the necessary systems for efficient business operations, this research focuses on the specific technology used in production spaces to monitor and enhance the production process.

Existing research primarily focuses on IT, which involves managing digital information and has historically been associated with office environments [27]. On the other hand, OT is commonly linked to the factory floor and oversees the control of physical processes and the technology utilised to carry out those processes [28]. However, some argue that the line between IT and OT has become blurred in recent times, making these terms less helpful [29]. Modern manufacturing companies now incorporate many digital elements into their operations, so this research needs to take into account all manufacturing systems alongside established OT devices.

2.3. Importance of cybersecurity in manufacturing

A recent report conducted on behalf of Deloitte revealed that nearly one-third of manufacturers have not yet implemented a cyber risk assessment specifically targeting their factory floor technology [30]. These statistics, combined with the increased adoption of connected devices and systems in manufacturing, have made the industry highly susceptible to cybercrime.

Traditional IT applications, which are used to handle data and manufacturing complexities, are increasingly being incorporated into OT systems [31]. The growing practice of utilising IT platforms to host vital OT applications, like human-machine interfaces, presents a range of intricate challenges and cybersecurity risks [32]. Originally, OT devices were kept isolated (air-gapped) to protect them from external attacks and reduce associated risks [33]. However, the decision to connect them to manufacturing networks has raised concerns, especially when considering hardware with redundant and unprotected operating systems, as well as the absence of fundamental security features like encryption and user authentication [34].

The outbreak of COVID-19 forced companies to embrace a remote working approach, which led to a rise in cyberattacks due to hastily implemented access requirements [35]. The Cybersecurity & Infrastructure Security Agency frequently issues alerts regarding cybercriminals who specifically target businesses by exploiting vulnerabilities in internet-accessible manufacturing resources and stealing access credentials from supervisory personnel [36]. This allows attackers to circumvent firewalls and gain entry to factory floor connections and machinery [33].

Recent high-profile attacks on manufacturing businesses include the well-known WannaCry and NotPetya incidents. In these cases, viruses were able to spread from IT network systems to manufacturing devices that were easily accessible [37]. As a result, organisations worldwide experienced extensive disruptions, leading to losses exceeding USD 14 billion [38].

2.4. Cybersecurity challenges in manufacturing

Previous literature has identified two main areas of vulnerability in manufacturing cybersecurity: technology and personnel [39,40]. One study emphasised the significance of considering technology, personnel, and procedures equally in order to achieve effective cybersecurity [41]. In terms of technology, as highlighted by this study, it is clear that the use of outdated and unsupported hardware and software creates a manufacturing environment where critical, yet vulnerable, devices are connected to an insecure network, thereby increasing the risk of cyberattacks [42].

The second group focuses on people, and according to University of Phoenix and ISC(2) [43], who conducted a report on cybersecurity workforce competencies, 'inexperienced end-users and dissatisfied workers' and 'user lack of knowledge about new cybercrime tactics' are two major contributing factors to significant cybersecurity breaches. An investigation into the cyberattacks on the control systems of the Ukrainian power grid in 2015/2016 revealed that the attack patterns used by the cybercriminals were similar to those documented in previous incidents against enterprise IT systems [32]. The attack employed spear-phishing techniques that targeted employees and system administrators [44], highlighting the importance of having an informed and well-educated workforce to mitigate such attacks.

A business that emphasises security, by involving employees and implementing clear procedures, creates an environment that tackles numerous underlying issues that contribute to data breaches [45]. Additionally, this helps develop a workforce that instinctively safeguards company information, thus ensuring strong cybersecurity [46,47]. It is acknowledged that a person's behaviour is influenced by their knowledge, skills, familiarity with cybersecurity, experiences, perspectives, mindsets, and beliefs [48]. Considering the demands of their roles, manufacturing employees often require extra time to contemplate the implications of cybersecurity, which makes establishing a more conscientious culture challenging [49].

Employees play a crucial role in implementing, utilising, and maintaining an effective cybersecurity policy [50]. To establish effective organisational cybersecurity, senior employees must follow a four-step process: identifying the company's critical assets, developing an understanding of relevant threats, designing procedures to prevent cybercrime, and educating and engaging staff [51]. The final step is particularly crucial, as it should not only provide information but also emphasise practicality, ease of implementation, and viability. Likewise, management personnel responsible for finance and resource allocation, such as machine operators, often require additional time to address cybersecurity issues, which hampers efforts to bring about change. Manufacturing leadership must actively support the implementation of cybersecurity measures and awareness, employing the same logic that initially led to the adoption of connected devices. The potential impact of a cyberattack should be considered as detrimental to the business as removing the systems [52].

Laperrière and Reinhart [26] identifies a challenge arising from the difference between IT culture, which prioritises confidentiality, and manufacturing culture, which emphasises availability. Historical disparities between IT and OT approaches have exacerbated this division. However, the collaboration between IT and manufacturing employees is essential in the current production environment to enhance cybersecurity [54]. An often-overlooked factor when analysing complex manufacturing organisations involves the utilisation of small or medium-sized businesses (SMBs) to supply, maintain, and upgrade manufacturing machinery, making them potential targets for cyberattacks [55]. SMBs often need assistance in implementing effective cybersecurity measures due to a lack of in-depth knowledge, expertise, and resources [56]. This issue has been extensively discussed in academic studies, industry accounts, and government support initiatives [48–57]. Despite the cybersecurity risks it poses to larger companies, SMBs will continue to be impacted by this issue due to resource and economic constraints [58].

2.5. Evaluating cybersecurity culture in manufacturing

Corporate culture coexists with formal corporate policies and embodies an informal directive, where formal rules are complemented by secondary, less formal understandings and practices [41]. While the link between corporate culture and company performance is widely acknowledged, efforts to measure culture and its correlation with performance have frequently yielded limited results [59]. Surveys, however, provide a valuable way to comprehend workforce attitudes, identify trends, and identify areas for improvement and consolidation. Several examples illustrate the use of survey-based approaches in evaluating manufacturing organisations. For example, the Manufacturing En-

Table 1
Services for cybersecurity consultancy.

Firm	Tasks and services	Associated action
Governance of IT	Consultancy service reviewing and auditing	Auditing and evaluating employee involvement.
Jaw Consulting	IT health check for weakest security areas	User awareness and training.
Fujitsu	Risk assessment and asset discovery.	Technology interviews and people process.
Romano Security Consulting	Cybersecurity audits	Emphasise staff education and awareness.

terprise Systems Association and the Manufacturing Operations Management/Capability Maturity Model developed a survey with 832 questions to evaluate the development and capability of production companies from a factory operations perspective [60]. Another survey-based approach, the Smart Manufacturing System Readiness Assessment, was designed to evaluate the readiness of a manufacturing environment to adopt smart manufacturing technologies [61]. While these approaches are valuable tools, neither they nor the subsequent literature associated with them specifically address cybersecurity. Dojkovski et al. [46] acknowledges that changing people's cybersecurity behaviours is challenging, given the difficulty of precisely measuring individuals' current knowledge, overlooked knowledge, and knowledge gaps. Nonetheless, some profitable consultancy firms specialise in providing advice on cybersecurity issues and conducting risk assessments [62]. A review of their prospectuses reveals that all of them include an employee evaluation component, as shown in Table 1.

A Deloitte report on cyber risk in advanced fabrication companies highlighted that 'Increasingly, people are the greatest cybersecurity risk; whether the intent is malicious or not, they are our most significant liability' [63]. The reviewed literature consistently emphasises that the workforce's comprehension and involvement in cybersecurity policies are the most crucial elements of a company's cybersecurity strategy [10,46].

Most existing literature indicates a difference between IT personnel, who are aware of the cybersecurity risks associated with manufacturing but focus on simple improvements such as securing vulnerable equipment through software patches, and the manufacturing workforce, who prioritise operations, data, and system availability and show indifference towards cybersecurity [64]. This conflict causes frustration among manufacturing personnel and increases the chances of bypassing security measures to implement local improvements [65]. Developing policies that aim to enhance the engagement, understanding, and practices of the manufacturing workforce will provide valuable insights for driving future strategies.

In conclusion, manufacturers have demonstrated an increasing tendency to network their equipment, enhance data accessibility, and take advantage of the opportunities provided by modern technology. Nevertheless, the integration of existing IT and OT technologies has outpaced the development of employee awareness and comprehension. The disconnect between the IT department and manufacturing is apparent in their approaches to cybersecurity: IT operations are becoming more proficient with production technology, while the manufacturing department has a limited understanding of the IT cybersecurity culture.

3. Survey design and method

3.1. Research method

This study utilised a survey as its main method of data collection because it has the ability to outline the data collection process and facilitate analysis and interpretation through specific analysis tools. Table 2 assesses research tools and ultimately selects the questionnaire approach. This approach was chosen because it enables data collection from a large number of participants and, when combined with anonymity, encourages honesty. The questionnaire was created and distributed using Qualtrics, an online tool that enables users to create, evaluate, share, and analyse questionnaires across multiple connected devices. The process of creating the questionnaire involved nine key steps. These steps included training and guidance on using Qualtrics, conducting research for question development, performing mock surveys, drafting the questionnaire, collecting user feedback, distributing a pilot version, seeking input from cybersecurity experts, finalising and publishing the questionnaire, and ultimately distributing it. The literature review confirmed the importance of using a high-quality questionnaire, leading to the addition of extra checkpoints for feedback during the questionnaire preparation process. The methodology flowchart for this research is shown in Table 2.

3.2. Questionnaire development

The creation of the questionnaire involved dividing the process into nine essential steps, as previously explained. Extensive literature research highlighted the crucial connection between the quality of the questionnaire and the attainment of reliable results. Therefore, the process of developing the questionnaire included several feedback checkpoints. Furthermore, the research emphasised the importance of question wording, highlighting that the language chosen significantly affects the responses received. Generally, questions should be concise, clear, and specific [66]. To improve the accuracy of responses and streamline the analysis that follows, it is recommended to minimise or eliminate open-ended questions [67,68]. The literature also emphasises the importance of aligning the design of the questionnaire with the objectives of the data analysis. This ensures that the questions asked contributes effectively to the overall goals and allows for a reduction in the total number of questions [69].

4. Results and discussion

4.1. Analysis approach

Following the data collection phase of the research, the responses were examined for errors, and only one incorrect selection was identified: one respondent described their employment as 'other' but contradicted themselves in the free-text field by selecting a department of manufacturing. To ensure consistency across the answers, a manual correction was made. Additionally, the responses of a single participant who indicated being employed in the IT function were excluded to avoid potential bias. Although certain roles received less feedback, the study gathered responses from a total of 144 employees, providing a satisfactory range of data to offer an illustrative perspective. The Microsoft BI software was used to analyse and present the results through the creation of reporting dashboards. The outcomes produced by this programme are interactive and easy to use, promoting greater engagement for the senior stakeholders who were part of the audience. The results examined in the following sections include excerpts from these dashboards.

4.2. General cybersecurity awareness

These surveys were conducted to evaluate employees' overall understanding of cybersecurity and their sense of accountability and personal responsibility. The findings show that the majority of respondents acknowledge their responsibility for upholding cybersecurity in their daily work, with fewer than 20 % providing a negative response. Likewise, an equal number of positive responses were received regarding the importance placed on cybersecurity in the manufacturing industry (see Fig. 3).

Table 2
Evaluation of research tools.

Method	Size of the sample		Bias in samples		Integrity of results		Analyse the results		Avg score
	Remarks	Score	Remarks	Score	Remarks	Score	Remarks	Score	
Questionnaire	Expect a mixed reaction, as non-personal distribution may influence engagement with a large audience, and follow-up is not possible.	8	The bias participation is less risky; we still anticipate a higher level of input from candidates who have a vested interest.	6	The anonymous technique increases the likelihood of truthful responses.	8	Assured qualitative data that will facilitate straightforward analysis.	10	8
Interview	Expect varied uptake. The duration of the interview might deter some. We can follow up to boost engagement.	6	There is a potential risk of bias favouring the involvement of applicants who have a vested interest in the issue.	4	There is a risk that answers may be biased and influenced by the interview setting, potentially leading to less truthful responses.	6	Converting interview output into quantitative data for comparison.	6	5.5
Corporate Data	It is challenging to make precise forecasts, but we anticipate that the available data will be quite limited.	6	It is difficult to forecast, but accessible data is likely to favour increasingly advanced, proactive production environment.	2	There is a chance that data will be erroneous or biased unknowingly.	4	There is a good likelihood that the data will be qualitative and easily evaluated.	8	5
Surveillance	There will be additional issues stemming from research ethics and participation concerns.	2	Controlling sampling bias and ensuring that all areas/functions are covered.	10	The surveillance approach may result in a variable likelihood of obtaining honest responses because subjects are aware of being under observation.	6	The surveillance approach can be structured to yield quantitative data, simplifying the analysis process.	8	6.5

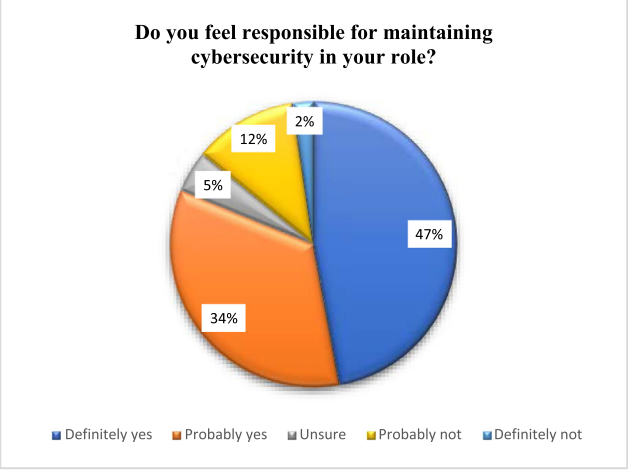

Fig. 3. Responsibility for cybersecurity.

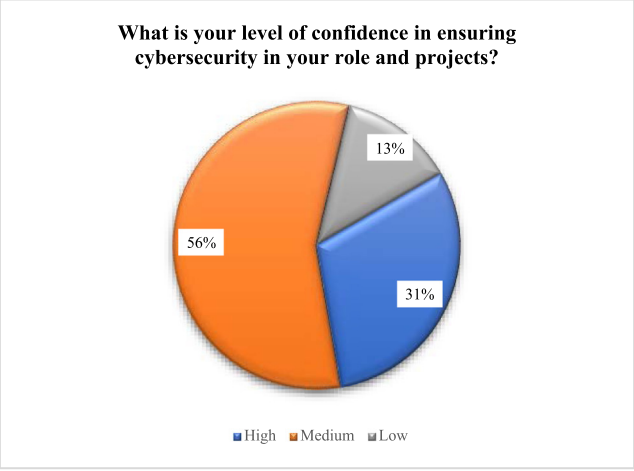

Fig. 4. Confidence in cybersecurity.

In contrast, the responses were less positive when asked about their level of confidence in strong cybersecurity and who they should notify in the event of a cyberattack. The available answer options received an equal number of responses, and only 25 % of respondents selected high confidence as their answer (see Fig. 4). No noticeable patterns were observed in any of the cybersecurity awareness questions when compared to the employee's business field, purpose, or role. These outcomes clearly highlight the contrast between individuals' awareness and their intention to follow correct procedures, as well as their proficiency, knowledge, and connections needed to achieve desired cybersecurity outcomes.

4.3. Equipment changes and cybersecurity

These questions were created to measure the respondents' understanding of the importance of maintaining strong cybersecurity practices when obtaining, upgrading, or supervising equipment. Out of the respondents surveyed, 55 individuals, which accounts for 45 % of the total, confirmed that they were responsible for specifying or installing new equipment. The idea of Industry 4.0, commonly known as 'Smart Factories', has been thoroughly examined in current literature. The findings of this research emphasise a significant trend towards interconnectedness within the manufacturing industry (see Fig. 5).

Overall, participants responded positively regarding the attention given to cybersecurity during equipment changes, with 69 % stating that they 'always' or 'most of the time' consider it. However, when asked about cybersecurity protocols and guidance concerning equipment, only 22 % answered affirmatively. This aligns with earlier responses suggesting a need for improved user knowledge and adequate guidance. In terms of software compliance reviews, the data indicates infrequent occurrences, with over 50 % of respondents selecting 'unsure' or 'never' (see Fig. 6). Additionally, only 68 % of responses indicated that equipment modifications are regularly reviewed within local network schematics.

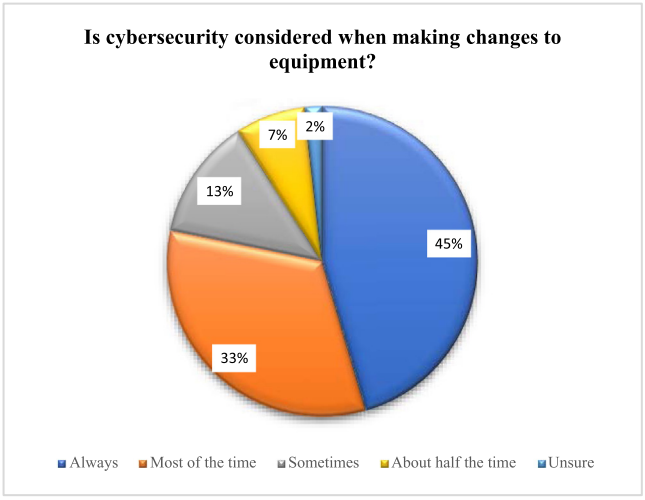

Fig. 5. Equipment connected to the network.

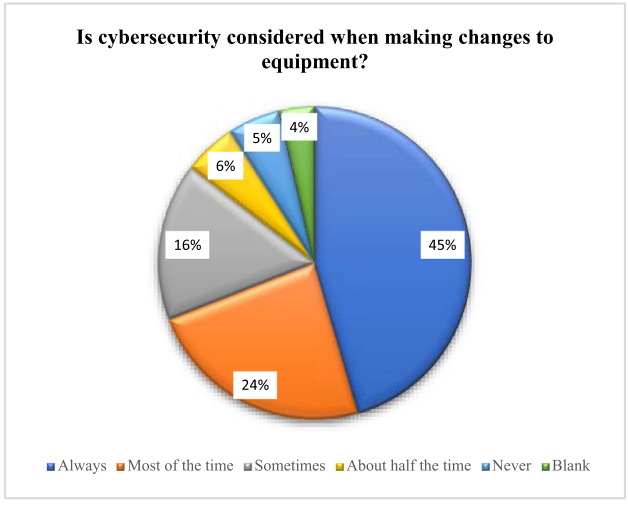

Fig. 6. Accountability for equipment.

Initially, there was a concern that the inclusion of an unequal number of employees from Capability Acquisition and Manufacturing Services, who are responsible for setting up and overseeing equipment, might have a negative impact on this dataset. However, a detailed analysis revealed that this concern was unfounded. The final questions in this section relate to employee experiences over the past two years.

Approximately 50 % of the respondents reported observing worrisome actions and procedures related to the installation and maintenance of hardware connections (refer to Fig. 7). This statistic highlights the existence of employee dissatisfaction. Employees noted that using approved secure channels to arrange equipment connections is difficult and inefficient, frequently impeding performance targets and deadlines. As a result, project teams and employees opt for the quicker solution of bypassing IT security protocols and connecting directly to the equipment.

4.4. Data management and cybersecurity

The survey questions were designed to evaluate respondents' knowledge, confidence, and experiences in relation to data management in manufacturing systems. These questions were specifically targeted at individuals who responded 'yes' to the scoping question 'Are you responsible for configuring, saving, uploading, or auditing data in manufacturing systems?' in order to ensure precise results. A total of 58 candidates,

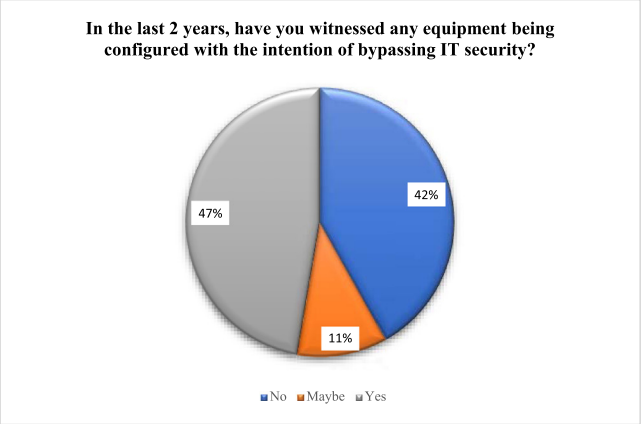

Fig. 7. Experiences of equipment connection.

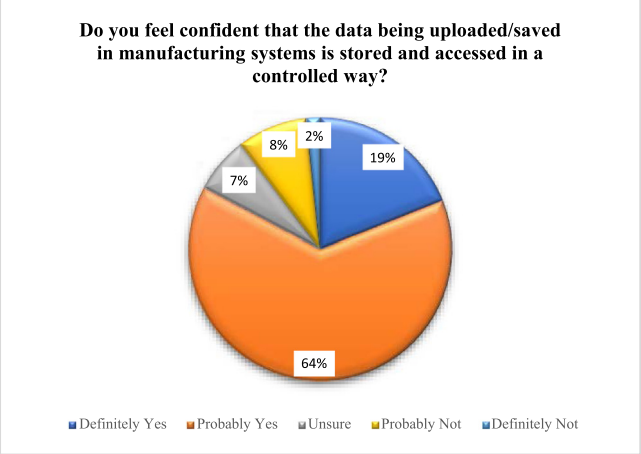

Fig. 8. Data management.

which makes up 84 % of the surveyed individuals, affirmed this responsibility. In terms of data storage and administration, more than 82 % of the respondents expressed their belief that data in manufacturing systems is stored and accessed in an organised manner, with the majority choosing 'definitely yes' or 'probably yes' (refer to Fig. 8). When evaluating their confidence in the organisation of the data, approximately 80 % of participants selected the highest rating. These findings emphasise the positive employee awareness and understanding of data management practices.

Despite the encouraging findings regarding employee awareness, 60 % of participants reported that internal data related to manufacturing systems had been externally accessible in the past two years (refer to Fig. 9). These results were expected, considering that the participants, who are employees in the manufacturing industry with cyber awareness, frequently encounter such incidents. The manufacturing industry prioritises output and meeting deadlines over data administration. This section of the survey focuses on threats and potential enhancements, recognising that data storage and portable memory devices, such as Universal Serial Bus (USB) flash drives, pose cybersecurity risks.

4.5. Management of user accounts and cybersecurity

These questions were designed to assess respondents' knowledge, procedures, and experiences in managing user accounts and privileges in manufacturing systems.

These questions were specifically directed at candidates who answered, 'yes' to the scoping question 'Are you responsible for the configuration or maintenance of manufacturing system user accounts and

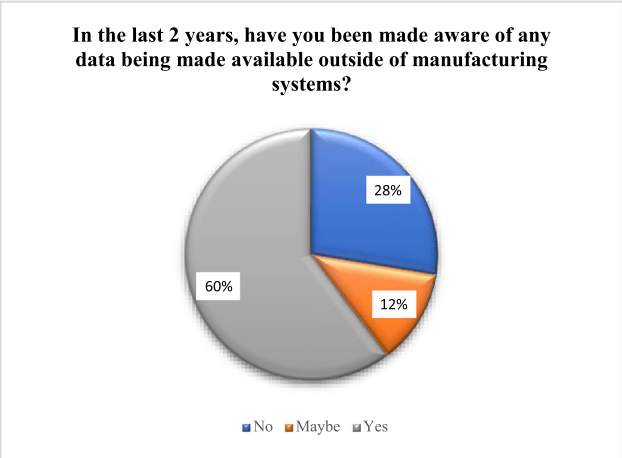

Fig. 9. Data behaviour results.

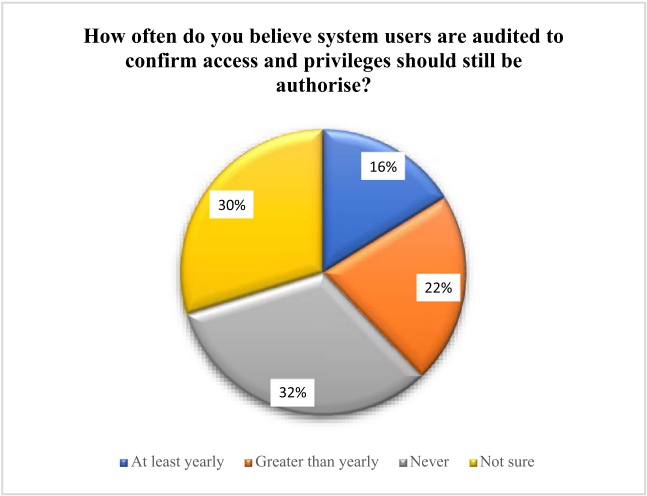

Fig. 10. Management of user accounts.

privileges?' to ensure accurate results. A total of 37 candidates, representing 43 % of the surveyed individuals, confirmed this responsibility.

Regarding the creation of user accounts and the granting of access privileges, the results were overwhelmingly positive. Only 10 % of participants expressed a need for strict protocols to follow when creating user accounts, and fewer than 10 % expressed a lack of confidence in the individual checks required before granting access or privileges.

However, regarding the frequency of audits and assessments of user accounts, the responses were troubling. One-third of the participants reported never undergoing these procedures, and only 32 % stated that the process was conducted on an annual basis. This approach presents a significant risk to manufacturing systems, as active accounts with user privileges can continue to be accessible even after personnel changes, potentially jeopardising product quality. Furthermore, the probability of undetected malicious accounts rises, posing greater threats to data storage and machine operations (see Fig. 10).

When reviewing the responses concerning employee experiences in the past two years, more than half of the participants answered 'yes' or 'maybe' when asked whether they were aware of colleagues who had obtained unauthorised system access, shared accounts, or bypassed access controls (see Fig. 11). Although unsatisfactory, these results were not surprising and emphasised a situation where the benefits of interconnected systems are sought after, but proper maintenance and oversight regarding access are deficient.

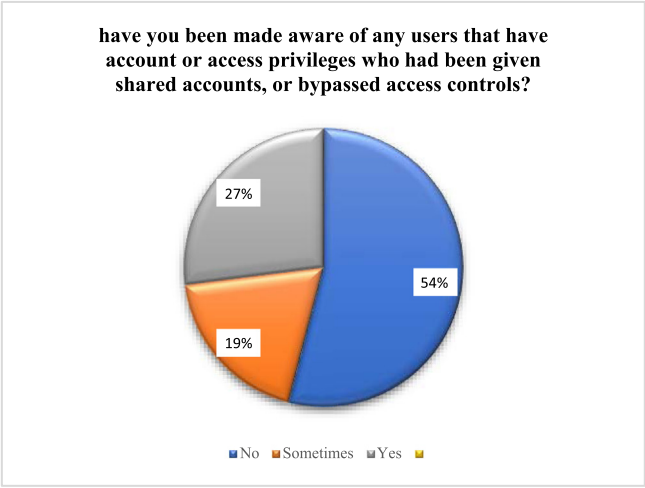

Fig. 11. User account experience results.

4.6. Cybersecurity opportunities and improvements

These questions were designed to gather information about candidates' ideas for improving cybersecurity in manufacturing systems. All candidates were asked these questions.

Two questions allowed participants to provide open-ended responses, which were then identified and evaluated to create a summarised set of results. Participants consistently highlighted three main risk factors: data storage and sharing, awareness and education, and third-party vendor access. System users ranked fourth in terms of the risk they pose.

When asked about how to improve cybersecurity, the most frequently mentioned suggestions revolved around simplifying system management and protocols to make them more practical for everyday use in the workplace (see Fig. 12). Many responses expressed dissatisfaction with complex and confusing IT and Information Assurance methodologies, which often led users to take shortcuts to bypass IT security and meet production goals. The next significant set of responses focused on enhancing employee education and raising awareness of relevant systems and procedures (see Fig. 13). These perspectives align with current literature and best practice models. Finally, participants were asked about their willingness to become cybersecurity champions and support colleagues and departments in gaining a better understanding of current issues. More than half of the respondents expressed potential interest in this role, indicating a possible area for development. Fig. 14 illustrates the results regarding cybersecurity champions.

4.7. Key findings

The results obtained from this survey can be considered reliable and a suitable assessment of the current situation due to high levels of participation. The survey assessed opinions and attitudes within an organisation, with responses categorised by role. It was found that Staff members made up the majority of respondents at 61.18 %, followed by Leaders at 28.24 %, and Senior Leaders at 10.59 %. This distribution highlights the varying levels of engagement across different organisational roles, offering a comprehensive view of the diverse perspectives and attitudes within the organisation, divided by role hierarchy. Throughout this paper, capability acquisition refers to the process by which an organization obtains the necessary skills, knowledge, technologies, and resources to perform tasks and achieve strategic objectives. Its implications include increased competitiveness, improved efficiency and productivity, enhanced innovation, strategic flexibility, risk mitigation, and employee development. The survey did experience some bias as a result of higher participation rates from employees in the Digital Manufacturing and

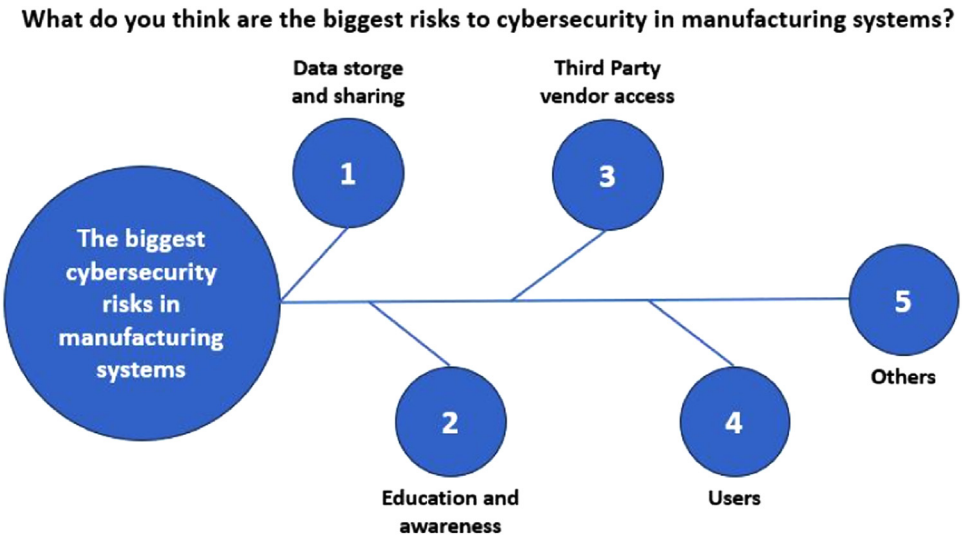

Fig. 12. Cybersecurity risks in manufacturing results.

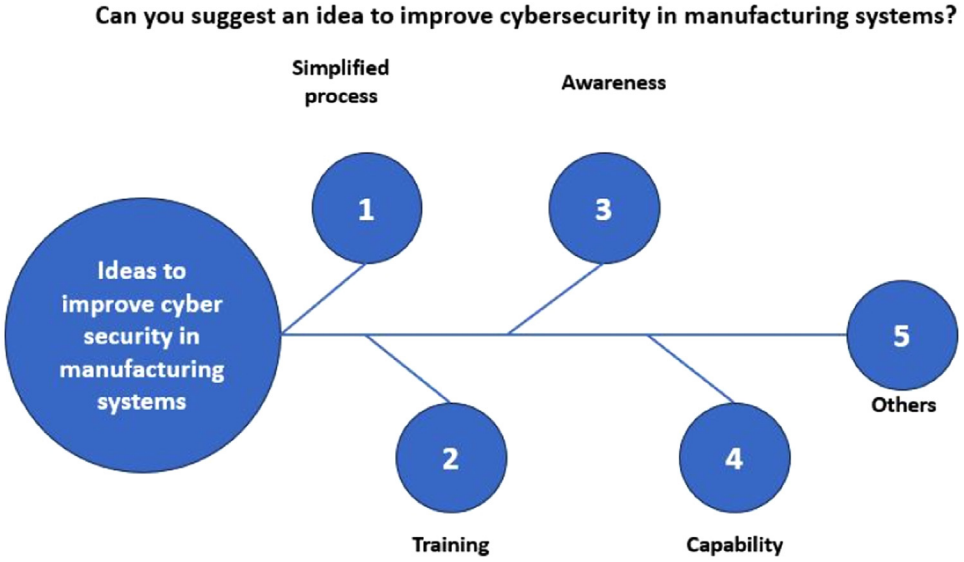

Fig. 13. Suggestions for improvement results.

Fig. 14. Cybersecurity champion results.

Manufacturing Engineering departments, compared to the number of participants from Operations, Capability Acquisition, and Manufacturing Services. This bias is in line with the findings of [70], which observed that individuals with pre-existing experience, interest, and knowledge are more likely to engage and contribute to further discussion. Supporting this idea, the data shows that questions about individual knowledge and accountability received positive responses, while responses related to poor practices by third parties were more negative. This pattern also emerged when considering risks and improvements: the free-text answers mainly focused on enhancing employee education levels, familiarity with appropriate procedures, and subsequent associated behaviours.

The most significant conclusion drawn from this research asserts that addressing issues related to uninformed, unaware, and disinterested individuals will lead to the most substantial improvements. Moreover, many negative responses stemmed from participant interactions with colleagues in everyday operational roles with limited exposure to cybersecurity protocols, making them less involved and unaware of the risks. Reference [63] reinforces the idea that cybersecurity threat prevention is only as effective as the weakest link in the chain, and employee education should prioritise raising awareness of current issues. This concern should be the primary focus for companies seeking to educate their staff: providing organised events or drop-in activities will only benefit those with existing knowledge and interest in the subject, while those with little to no interest are unlikely to derive significant benefits from this approach.

Table 3
Framework for improvement and key focus areas.

The improvement framework and focus area for cyber security in the manufacturing systems					
Activity	Function				
	Digital Manufacturing	Manufacturing engineering	Capability Acquisition	Manufacturing Services	Operations
Basic cyber security awareness campaign	G	M	M	M	H
Cyber security champions	M	M	M	M	M
Equipment remote vendor access	M	M	H	H	N
Equipment cyber security processes	M	M	H	M	N
User account management standards	H	M	N	N	M
Data management review	H	M	N	N	M

Key table	
G	Continue as-is
M	Increase Focus
H	High Focus Required
N	Not applicable

Responses regarding individual accountability, the implementation of cybersecurity training in the manufacturing environment, and an increased focus on cybersecurity were met with positive reactions.

The need for increased employee education and awareness exists parallel to four other focused areas.

4.7.1. Prioritisation and resource availability

Negative responses have arisen from insufficient maintenance and system management, which are regarded as low priority and frequently overlooked due to resource limitations.

4.7.2. Procedural simplification

Negative responses typically stem from complex, time-consuming, and restrictive protocols that impede operational priorities. As a result, employees often circumvent IT security measures, thereby heightening the potential risk to company systems and equipment.

4.7.3. Remote vendor access

Enabling secure remote access for third-party external vendors presents a challenge within the existing infrastructure. Vendors are often inclined to utilise wireless technologies such as 4 G to circumvent IT security protocols and gain access.

4.7.4. Data storage and sharing

Responses indicate that data storage and sharing are considered the main risks in manufacturing cybersecurity. Several responses mentioned the use of USB flash drives for storing data, even though there is a recent IT mandate prohibiting their use.

5. Research limitations

The data for this study was collected voluntarily from employees who work with manufacturing systems. While the results provide valuable insights, their accuracy and validity could be enhanced by including employees from all sectors of the manufacturing industry. Furthermore, the subjects selected for this research are all employed by a single manufacturer; expanding the scope to include other manufacturers could facilitate further analysis and the identification of similar trends, offering a broader overview of the current situation. To improve the generalisability of the findings, future research should aim to involve a more diverse range of participants from various sectors within the manufacturing industry. Additionally, collecting data from original equipment manufacturers (OEMs) would provide additional insights and may enable the identification of more cybersecurity vulnerabilities.

6. Framework for cybersecurity improvements in the manufacturing industry

Based on the critical findings, a framework (shown in Table 3) has been proposed to enhance cybersecurity in manufacturing systems, with suggested levels of emphasis allocated to each functional area. The first area involves implementing an awareness campaign aimed at disseminating the importance of cybersecurity throughout the company, explaining its relevance to each function and the systems it uses. The research revealed that individuals employed in digital manufacturing roles already have a good understanding of cybersecurity. Therefore, the focus should shift towards those working in operations who have not yet been exposed to the topic. It is recommended that these events prioritise engaging, interactive, and manageable tasks designed for an audience

Table 4
Concrete cybersecurity recommendations for various industries [74,75].

Industry	Company size	Concrete recommendations
Manufacturing	Small	Implement access controls and frequently update incident response plans. Utilize cybersecurity by design for new systems and products.
	Medium	Establish cybersecurity training programs for all employees. Involve in cross-industry information sharing to enhance threat intelligence.
	Large	Drive cybersecurity standardization efforts. Implement cybersecurity and privacy certification schemes to boost consumer and partner confidence.
Healthcare	Small	Ensure compliance with health data protection standards and guidelines. Use encryption for patient data and secure patient data exchange and storge.
	Medium	Develop comprehensive risk management strategies that include vulnerability assessments. Encourage partnerships with academia to translate research into practical cybersecurity enhancements.
	Large	Lead initiatives for global cybersecurity frameworks that address specific needs of the healthcare industry. Implement efficient disaster recovery protocols.
Finance	Small	Invest in strong multi-factor authentication and encryption methods to protect sensitive financial data.
	Medium	Adopt advanced cybersecurity technologies such as security monitoring and behavioural analytics for detecting suspicious activities. Increase investments in cybersecurity awareness and training.
	Large	Establish a dedicated cybersecurity task force to focus on emerging threats and compliance with global financial regulatory requirements. Promote a culture of continuous improvement in cybersecurity practices.
Retail	Small	Use secure and updated point-of-sale (POS) systems to protect against data breaches. Implement basic cybersecurity measures like antivirus, firewalls, and secure Wi-Fi networks.
	Medium	Develop a comprehensive data protection strategy that includes end-to-end encryption and data tokenization to protect customer information during transactions.
	Large	Lead development and adoption of industry-wide security standards. Invest in advanced threat detection and response capabilities. Organize regular security audits and penetration testing.
Education	Small	Secure sensitive student data through encryption and secure access controls. Provide basic cybersecurity training to all employees.
	Medium	Develop policies for the safe use of personal devices on campus networks. Invest in cybersecurity tools that provide visibility into network traffic to detect unauthorized access attempts.
	Large	Establish partnerships with cybersecurity firms to enhance security infrastructure and incident response capabilities. Offer advanced cybersecurity training and education programs to staff and students, focusing on the specific threats facing the education sector.

with limited technical background. These sessions should be kept brief to ensure that operational priorities do not hinder participation.

The second proposal involves the introduction of cybersecurity champions who will be placed within each organisation. These champions will act as the main point of contact for individuals in need of IT assistance. They will receive additional training in IT and cybersecurity to help support their colleagues. Importantly, they will serve as a crucial link between IT security teams and end-users. They will be equipped to offer solutions and address any inefficiencies or frustrations that could potentially cause individuals to bypass current security protocols.

The next two proposals aim to enhance equipment procedures and external vendor access. Feedback from the survey suggests that these areas led to dissatisfaction and exposed a lack of awareness and understanding of these challenges. Improving collaboration between Capability Acquisition, IT Security, and Manufacturing Services to tackle these concerns would be a positive move. By defining vendor requirements, the IT Security team can work together with Capability Acquisition and Manufacturing Services to establish a secure and mutually beneficial system that facilitates equipment installation and updates. In addition, technological upgrades in cybersecurity are important for protecting manufacturing systems against sophisticated cyber threats. Implementing advanced technologies such as AI, machine learning, and blockchain can enhance the detection, prevention, and response capabilities of an organization, ensuring robust security and operational integrity. The final activities recommended by this research involve reviewing the current user account management systems and assessing the existing data storage and management systems. These two activities aim to ensure that all user accounts are up-to-date and that data is securely stored and efficiently managed. Additionally, they enable management personnel to establish and maintain the necessary resources to regularly conduct these reviews.

7. Theoretical and managerial implications from a cybersecurity perspective

Current research project studies theoretical understanding alongside the practical applications of Industry 4.0 cybersecurity and it has more focus on the manufacturing aspect [71,72]. The results and findings of such a study depict several influences on academics, industry practitioners, and policymakers.

7.1. Theoretical implications

7.1.1. Cybersecurity vulnerabilities from technical to concepts

This study increases the theoretical framework surrounding cybersecurity by highlighting specific vulnerabilities within the manufacturing sector. It must incorporate the integration of IT and OT with the heightened risk profile, thereby providing a view of cybersecurity challenges specific to industrial settings. Furthermore, tailored cybersecurity policies and protocols for fighting vulnerabilities in the industrial domain would need more academic support to transfer manufacturing safety and security knowledge and experience to cybersecurity perspective [73]. For instance, the mitigation and the time and cost estimations resulting from assessing risk of ongoing vulnerability in Industry 4.0 would not be as accurate as expected if it were coming up from an individual opinion. It should be an approach based on an academic concept.

7.1.2. Employee awareness culture

The findings explain the importance of employee awareness as a critical factor in cybersecurity. This aligns with and expands upon existing theories that suggest organizational culture significantly impacts cybersecurity effectiveness. This research contributes to the theory by detailing how awareness and training modify risk perceptions and behaviour in a manufacturing context.

7.1.3. Framework for cybersecurity improvements

By proposing a comprehensive framework that includes awareness campaigns, cybersecurity champions, and enhanced procedural protocols, this study offers a theoretical model for improving cybersecurity postures within manufacturing environments. This framework can serve as a basis for further academic exploration and validation.

7.2. Managerial implications

7.2.1. Strategic resource allocation

For industry leaders, the emphasis on redirecting cybersecurity resources towards manufacturing highlights the need for strategic investment in cybersecurity infrastructure and training. This paper provides a clear rationale for prioritizing budget allocations, which is crucial for managerial decision-making.

7.2.2. Implementation of a cybersecurity framework

The proposed framework serves as a practical guide for manufacturing companies seeking to enhance their cybersecurity measures. Managers can adopt this framework to structure their cybersecurity efforts systematically, ensuring comprehensive coverage of both technological and human factors.

7.2.3. Cybersecurity as a continuous process

The study advocates for the continuous evaluation and adaptation of cybersecurity practices. This has direct managerial implications as it calls for ongoing training programs, regular audits, and updates to security protocols to keep pace with evolving cyber threats and technological advancements. Role of Cybersecurity Education: This research highlights the critical role of targeted education and training programs in reducing cybersecurity risks. Managers are encouraged to implement regular, engaging, and practical cybersecurity education that reaches all employee levels, thereby fostering a proactive security culture.

By incorporating these sections, the paper meets the academic rigor expected in scholarly publications and provides tangible, actionable recommendations that can be implemented in practical settings. These implications strengthen the bridge between theoretical research and real-world application, making the findings relevant to a broader audience including those directly involved in the operational and strategic oversight of manufacturing entities.

Based on the study results and sources, Table 4 has been constructed that delineates concrete recommendations for managers across various industries and organizational sizes. Table 4 specifies actions that managers can undertake to bolster cybersecurity measures within their respective sectors.

8. Conclusion and future work

This survey analysed participants' comprehension, knowledge, and encounters with cybersecurity in manufacturing systems. In particular, the results were considered reliable and offered a suitable evaluation of the present situation due to the significant level of participation.

As a result, the findings revealed that individuals had positive knowledge and accountability for cybersecurity, while responses regarding poor practices by third parties were pessimistic. It was concluded that addressing issues related to uninformed, unaware, and disinterested individuals would lead to the greatest improvements. Employee education and cybersecurity awareness were identified as crucial factors, suggesting that companies should prioritise raising awareness among all employees, rather than solely focusing on those with existing knowledge or interest in the subject.

Although, the data collection was voluntary and limited to employees of a single manufacturer working with manufacturing systems. To enhance the accuracy and validity of the results, it would be beneficial to include employees from various sectors of the manufacturing industry and different manufacturers. Furthermore, collecting data from OEMs could provide valuable insights into cybersecurity vulnerabilities.

Moreover, a proposed framework for enhancing cybersecurity in the manufacturing industry includes implementing an awareness campaign featuring interactive events for operational employees and introducing cybersecurity champions as points of contact. Key recommendations emphasize improving equipment procedures, addressing external vendor access issues, and reviewing user account management and data storage systems. Additionally, maintaining comprehensive, ongoing training programs and implementing a multi-level access control system are advised to minimize internal threats. The research underscores the importance of employee education, operational priorities, and IT security collaboration.

Future studies should encompass diverse participants across the manufacturing sector to gain a broader understanding of cybersecurity challenges and strategies. The recommendations outlined in the improvement framework provide a roadmap for organisations to enhance their cybersecurity measures and effectively mitigate risks. By prioritising these areas and regularly reviewing user account management and data storage systems, companies can strengthen their cybersecurity posture and safeguard their manufacturing systems and data.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

CRediT authorship contribution statement

Adel Alqudhaibi: Writing – review & editing, Writing – original draft, Visualization, Validation, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Majed Albarrak:** Writing – review & editing, Writing – original draft, Visualization, Validation, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Sandeep Jagtap:** Writing – review & editing, Writing – original draft, Supervision, Software, Resources, Project administration, Funding acquisition. **Nikki Williams:** Writing – review & editing, Writing – original draft, Supervision, Formal analysis, Data curation, Conceptualization. **Konstantinos Salonitis:** Writing – review & editing, Writing – original draft, Resources, Project administration, Funding acquisition.

References

[1] P.G.S. Contieri, R. Anholon, L.A. De Santa-Eulalia, Industry 4.0 enabling technologies in manufacturing: implementation priorities and difficulties in an emerging country, Technol. Anal. Strateg. Manag. 34 (5) (2022) 489–503, doi:10.1080/09537325.2021.1908536.

[2] V. Morfino, S. Rampone, Towards near-real-time intrusion detection for IoT devices using supervised learning and apache spark, Electronics (Switzerland) 9 (3) (2020), doi:10.3390/electronics9030444.

[3] I. Agrafiotis, J.R.C. Nurse, M. Goldsmith, S. Creese, D. Upton, A taxonomy of cyber-harms: defining the impacts of cyber-attacks and understanding how they propagate, J. Cybersecur. 4 (1) (2018) Oxford University Press, doi:10.1093/cybsec/tyy006.

[4] A. Bazzi, M. Chafii, Secure full duplex integrated sensing and communications, IEEE Trans. Inf. Forensics Secur. 19 (2024) 2082–2097, doi:10.1109/TIFS.2023.3346696.

[5] G. Tsochev, R. Trifonov, O. Nakov, S. Manolov, G. Pavlova, Cyber security: threats and challenges, in: 2020 International Conference Automatics and Informatics (ICAI), Varna, Bulgaria, 2020, pp. 1–6, doi:10.1109/ICAI50593.2020.9311369.

[6] Yozawa, K. (2019). 2021 Global Threat Intelligence Report Together we do great things INSIGHTS DRIVEN BY DATA 2 | 2021 Global Threat Intelligence Report Contents Access date July 8, 2024 (672544-2021-Global-Threat-Intelligence-Report-full-report.pdf (nttdata.com)).

[7] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1," Gaithersburg, MD, 2018. doi: 10.6028/NIST.CSWP.04162018.

[8] IBM, "IBM Security X-Force Threat Intelligence Index 2023," 2023. Accessed: Jan. 16, 2024. Available: https://www.ibm.com/downloads/cas/DB4GL8YM

[9] J. Srinivas, A.K. Das, N. Kumar, Government regulations in cyber security: framework, standards and recommendations, Future Gener. Comput. Syst. 92 (2019) 178–188 ISSN 0167-739X, doi:10.1016/j.future.2018.09.063.

[10] A. Staves, T. Anderson, H. Balderstone, B. Green, A. Gouglidis, D. Hutchison, A cyber incident response and recovery framework to support operators of industrial control systems, Int. J. Crit. Infrastruct. Prot. 37 (2022) 100505, doi:10.1016/j.ijcip.2021.100505.

[11] National Cyber Security Centre, "Cyber Security Toolkit for Boards - NCSC.GOV.UK," Crown. Accessed: Nov. 25, 2023. Available: https://www.ncsc.gov.uk/collection/board-toolkit.

[12] M. Barrett, "Framework for Improving Critic al Infrastructure Cybersecurity, Version 1.1," Gaithersburg, MD, 2018. doi: 10.6028/NIST.CSWP.04162018.

[13] M. Hill and D. Swinhoe, "The 15 biggest data breaches of the 21st century | CSO Online." Accessed: Nov. 25, 2023. Available: https://www.csoonline.com/article/534628/the-biggest-data-breaches-of-the-21st-century.html.

[14] J. Sullivan and J.R.C. Nurse, "Cyber Security Incentives and the Role of Cyber Insurance," 2021. Accessed: Oct. 16, 2023. Available: https://kar.kent.ac.uk/89042/1/RUSI-Kent-EIP-Cyber-insurance.pdf.

[15] G. Falco, R. Thummala, A. Kubadia, Wannafly: an approach to satellite ransomware, in: 2023 IEEE 9th International Conference on Space Mission Challenges for Information Technology (SMC-IT), IEEE, 2023, pp. 84–93, doi:10.1109/SMC-IT56444.2023.00018.

[16] Q. Li, M. Brundage, B. Kulvatunyou, D. Brandl, S. Do Noh, Advances in production management systems. the path to intelligent, collaborative and sustainable manufacturing, IFIP Advances in Information and Communication Technology, 513, Springer International Publishing, Cham, 2017, doi:10.1007/978-3-319-66923-6.

[17] I. Agrafiotis, J.R.C. Nurse, M. Goldsmith, S. Creese, D. Upton, A taxonomy of cyber-harms: defining the impacts of cyber-attacks and understanding how they propagate, J. Cybersecur. 4 (1) (2018), doi:10.1093/cybsec/tyy006.

[18] S. Kamiya, J.K. Kang, J. Kim, A. Milidonis, R.M. Stulz, Risk management, firm reputation, and the impact of successful cyberattacks on target firms, J. Financ. Econ. 139 (3) (2021) 719–749, doi:10.1016/j.jfineco.2019.05.019.

[19] Pankaj Pandey, Sokratis Katsikas, The future of cyber risk management: AI and DLT for automated cyber risk modelling, decision making, and risk transfer, in: Handbook of Research on Artificial Intelligence, Innovation and Entrepreneurship, Edward Elgar Publishing, 2023, pp. 272–290.

[20] HISCOX, "Don't let cyber be a game of chance. Hiscox Cyber Readiness Report 2021," 2021. Accessed: Nov. 25, 2023. Available: https://www.hiscox.co.uk/sites/default/files/documents/2021-04/21486-Hiscox-Cyber-Readiness-Report-2021-UK.pdf

[21] A. Minnar, Cybercrime, cyber attacks, and problems of implementing organizational cybersecurity, in: Global Issues in Contemporary Policing, Routledge, 2017, pp. 147–164. eBook ISBN 9781315436975.

[22] D. Galinec, D. Možnik, B. Guberina, Cybersecurity and cyber defence: national level strategic approach, Automatika 58 (3) (2017) 273–286, doi:10.1080/00051144.2017.1407022.

[23] ENISA. Consultation Paper - EU ICT Industrial Policy: Breaking the Cycyle of Failure. 2019. Accessed: 24 April 2024. Available at: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/eu-ict-industry-consultation-paper.

[24] R. Sabillon, J. Serra-Ruiz, V. Cavaller, J. Cano, A comprehensive cybersecurity audit model to improve cybersecurity assurance: the cybersecurity audit model (CSAM), in: 2017 International Conference on Information Systems and Computer Science (INCISCOS), IEEE, 2017, pp. 253–259, doi:10.1109/INCISCOS.2017.20.

[25] M. Soori, B. Arezoo, R. Dastres, Virtual manufacturing in industry 4.0: a review, Data Sci. Manag. (2023), doi:10.1016/j.dsm.2023.10.006.

[26] Enisa, "Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity About ENISA Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity," 2018, doi:10.2824/324042.

[27] V. Gkioulos, N. Chowdhury, Cyber security training for critical infrastructure protection: a literature review, Computer Science Review, 40, Elsevier Ireland Ltd, 2021, doi:10.1016/j.cosrev.2021.100361.

[28] M. Felser, M. Rentschler, O. Kleineberg, Coexistence standardization of operation technology and information technology, Proc. IEEE 107 (6) (2019) 962–976, doi:10.1109/JPROC.2019.2901314.

[29] L. Laperrière, G. Reinhart, CIRP Encyclopedia of Production Engineering, Springer Berlin, 2014, doi:10.1007/978-3-642-20617-7.

[30] W.J. Orlikowski, S.R. Barley, Technology and institutions: what can research on information technology and research on organizations learn from each other? MIS Q. (2001) 145–165, doi:10.2307/3250927.

[31] Gartner, "Definition of Operational Technology (OT) - Gartner Information Technology Glossary." Accessed: May 15, 2021. Available: https://www.gartner.com/en/information-technology/glossary/operational-technology-ot.

[32] A.H. Maulana, I.G.P. Ari Suyasa, E. Kurniawan, Analysis of the demilitarized zone implementation in Java Madura Bali electrical systems to increase the level of IT/OT cyber security with the dual DMZ firewall architecture method, in: 2023 International Conference on Smart Applications, Communications and Networking (SmartNets), Istanbul, Turkiye, 2023, pp. 1–6, doi:10.1109/SmartNets58706.2023.10215960.

[33] C.A. Giffi, B. Dollar, B. Gangula, and M.D. Rodriguez, "Exponential manufacturing A collection of perspectives exploring the frontiers of manufacturing and technology," 2017. Accessed: Nov. 26, 2023. Available: https://www2.deloitte.com/content/dam/insights/us/collections/exponential-manufacturing/DUP_Exponential-Manufacturing.pdf.

[34] O. Givehchi, K. Landsdorf, P. Simoens, A.W. Colombo, Interoperability for industrial cyber-physical systems: an approach for legacy systems, IEEE Trans. Ind. Inform. 13 (6) (2017) 3370–3378.

[35] O. Alexander, M. Belisle, and J. Steele, "MITRE ATT&CK® for Industrial Control Systems: design and Philosophy," 2020. Accessed: Nov. 26, 2023. Available: https://attack.mitre.org/docs/ATTACK_for_ICS_Philosophy_March_2020.pdf.

[36] M. Guri, M. Monitz, Y. Elovici, Bridging the air gap between isolated networks and mobile phones in a practical cyber-attack, ACM Trans. Intell. Syst. Technol. (TIST) 8 (4) (2017) 1–25, doi:10.1145/2870641.

[37] National Security Agency and Cybersecurity and Infrastructure Security Agency, "NSA and CISA Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems," 2020. Accessed: Nov. 26, 2023. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-205a.

[38] D. Thangam, T. Arumugam, K. Velusamy, M. Subramanian, S.K. Ganesan, M. Suryakumar, COVID-19 pandemic and its brunt on digital transformation and cybersecurity, in: Cybersecurity Crisis Management and Lessons Learned From the COVID-19 Pandemic, IGI Global, 2022, pp. 15–42, doi:10.4018/978-1-7998-9164-2.ch002.

[39] B. Williams, M. Soulet, A. Siraj, A taxonomy of cyber attacks in smart manufacturing systems, in: 6th EAI International Conference on Management of Manufacturing Systems, Springer International Publishing, Cham, 2022, pp. 77–97, doi:10.1007/978-3-030-96314-9_6.

[40] M. Ryan, M. Ryan, Ransomware case studies, in: Ransomware Revolution: The Rise of a Prodigious Cyber Threat, 2021, pp. 65–91, doi:10.1007/978-3-030-66583-8_5.

[41] D. Kurt, "The 10 Most Expensive Cyberattacks of All Time." Accessed: May 31, 2021. Available: https://www.investopedia.com/financial-edge/0512/10-of-the-most-costly-computer-viruses-of-all-time.aspx.

[42] U.P.D. Ani, H. He, A. Tiwari, Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective, J. Cyber Secur. Technol. 1 (1) (2017) 32–74, doi:10.1080/23742917.2016.1252211.

[43] V. Mullet, P. Sondi, E. Ramat, A review of cybersecurity guidelines for manufacturing factories in industry 4.0, IEEE Access. 9 (2021) 23235–23263, doi:10.1109/ACCESS.2021.3056650.

[44] A.W. Batteau, Creating a culture of enterprise cybersecurity, Int. J. Bus. Anthropol. 2 (2) (2011) Accessed: Nov. 26, 2023. Available: https://www.academia.edu/download/81761133/1118.pdf .

[45] Ö. Aslan, S.S. Aktuğ, M. Ozkan-Okay, A.A. Yilmaz, E. Akin, A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions, Electronics 12 (6) (2023) 1333, doi:10.3390/electronics12061333.

[46] University of Phoenix and (ISC)2, " Cybersecurity Workforce Competencies: preparing Tomorrow's Risk-Ready Professionals," 2014.

[47] R.M. Lee, M.J. Assante, and T. Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case," Bethesda, MD, USA, 2016.

[48] S.A. Talesh, Data breach, privacy, and cyber insurance: how insurance companies act as "compliance managers" for businesses, Law Soc. Inq. 43 (2) (2018) 417–440, doi:10.1111/lsi.12303.

[49] S. Dojkovski, S. Lichtenstein, M. Warren, Developing information security culture in small and medium size enterprises: australian case studies, in: 6th European Conference on Information Warfare and Security 2007, ECIW 2007, 2007, pp. 55–65.

[50] ENISA, Cybersecurity Culture Guidlines: Behavioural Aspects of Cybersecurity, no. 2018. doi: 10.2824/324042.

[51] M. Bada, J.R.C. Nurse, Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs, Inf. Comput. Secur. 27 (3) (2019) 393–410, doi:10.1108/ICS-07-2018-0080.

[52] Fagbule, O., 2023. Cyber Security Training in Small to Medium-sized Enterprises (SMEs): Exploring Organisation Culture and Employee Training Needs (Doctoral dissertation, Bournemouth University) Access date 9 July 2024 (https://eprints.bournemouth.ac.uk/39148/).

[53] A. Alqudhaibi, A. Aloseel, S. Jagtap, and K. Salonitis, "Identifying and Predicting Cybersecurity Threats in Industry 4.0 Based on the Motivations Towards a Critical Infrastructure," 2022. doi: 10.3233/ATDE220599.

[54] A. Alqudhaibi, M. Albarrak, A. Aloseel, S. Jagtap, K. Salonitis, Predicting cybersecurity threats in critical infrastructure for industry 4.0: a proactive approach based on attacker motivations, Sensors 23 (9) (May 2023) 4539, doi:10.3390/s23094539.

[55] D. Dickinson, "Building A Business Case for Operational Technology Cybersecurity," 2016. Accessed: Nov. 26, 2023. Available: https://www.isa.org/intech-home/2016/november-december/features/building-a-business-case-operational-technology.

[56] NDIA Cybersecurity for Advanced Manufacturing, "Cybersecurity for Manufacturing Networks The NDIA Cybersecurity for Advanced Manufacturing Joint Working Group (CFAM JWG)," 2017. Accessed: Nov. 26, 2023. Available: https://www.ndia.org/-/media/sites/ndia/divisions/working-groups/cfam/ndia-cfam-2017-white-paper-20171023.ashx?la=en.

[57] C. Paulsen, Cybersecuring small businesses, Computer (Long. Beach. Calif) 49 (8) (2016) 92–97, doi:10.1109/MC.2016.223.

[58] Bagwell, M.A., 2016. Organizational decisions about cyber security in small to mid-sized businesses: a qualitative study (Doctoral dissertation, Northcentral University). Access date 9 July 2024 (https://www.proquest.com/openview/d5e2775e9da54cc9f1a43d89647b4379/1?cbl=18750&pq-origsite=gscholar&parentSessionId=EX%2BcTyW5Hm1WuUzbCb%2F%2FFWNWuh%2F%2FMbPgDVNa%2FuwlM0g%3D).

[59] NCSC, "Cyber Security Small Business Guide Small Business Guide Collection How to improve your cyber security; affordable, practical advice for businesses National Cyber Security Centre 2," 2020. Available: https://www.cyberessentials.ncsc.gov.uk/

[60] Cisco, "Small and Mighty How Small and Midmarket Businesses Can Fortify Their Defenses Against Today's Threats CYBERSECURITY SPECIAL REPORT," 2018. Accessed: Nov. 26, 2023. Available: https://www.cisco.com/c/dam/global/en_hk/products/security/security-reports/Cisco_2018_SMB_Final.pdf.

[61] E. Ogbonna, L.C. Harris, Leadership style, organizational culture and performance: empirical evidence from UK companies, Int. J. Hum. Resour. Manag. 11 (4) (2000) 766–788, doi:10.1080/09585190050075114.

[62] Q. Li, M. Brundage, B. Serm Kulvatunyou, D. Brandl, S. Do Noh, Improvement strategies for manufacturers using the MESA MOM capability maturity model, in: IFIP Advances in Information and Communication Technology, 2017, pp. 21–29, doi:10.1007/978-3-319-66923-6_3.

[63] K. Jung, B. Kulvatunyou, S. Choi, and M.P. Brundage, "An Overview of a Smart Manufacturing System Readiness Assessment," 2011. doi: https://doi.org/10.1007/978-3-319-51133-7_83.

[64] T. Huelsman, E. Powers, S. Peasley, and R. Robinson, "Cyber risk in advanced manufacturing," 2016. Accessed: Nov. 26, 2023. Available: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/manufacturing/us-manu-cyber-risk-in-advanced-manufacturing.pdf.

[65] F. Kitsios, E. Chatzidimitriou, M. Kamariotou, Developing a risk analysis strategy framework for impact assessment in information security management systems: a case study in it consulting industry, Sustainability 14 (3) (2022) 1269, doi:10.3390/su14031269.

[66] U.P.D. Ani, H.(Mary) He, A. Tiwari, Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective, J. Cyber Secur. Technol. 1 (1) (2017) 32–74, doi:10.1080/23742917.2016.1252211.

[67] K. Sehgal, N. Thymianis, Cybersecurity Blue Team Strategies: Uncover the Secrets of Blue Teams to Combat Cyber Threats in Your Organization, Packt Publishing Ltd., 2023 ISBN 978-180107-247-2.

[68] A. Williams, How to … Write and analyse a questionnaire, J. Orthod. 30 (3) (2003) 245–252, doi:10.1093/ortho/30.3.245.

[69] E. McColl et al., "Design and use of questionnaires: a review of best practice applicable to surveys of health service staff and patients," 2001, Accessed: Nov. 26, 2023. Available: https://www.academia.edu/download/46168290/Design_and_Use_of_Questionnaires_A_Revie20160602-6738-1l9ett.pdf.

[70] J.A. Krosnick, Survey research, Annu. Rev. Psychol. 50 (1) (1999) 537–567 Accessed: Nov. 26, 2023. Available: https://www.annualreviews.org/doi/pdf/10.1146/annurev.psych.50.1.537 .

[71] N. Burgess, S. Becker, J.A. King, J. O'Keefe, Memory for events and their spatial context: models and experiments, Philos. Trans. R. Soc. B 356 (1413) (2001) 1493–1503, doi:10.1098/rstb.2001.0948.

[72] M. Bada, A.M. Sasse, and J.R.C. Nurse, "Cyber security awareness campaigns: why do they fail to change behaviour?," 2019. doi: https://doi.org/10.48550/arXiv.1901.02672.

[73] A. Bazzi, M. Chafii, On integrated sensing and communication waveforms with tunable PAPR, IEEE Trans. Wirel. Commun. 22 (11) (2023) 7345–7360, doi:10.1109/TWC.2023.3250263.

[74] S. Naoumi, A. Bazzi, R. Bomfin, M. Chafii, Complex neural network based joint AoA and AoD estimation for bistatic ISAC, IEEE J. Sel. Top. Signal Process. (2024) 1–15.

[75] S. Jagtap, H. Trollman, F. Trollman, G. Garcia-Garcia, W. Martindale, Surviving the storm: navigating the quadruple whammy impact on Europe's food supply chain, Int. J. Food Sci. Technol. (2024), doi:10.1111/ijfs.17106.