Discover Food

Discover

Case Study

Cybersecurity 4.0: safeguarding trust and production in the digital food industry era

Adel Alqudhaibi[1] · Ashish Krishna[1] · Sandeep Jagtap[1,2] · Nikki Williams[3] · Mohamed Afy-Shararah[1] · Konstantinos Salonitis[1]

Received: 5 September 2023 / Accepted: 28 December 2023
Published online: 04 January 2024

Abstract
The food industry is vital manufacturing sector globally, with an ever-increasing reliance on digitalisation and technology-driven processes. However, this advancement introduces inherent cyberattack risks, encompassing data breaches and system disruptions, which can severely impact production and disrupt the entire food chain. Consequently, cyber threats can evoke fear and mistrust among consumers, potentially tarnishing a company's brand. This paper presents a comprehensive research methodology, including an extensive literature review and a detailed survey, aimed at assessing the current state of cybersecurity within the food industry. The problem at hand is the industry's apparent lack of robust cybersecurity measures to protect against the growing threat landscape, which this research aims to address. Our findings reveal a clear gap in cybersecurity preparedness within the food industry, with potential vulnerabilities that could be exploited by cyber adversaries. In response, we propose a specialised security framework designed to mitigate these risks. The framework is built upon a thorough analysis of the industry's existing cybersecurity posture and the identification of both current and emerging cyber threats. The contribution of this research relies in the development of a security framework that strengthens the industry's cyber defenses, thereby enhancing its competitive advantage. The framework emphasizes the importance of continuous employee education and training as a cornerstone for improving the security environment. Enhancing the security environment through ongoing employee education and training is crucial for fostering consumer trust and enabling seamless growth within the industry. By adopting a proactive approach to cybersecurity, the food industry can ensure the sustainability and reliability of its operations in the face of evolving cyber threats.

Keywords Cybersecurity · Cyberattacks · Food sector · Supply chain · Digitalization · Employee training

1 Introduction

Every industry is seeing an increase in cyberattacks, and the food industry, a vital component of the global economy, is not immune. Securing food industry is crucial to consider this because the 2021 survey on Cybersecurity Breaches revealed significant insights into the need for a global focus on cybersecurity in the food sector [1]. For instance, the construction industry and the UK food and beverage industries perceive cybersecurity as less worried about the

✉ Adel Alqudhaibi, adel.alqudhaibi@cranfield.ac.uk | [1]Sustainable Manufacturing Systems Centre, School of Aerospace Transport and Manufacturing, Cranfield University, Cranfield MK43 0AL, UK. [2]Division of Engineering Logistics, Department of Mechanical Engineering Sciences, Faculty of Engineering, Lund University, Ole Römers Väg 1, M-Building, 22363 Lund, Sweden. [3]Cranfield Defense and Security, Cranfield University, Cranfield MK43 0AL, UK.

implications of cybersecurity, with 62% and 64% considering it highly important, compared to 77% of trades overall. These outcomes remained consistent between 2020 and 2021 [1].

The food industry is one of the largest and fastest-growing industries worldwide, especially as the global population continues to rise, potentially reaching 9.7 billion by 2050, according to the United Nations projections on population. This increase implies a greater demand for food products. The food industry encompasses primary production, distribution, farming, and cultivation [2].

In today's dynamic business landscape, rapid knowledge exchange and idea generation are essential for success, and technological advancements are facilitating this process. Driven by innovations in information and communication technology (ICT), rapid global digitization has revolutionized various market sectors, and the food industry is no exception. This transformation has opened many opportunities for businesses in this field [3].

Industry 4.0 principles, including task automation, quality control, and intelligent manufacturing, are being implemented in the food industry [4]. As a result of utilizing information technology, food companies have noticeably benefited from globalization and enhanced supply chain management [5]. However, this also exposes them to cyber risks and crimes, highlighting the crucial importance of cybersecurity.

Food manufacturers often perceive their data as relatively insignificant and believe it has a low probability of being targeted by cybercriminals. Nevertheless, the potential threats of plant safety compromise, intellectual property theft, financial harm, and reputational damage should not be ignored or disregarded [6].

The UK food industry's emphasis and investment in integrating new technologies to enhance efficiency, optimize distribution, and establish stringent quality standards throughout the production process are poised to elevate customer experience and satisfaction. Existing food suppliers are forming increasingly interconnected networks. Effective inventory management will be streamlined across supply chain stages, necessitating information exchange both within and beyond the organization, and fostering communication processes and the utilization of digital tools. These efforts reveal vulnerabilities to cyber threats, prompting a thorough assessment when establishing a robust cybersecurity framework.

Understanding the root causes of cyberattacks is essential. According to Khurshid et al., such attacks arise for several reasons, including inadequate existing cybersecurity systems, untrained personnel who are not familiar with cyber threats, a negative security infrastructure, and an industry-wide misconception that information-related risks are limited to core enterprise functions [7]. The potential impact extends to crippling an organization's entire business processes and causing widespread disruption across the supply chain [8]. These challenges pose significant threats to the food market. Consequently, they underscore the imperative of implementing robust cybersecurity measures and formulating comprehensive policies to safeguard the industry from cyberattacks. As a result, the food industry and its organizations are potentially vulnerable to cyberattacks that could disrupt entire production operations and interfere with overall supply chain management [9]. This situation necessitates further research into the cyber risks facing the global food industry, the implementation of cybersecurity measures, and the development of a more robust framework to safeguard the sector from cyberattacks [10].

This work aims to assess the critical importance of cybersecurity for the food industry, identify and highlight potential risks stemming from inadequate cybersecurity protections, and develop a security framework to defend against cyberattacks. To achieve this goal, the study will gain a deeper understanding of the current cybersecurity situation in the food industry and its readiness to handle cyber threats, identify the present and future cybersecurity risks it faces, and create a framework to enhance the food industry's cybersecurity, thereby improving its competitiveness. The methodology applied in this paper will include conducting a systematic literature review and survey. This research is structured as follows. The first part of the research provides an introduction and comprehensive review of the relevant literature. The second part presents the research methodology employed, including the systematic review of literature and the conduct of the survey. The third part shows the survey results and includes discussion. Finally, the proposed cybersecurity framework is established in part four and summarises the findings of the study and suggests directions for future research.

2 Literature review

2.1 Risk landscape of cyberattacks in the food industry

In this sub-section we capture the essence of various aspects of vulnerability, potential disruptions, and adverse impacts of cyberattacks in the context of the food industry. Cyberattacks can affect the food section in following ways:

a) Cyber incidents can cause interruptions in the production process that may jeopardise the company's profitability, reputation, goodwill, and brand. A cyberattack can potentially disrupt the manufacturing line within the food sector, jeopardising the company's profitability, reputation, goodwill and brand.
b) The corporate's integrity and profitability can be harmed and destroyed by interrupting the production line. The corporate's integrity and profitability hang in the balance when the production line is interrupted, making it susceptible to damage and devastation that cannot be repaired.
c) Food can be contaminated by changing the serial number, expiry date and other important information making it unsafe for sale, resulting in loss of the company brand reliability and business. Food products risk contamination if there are illicit alterations to vital details such as the serial number, expiry date and other important information making them unsafe for consumption and jeopardizing the company's brand reliability and business and business.
d) Hackers possess the power to inflict severe damage to companies' reputations by trespassing IPR (trade secrets and patents) in recipes and production processes.
e) Customer personal information can also fall prey to unscrupulous entities, leading to the violation of GDPR. It can lead to severe financial penalties.
f) With its destructive power, a cyber-attack can cripple the food distribution supply chain and storage, bringing the company's operation to a standstill.

2.2 Cybersecurity challenges in food sector

Through an extensive review of scholarly papers describing the different cyberattacks, Barreto and Amaral [11] and Tuptuk and Halies [12] papers emerge as pivotal sources which were found to give a comprehensive outlook on the security threats encountered by the food sector which has been summarised below:

a) Data ownership, confidentiality and safety with the increasing adoption of technologies such as the IoT for data collection have become increasingly popular and pervasive, users' data ownership, confidentiality, and safety are getting into question. All the Global Positioning Systems (GPSs) have the intelligence to locate locations that might be troublesome. The users are completely unaware that they are being followed.
b) Users' data ownership, confidentiality, and safety are misconstrued due to the increasing adoption and pervasiveness of technologies like the IoT for data collecting. As GPS systems and IoT-enabled devices track and collect data, this sensitive information's very ownership and privacy are questioned. Unbeknownst to users, these systems possess the intelligence to monitor and trace their every move, leading to potential risks and invasions of privacy [13].
c) The use of the Internet of Things is a technical breakthrough that harnesses the power of GPS technology to improve and increase agricultural production efficiency, and so, be it farming data or data utilised in food manufacturing plants, this transformative integration of IoT has ushered a new era of increased efficiency, as data becomes increasingly sensitive, preserving its confidentiality assumes unprecedented importance [7]. Farmers can incur severe financial and personal harm due to data breaches, highlighting the critical security challenges that the agricultural industry faces in the space of data privacy and ownership [14]. Privacy problems loom as the Internet of Things grows and is used, necessitating cybersecurity in the food industry must be addressed and handled seriously. One such threat, spoofing, is an example of an attack where a hacker steals personal data to impersonate another to gain unauthorised access.
d) Social Engineering is a cybercrime tactic aimed at manipulating people's minds to deceive them into making security mistakes or extracting sensitive information. As a result, cybersecurity encompasses more than just technological fortifications; corporate personnel must be made aware of cyber risk and educated to thwart the unauthorised

acquisition of sensitive information. This information can be categorised under digital literacy, which needs to be revised in the food industry. Phishing serves as a notable illustration of social engineering cyber threats.

e) Ransomware is a type of malware in which the hacker seizes control of your data, rendering it inaccessible to its rightful owners until a ransom is paid. The main motive of this kind of attack is to extort funds from the targeted company. There are two distinct attack types of ransomwares, encrypting and destructive. Encrypting ransomware holds vital assets and system files hostage presenting a message on how to pay an undetectable ransom to recover the files; conversely, destructive ransomware warns the user of its existence on the system by restricting administrator excess and demanding payment to avert data destruction [15]. Ex. WannaCry and Petya are two notable examples of destructing ransomware that affected the industry in 2017 [16]. Due to a Ransomware attack on JSB US beef, the facility was compelled to suspend operations as a direct result of a ransomware attack [17].

f) Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks force servers or networks to fail, leaving the system incapacitated to process incoming requests. This malicious cyber-attack jeopardies data availability, overwhelming servers with an excessive influx of instructions and rendering them inoperable [18]. The foundation of intelligent farming and industries is based on IoT connectivity and internet access. Since DoS cyberattacks are difficult to anticipate, necessitating a proactive approach focused on prevention rather than response, cybersecurity emerges as a crucial tool in avoiding and controlling the disruptive effects of DoS attacks. Distributed denial of services (DDoS) uses numerous compromised systems infected with malware to attack a target.

g) Man-in-the-middle attack: The attacker resides between communicating devices to intercept and manipulate their communications [19]. This insidious tactic can disrupt the key exchange protocol between a control system and an actuator device (many industrial control systems perform this in the open, without encryption).

h) Cyber-Espionage—As food manufacturers and producers increasingly rely on software and hardware, the spectre of Cyber-Espionage emerges as a formidable threat. As the food sector progressively embraces more innovative and robust automation technologies within its processing operations, it inadvertently exposes itself to heightened vulnerability against cyberattacks [20]. Through this, cybercriminals seize the opportunity to spy on business rivals for monetary gains, such as gaining access to trade secrets and intellectual property (IP), which encompasses patents, copyrights, trademarks, recipes, product formulations, theories, software, processing technique, design, or data that could impact value for commercial gain. Cyber Espionage is one of the easiest and low-cost methods to attack, and that is why Cyber Espionage threats make it an increasingly prevalent and concerning avenue of threat.

i) Supply Chain—In food industry, supply chain represents an indispensable foundation of food security, but it concurrently manifests as an increasingly susceptible dimension [21]. Within the intricate web of agri-food trade, numerous stakeholders, including farmers, processors, traders, wholesalers, retailers, and consumers, collaborate to ensure the seamless flow of goods. When cybersecurity transcends the boundaries of one organisation's control, it is necessary to identify and fortify the entire digital chain. These security vulnerabilities must be identified in supplier products subject to phishing attempts and the theft of privileged credentials, culminating in the potentially catastrophic disclosure of massive volumes of sensitive data.

2.3 Threat analysis framework relevant to food sector

A framework serves as a versatile guideline for organisations of various market capitalisations, sizes, and levels of expertise to deal with cyber threats and risks. It may be used by a company to evaluate its present cybersecurity programme or to start from scratch by defining cybersecurity goals that are appropriate for their business environment needs or can incorporate improvisation into the current system by recognising its flaws and gaps [22]. Researchers have developed various notable security frameworks in the field:

Brachoa et al.'s, Game Theory Framework in Cybersecurity- Game theory is a decision-making tool for analysing the behaviours of competing agents under a conflict condition. It assesses the conflicting and cooperative nature of rational agents who try to pursue their benefits [23].

Jason West emphasises three crucial components that must be considered while developing a food industry (agriculture) framework: abnormal measurement detection, access control, and encryption [15].

Gomez et al. introduced the 'Safeman' framework, a comprehensive set of applications and services designed to continuously monitor and evaluate the cybersecurity and safety risks associated with manufacturing industrial processes. By leveraging machine learning and deep learning algorithms, the framework utilises anomaly detection strategies based on edge computing to identify cyber threats (EC) [16].

Though, other industries recognised frameworks like STRIDES from Microsoft. It is a cyber-physical system (CPS) threat modelling technique that makes it easier for security analysts to discover vulnerabilities and develop suitable component-level security solutions at the system design stage. Microsoft proposes the STRIDE method and provides instructions to address six different types of security threats (i) Spoofing impersonates a genuine user, process or system element. (ii) Tampering: modifying valid information. (iii) Repudiation: Denying or disowning a system action, (iv) Information disclosure: Data breach or unauthorised access to confidential information, (v) DoS: Service disruption for legitimate users, and (vi) Elevation of privilege: A user with restricted authority gaining higher privilege access to a system element [24].

NIST, National Institute of Standards and Technology, provides a widely recognised roadmap for organisations to manage their internal and external cybersecurity risks. It consolidates the best practices and standards across the industry to fight cybercrime. Though initially, it was built to be used by the sector qualifying in critical infrastructure, it slowly extended to other industries too. It contains five functions: identify, protect, detect, respond and recover [22].

2.4 Examples of cyber-attack in other sectors relevant to the food industry

a) Cyberattack on the water sector: Water assumes a pivotal role within the food production business, from agricultural fields to processing units, as a vital resource indispensable at every stage. According to Kozik and Choras, the water sector employs Supervisory Control and Data Acquisition systems (SCADA), which are a cyber component and vulnerable to cyberattacks [25]. In 2006, a foreign hacker used the internet to break the security of a water purification facility in the United States by using malware capable of affecting water treatment procedures.
b) Cyber-attack in the power sector: A well-coordinated and orchestrated cyber-attack damaged three Ukraine regional power distribution firms in December 2015, disrupting electricity to 225,000 homes [26]. This incident marked a significant milestone, one of the earliest successful cyber-attacks on the power sector. Laing et al., in their journal, shed light on the intricacies of the attack, revealing that three malwares were distributed through spear-phishing e-mail. This nefarious strategy leverages information gathered from social media to craft convincing messages tailored for key personnel. In this incident, the hacker assumed control of the SCADA network, conducted a telephonic denial-of-service attack to prevent outage reports from reaching contact centres, and destroyed master boot records on workstations, delaying restoration attempts [27].
c) Cyber-attack in the supply chain sector: JBS S.A., the world's largest meat processing firm, has recently been subjected to several cyberattacks. The most famous event was a ransomware attack on May 30, 2021, which caused severe operational interruptions throughout JBS's facilities in the United States, Canada, and Australia, leading the company to concede to the hacker's demands and pay a $11 million ransom [37].

The above episode shows that no industry is immune to cyberattacks, and the food industry is no exception.

2.5 Key factors indicating the non-implementation of cybersecurity in the food industry due to following reasons

Use of old ICS (Industrial Control System) legacy system: The system needs to be updated and intricately interconnected with other systems that are difficult to remedy. This needs to be either updated or replaced in the system. They need to be more competent to tackle modern cyber threats.

a) Lack of knowledge and awareness among stakeholders and senior executives regarding cybersecurity and threats.
b) Small and mid-size companies outsource their IT services and rely on their vendor or remote access for technical support; this dependency increases their vulnerability and exposes potential weaknesses that can propagate up the supply chain, even affecting larger companies with their IT infrastructure. Unlike food safety, there are no best manufacturing practices for cybersecurity for mid and small companies (SMEs) to follow.
c) Information Technology department often lacks compelling evidence regarding the cyberattack to show a business case to senior management for investment.
d) Lack of information on how ICS and IT system communicates- many companies are not aware of or have a proper record of identifying the number of ICS connected to their network, where they are, who owns them, and the existence of this confusion can be attributed to a knowledge and cultural gap with inadequate coordination between plant floor operation staff and IT.

e) Stakeholders operating in isolation must be made aware of the availability of informative tools, which increases the risk of cyber-attack and limits cybersecurity.
f) Skill gap—The food industry lacks cyber-skilled individuals to understand and handle cyber threats and risks. The people responsible for ICS are mainly experts in food safety and production, not cybersecurity.

3 Research method

This research utilized a combination of a literature review and actual data collected and assessed via food company surveys. The methodology has been separated into two stages: stage 1 and stage 2. The first stage comprises a systematic literature study, whereas the second stage includes a survey of food firms to determine the level of awareness and the process used for cybersecurity. As illustrated in Fig. 1, the suggested method is primarily meant to collect more information from earlier papers and research on this topic through a systematic review of the literature.

3.1 Systematic literature review (SLR)

The systematic literature review is used to identify and evaluate the current status of cybersecurity in the food sector and to generate the necessary knowledge from the literature for data collection and analysis. SLR included four steps: establishing the scope of the study, creating the research questions, searching for current research papers, analysing, extracting information, and data gathering and synthesis.. The scope of the research provides greater clarity, resulting in straightforward research questions that can be addressed. The research questions are derived from the specified objective, aim, and previous studies.

3.1.1 Defining the research scope and formulating research questions

a) What is the current level of cybersecurity in the food industry, and how important is it?
b) What are the current cyber threats to the food sector?
c) What are the existing cybersecurity frameworks protecting against cyberattacks?

The questions above underline and emphasise the significance of cybersecurity in the food industry. It is intended to provide a better understanding and justification for why cybersecurity should be adopted in the food business.

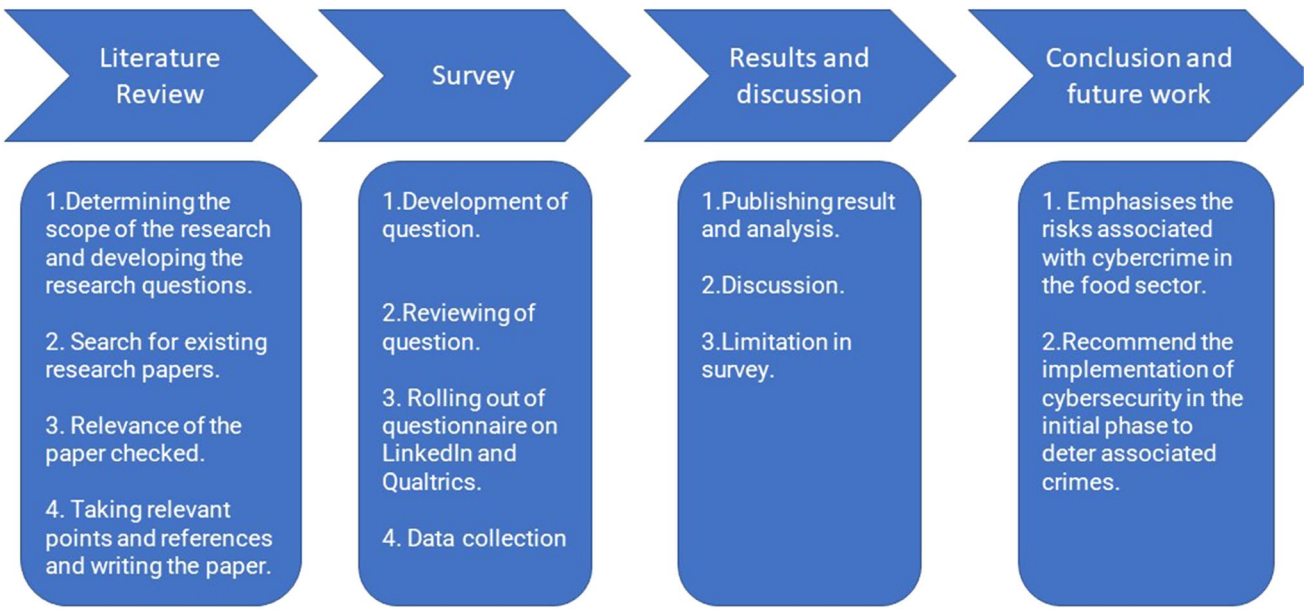


Fig. 1 Suggested method

It also attempts to understand the various cybersecurity frameworks used in the food business and to create a new framework to improve cybersecurity.

3.1.2 Search for existing research papers

Three electronic databases were used for the literature search: Google Scholar, Scopus, and ProQuest. These three digital libraries were chosen as relevant search engines with large databases that offer valuable tools for conducting advanced searches based on keywords, year of publication, and other criteria. Aside from a published conference paper, books, and journals, a few news academic papers were also considered. As shown in Fig. 2 multiple search strings were constructed using various combinations and permutations, and the closest search string combinations were finalised and selected.

Further, the inclusion of specific terminology significantly enhanced the search methodology. Throughout this paper, the terms "food" and "cyber" were introduced and synthesized with additional lexemes including "security," "threat," "attack," "interruption of service," "crime," "resilience," "breach," and "theft." These terms are reflective of some of the most prevalent lexicon employed in the discourse on cyber risk management. These terms are often found in discussions pertaining to cyber risk management.

3.1.3 Evaluating the relevance of the paper, and the extraction and collection of data

In this phase, the research papers have been reviewed and evaluated based on the research questions. The evaluation criteria for this study were papers published after 2005 until date, English published papers, papers related to the food industry and other cybersecurity, experience reports based on experts and empirical studies. The total publication papers were discovered was 20,513 publications, 16,400 on Google Scholar 3,487 on Scopus and 626 on ProQuest.

3.2 Food industry survey

An online survey was carried out, with the questionnaire hosted on Qualtrics, a widely used online survey tool. Additionally, emails containing the survey link were sent to a sample of 40 food companies, which represented a mix of market capitalizations, predominantly consisting of small companies, but also including a few medium and large-sized enterprises. The emails were addressed to a broad array of employees within these food companies, with a request to circulate the survey link to colleagues within the information technology department or those tasked

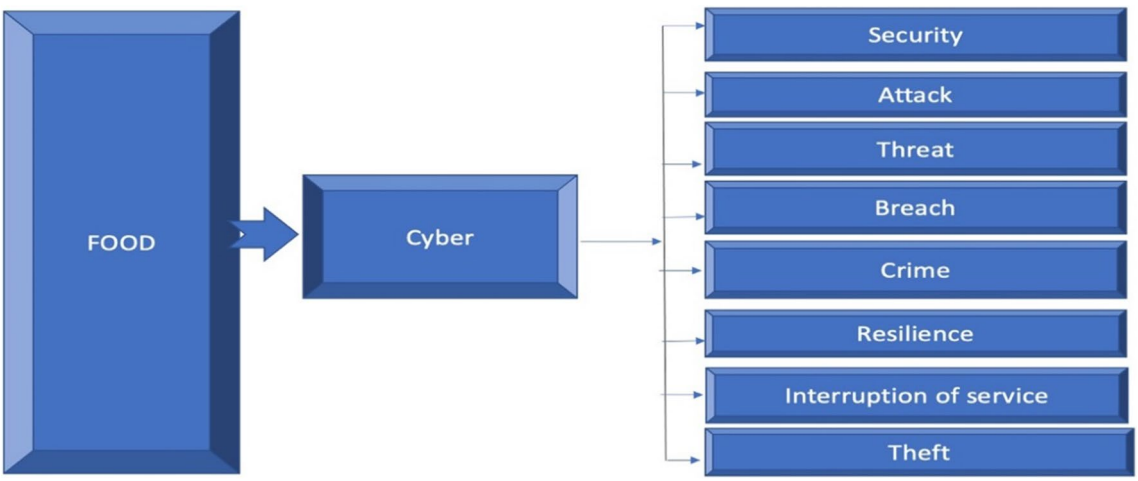


Fig. 2 Utilizing search terms to collect academic articles

with responsibilities related to their organization's IT. Additionally, some emails were directly dispatched to personnel within the information technology (IT) departments of food companies.

4 Survey results, discussions and limitations

4.1 Results

The Evaluation of Cybersecurity Awareness, Preparedness, and Technology Adoption in the Food Industry:

To gauge the extent of importance placed on cybersecurity by food companies, a comprehensive questionnaire was designed to assess their awareness, preparedness, and technological measures against cyberattacks. The questionnaire covered various aspects, with questions 1 and 5 focused on measuring awareness, questions 2, 3, 4, 7, and 8 aimed at assessing preparedness, and question 6 targeting the technologies in use. To learn more about "To what extent the food companies value cybersecurity," a few questions and their answers have been provided below.

Given that the respondents were people employed by food firms, notably in the information technology division or with duties associated therewith the likelihood of collecting misleading or erroneous data is minimal.

1. Does your company have any cybersecurity concerns?

This question was aimed to ascertain the outlook of the food companies towards cybersecurity in the organization and the industry as a whole. The results indicate that 45.83% of companies believe they have cybersecurity concerns, while 37.50% strongly believes, 12.50 % are uncertain and 4.17% disagree as shown in Fig. 3. This shows that people working in food companies are concerned and aware of security breaches taking place in cyber world which is an encouraging sign. However, it is surprising to note that robust measures to address these concerns have not been implemented. Possible reasons for this could include the lack of stakeholder focus and they take it as information and technology risk rather than a business risk, leading to its relegation to a lower priority [28].

2. Has the company implemented any anti-virus software on each computer?

This question aimed to understand the outlook of food companies regarding cybersecurity within their organization and the broader industry. As shown in Fig. 4 the survey results reveal that 50% of the companies have implemented antivirus software, while 41.67% have not. Additionally, 4.17% stated that antivirus software is not required, and an equal percentage reported being unaware of its necessity. The fact that only 50% of companies have implemented antivirus software is not commendable as installing antivirus software is a fundamental and essential step in safeguarding systems

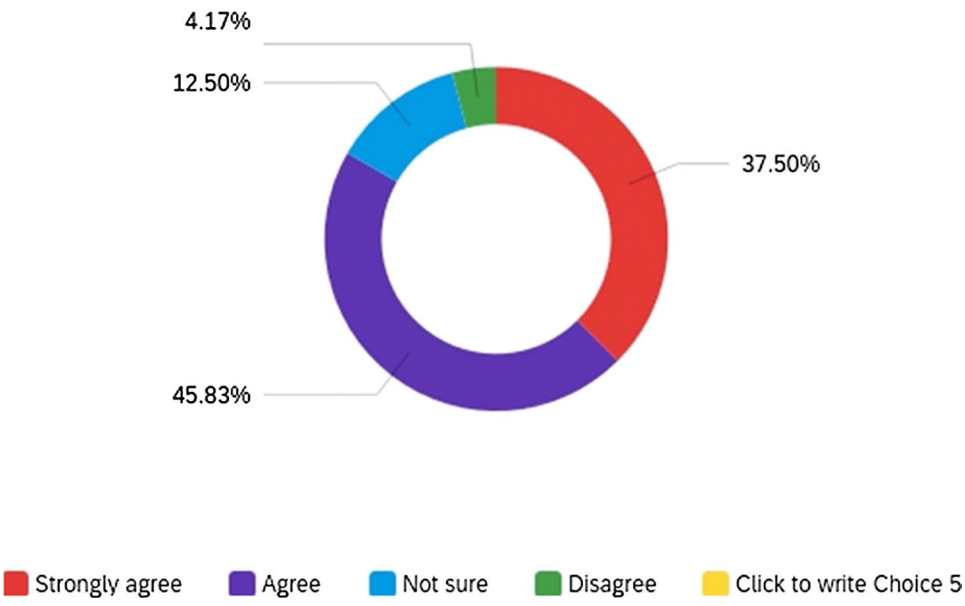


Fig. 3 The level of cybersecurity concerns

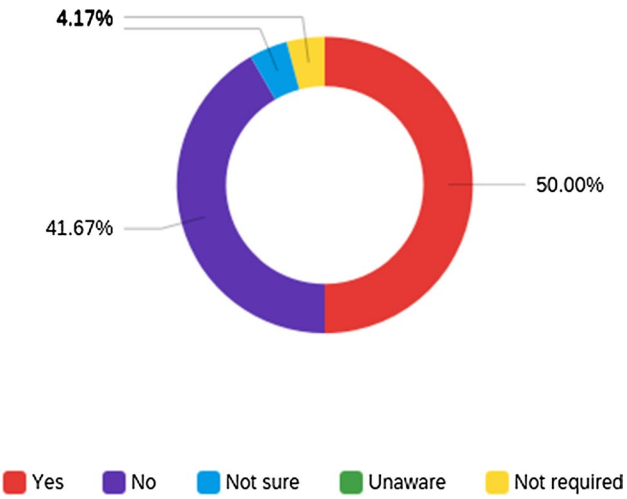


Fig. 4 The rate of implementation of antivirus software on each computer

against any malicious activity. The lack of a satisfactory level of commitment to this basic measure suggests that some companies may hold the belief that they have nothing to lose. This demonstrates that food companies have not yet recognized the value of securing their specialized information and intellectual property, which can be compromised or stolen.

3. Do all IT systems adhere to security policies, and do you undertake network penetration testing to detect risk and address them?

With the help of this question, we have tried to discover whether food companies have established guidelines or practices to evaluate their cybersecurity posture and just over of a quarter of the respondents agree that the companies adhere to security policies while 45.83% do not. Additionally, 16.67% were not sure, 8.39% were not aware and 4.17% considered adherence to security policies unnecessary as showed in Fig. 5. To understand if there is any anomaly in the network or system time to time penetration test is crucial. However, the survey reveals that only 25% of the companies undertake such tests. These findings suggest a lack of comprehensive policies or guidelines to detect and mitigate cyber threats. The absence of clear demarcation between operational and information technology domains further exacerbates the situation Just as the food industry has established guidelines like HACCP for food safety, a similar framework is needed to address cybersecurity concerns.

4. Are all employees trained on cyber security to spot the risk?

Literature review indicates that many cybercrimes occur due to employee ignorance and lack of awareness [28]. The survey findings in Fig. 6 show that only 25% of the staff confirmed receiving cybersecurity training and being able to

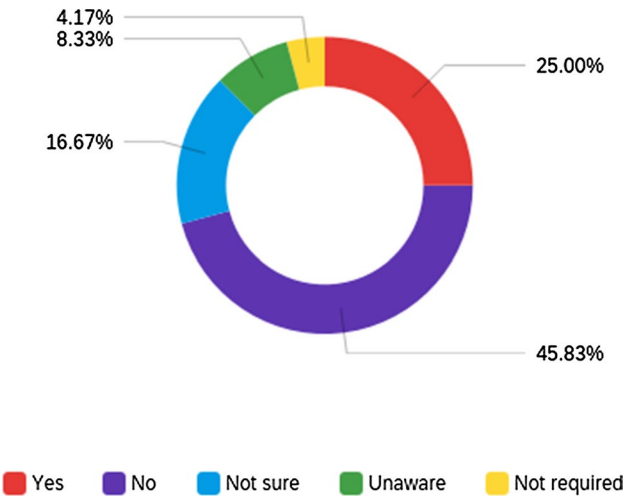


Fig. 5 Observing to security policy and penetration test

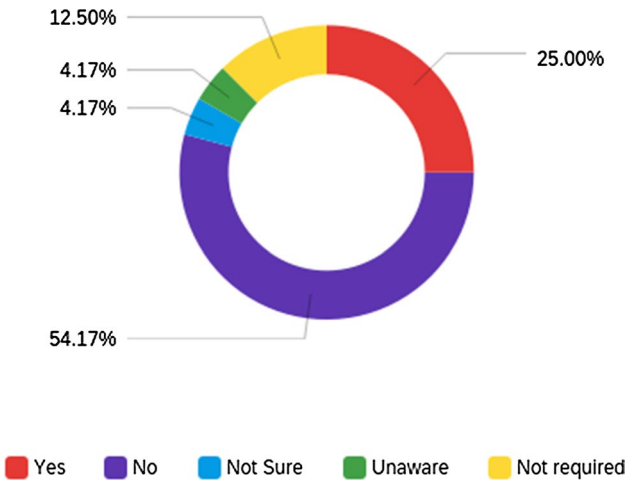


Fig. 6 The number of employees trained in cybersecurity and can spot cyber risk

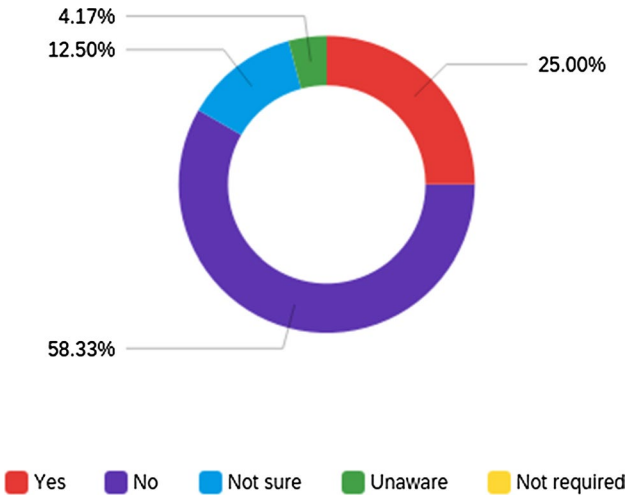


Fig. 7 Data security

spot the risk, in contrast, 54.17% have not received such training, and 12.50% believe it is unnecessary. Training creates awareness and contribute to system maintenance and fighting with the loose notes available in the system. It can help in eliminating the cyberthreats in the initial stage itself.

5. Do you all have a good understanding of to what extent data is secured?

The food sector generates vast amounts of data, necessitating robust guidelines for its protection. However, the survey results indicated that only 25% of respondents were aware of the extent to which their data is secured, while 58.33% stated that they were not aware as showed in Fig. 7. This once again highlights the lack of seriousness and insufficient training and knowledge regarding information security. Data security is a critical aspect that requires immediate attention.

6. Does your company use any of the following technologies from Industry 4.0 to enhance the food manufacturing process?

Question was aimed to understand the most commonly utilized technologies by the food companies so that right cybersecurity strategy can be researched. The findings as showed in Fig. 8 revealed that the majority of companies utilize the Internet of Things (IoT), whereas few also employing big data and one under naming other devices. This shows that food companies are leveraging Industry 4.0 tools to harness live data enhancing product quality and safety but on the other hand they are negligent towards securing the device and missing one of the most essential elements of Industry 4.0 which is cybersecurity.

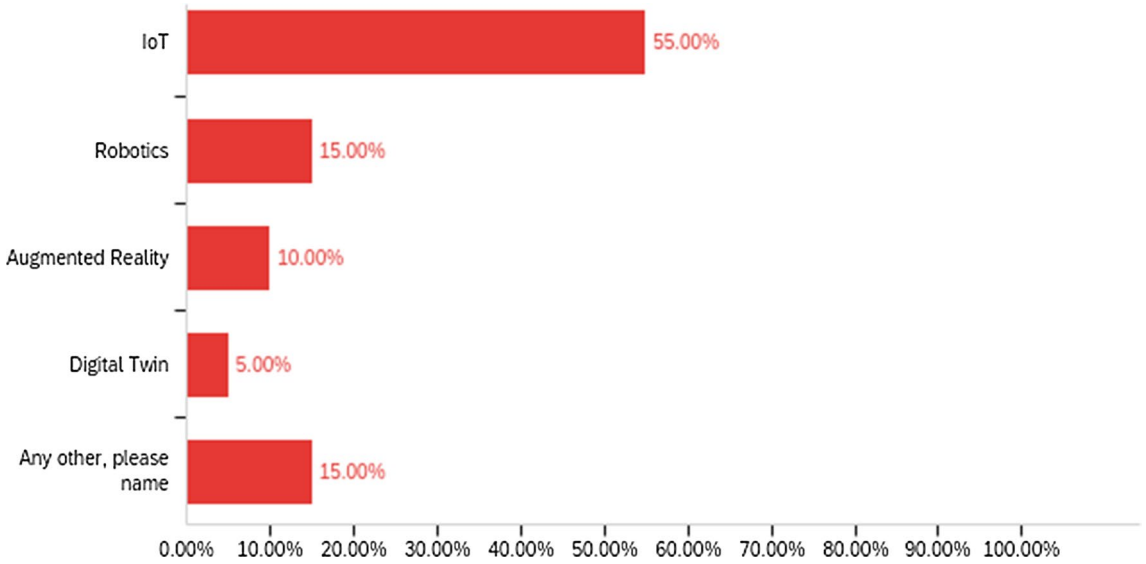


Fig. 8 Technologies used by food sector from industry 4.0

Fig. 9 No method at place to analyse cyber threat from third party

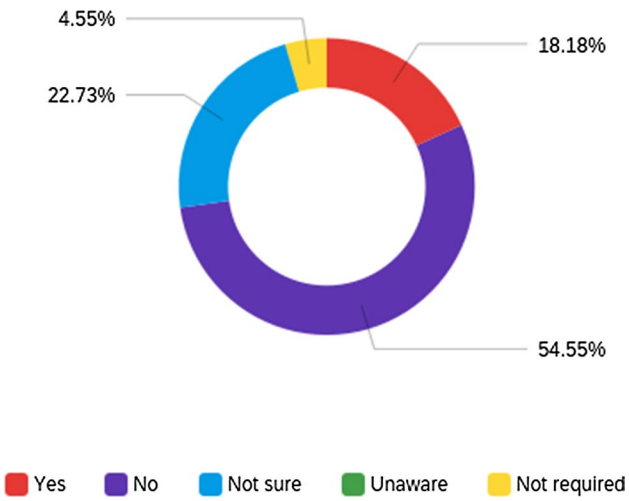
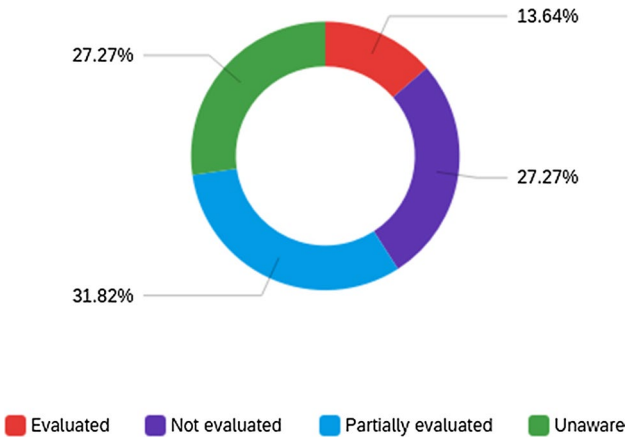


Fig. 10 Financial evaluation done by food companies in case of data breach



7. Do you have any procedures or checklists in place to analyse the cyber threat posed by your vendor or any other third party?

The 54.55% of the companies do not have established procedure or checklists to analyse the cyber threats posed by vendors or third parties as showed in Fig. 9. This creates an easy pathway for cybercriminals to get through the network to exploit.

8. Have you evaluated the financial penalties of leaking high-risk data?

The survey revealed that 13.64% of respondents have evaluated the financial penalties involved in the event of data leaks resulting from cyberattacks. Meanwhile, 31.82% have partially evaluated them, 27.27% have not conducted any evaluation, and 27.27% are unaware of their evaluation status, as shown in Fig. 10. This shows the lack of awareness and a causal approach of the food companies.

This section reveals that most food companies are aware of cybersecurity risks but lack strong measures to combat them. Only half have antivirus software, and a mere quarter follows security policies or conducts penetration tests. Training on cybersecurity is provided to just 25%, with many employees unaware of data security levels. Despite using Industry 4.0 technologies like IoT, food companies neglect cybersecurity for these systems. Furthermore, most lack protocols for evaluating cyber threats from vendors or the financial impact of data breaches. Table 1 summarises the key findings for this survey.

4.2 Discussion

In the food industry, there is a prevailing assumption that cybersecurity awareness is weak [29]. However, there is no comprehensive scholarly study that backs up this claim so through survey an effort has been put to understand the level of awareness. It has also been discovered that be it related to smart farming or smart manufacturing the stakeholders and senior management do not perceive cyber threats as business risk and consequently, no well-defined strategies or framework has been highlighted or framed for the sector [30]. There exists a significant disparity between awareness and the implementation of defense in depth. It has been also observed during the initial implementation of new operational technology, cybersecurity is not adequately considered as a project component. Instead, it is addressed as the threat feature and leading to patchwork solutions that add unnecessary costs and act as a deterrent to the implementation of cybersecurity in the food sector.

There is a widespread belief in the industry that the food sector is not a lucrative target for cyber attackers, primarily due to the misconception that there is little financial gain associated with targeting this sector. But this myth can be refuted by the fact that food and beverage sector is one of the largest sectors comprising 10,990 food and drinks manufacturing businesses, 7,585 employers are associated with this industry, contributing worth more than £120bn to the economy [31]. Notably, 97% of these businesses are SMEs. While regulation has been slow to catch up with providing robust cybersecurity support to the industry, one positive development is that the UK government has classified the food sector as one of the 13 critical infrastructures, although it has not got that much weightage and regulatory supervision, unlike other critical infrastructures have enjoyed in terms of resilience. This observation is evident from the report published by Centre for the Protection of National Infrastructure (CPNI) report in 2010 [32] and the guidance was more focused on natural disaster rather than cybersecurity. Nevertheless, recent events, such as the significant cyber-attack in 2017, have triggered a change and the report published in 2018 has mentioned regarding good practice guidance on cyber security [33, 34]. This effort signifies the increasing recognition of the criticality of cybersecurity for food security.

Table 1 Of key survey findings

Question	Yes	No	Unsure/not aware	Not required
Cybersecurity concerns	45.83%	4.17%	12.50%	–
Anti-virus software installed	50%	41.67%	–	4.17%
Adherence to security policies	25%	45.83%	16.67%	4.17%
Employee training on cybersecurity	25%	54.17%	–	12.50%
Understanding of data security	25%	58.33%	–	–
Use of Industry 4.0 technologies	Mostly IoT then robotics			
Procedures for third-party cyber threat	–	54.55%	–	–
Evaluated financial impact of data leak	13.64%	27.27%	27.27%	–

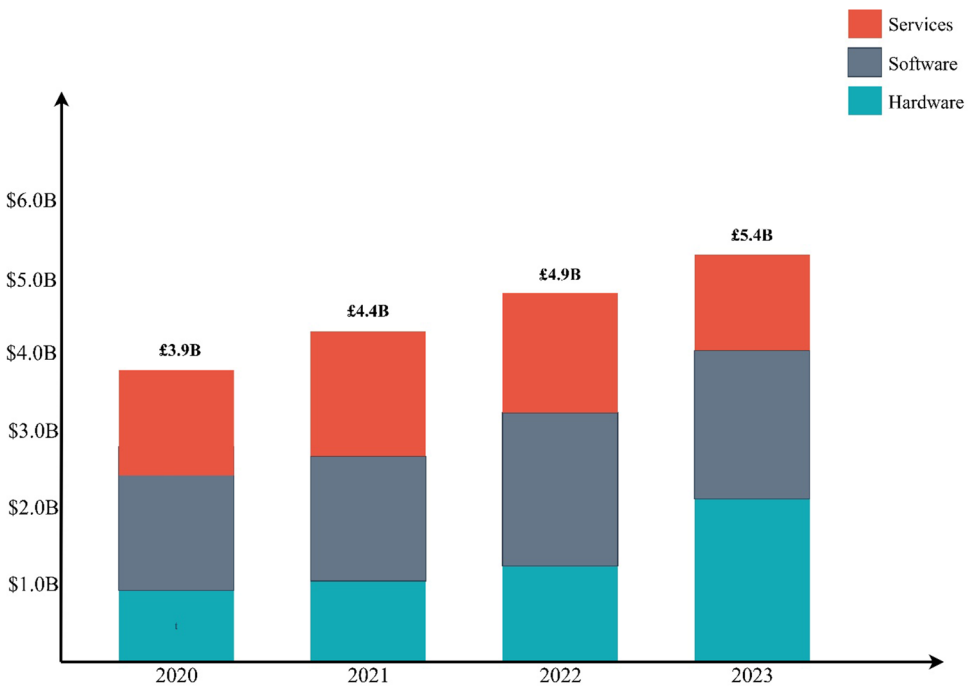


Fig. 11 Revenue from cybersecurity in the consumer goods sector from (2020–2023) [38]

Though it's a long journey and more concerted efforts are required to make organisation take cybersecurity in their framework as they take food security. Figure 11 shows the proceeds generated by the sale of cybersecurity products and services to businesses operating in the consumer goods sector, encompassing the period from 2020 to 2023.

From the literature review and survey, it can be concluded that there are limited case studies or examples available in the food sector to reflect the importance of cybersecurity and this scarcity contributes to the lack of seriousness among personnel and management of the companies within the sector. The number of cyberattacks incidents are low in the food sector compared to other industries such as financial, health and that also contributes to ignorance, non-implementation and low expenditure on cybersecurity within the sector.

4.3 Limitation of the survey

The sample size and low participation rate from food companies can be taken as a major limitation in depicting a better result and clarity. Despite assurances of anonymity and confidentiality, many food companies were reluctant to participate or disclose their responses to these sensitive issues. Extensive efforts were made, including follow-up calls to encourage participation. While conducting interviews with industry professionals could have yielded better data, this approach was discarded due to stricter regulations after COVID-19 pandemic outsider are not allowed to protect staff from contracting any disease and time constraints.

5 Cybersecurity strategical framework

Fundamentally, any organization is composed of three elements: people, processes, and systems (machines) that facilitate the execution of work. It is often observed that significant cyber-attacks occur due to employee negligence or system vulnerabilities [35]. Not all cyber-attackers are external; they can also be disgruntled employees, partners, or management [28]. Not all cyber attackers are external; they can also be disgruntled employees, partners, or even management [36]. Keeping this information in view the following framework has been constructed. While numerous frameworks recommended by various organisations and other researchers, however, very few are specific to the food industry, and some are excessively lengthy and cumbersome or technology specific. Given the complex interdependencies within the food industry, it is crucial for all stakeholders to contribute to the development of a comprehensive cybersecurity framework that considers the holistic nature of the business, rather than focusing solely on information and communication technology. A patchwork or hasty approach will not be sufficient. Food companies must embrace security standards throughout the whole organisation and linked networks in order to address rising risks. Large-scale food companies usually have

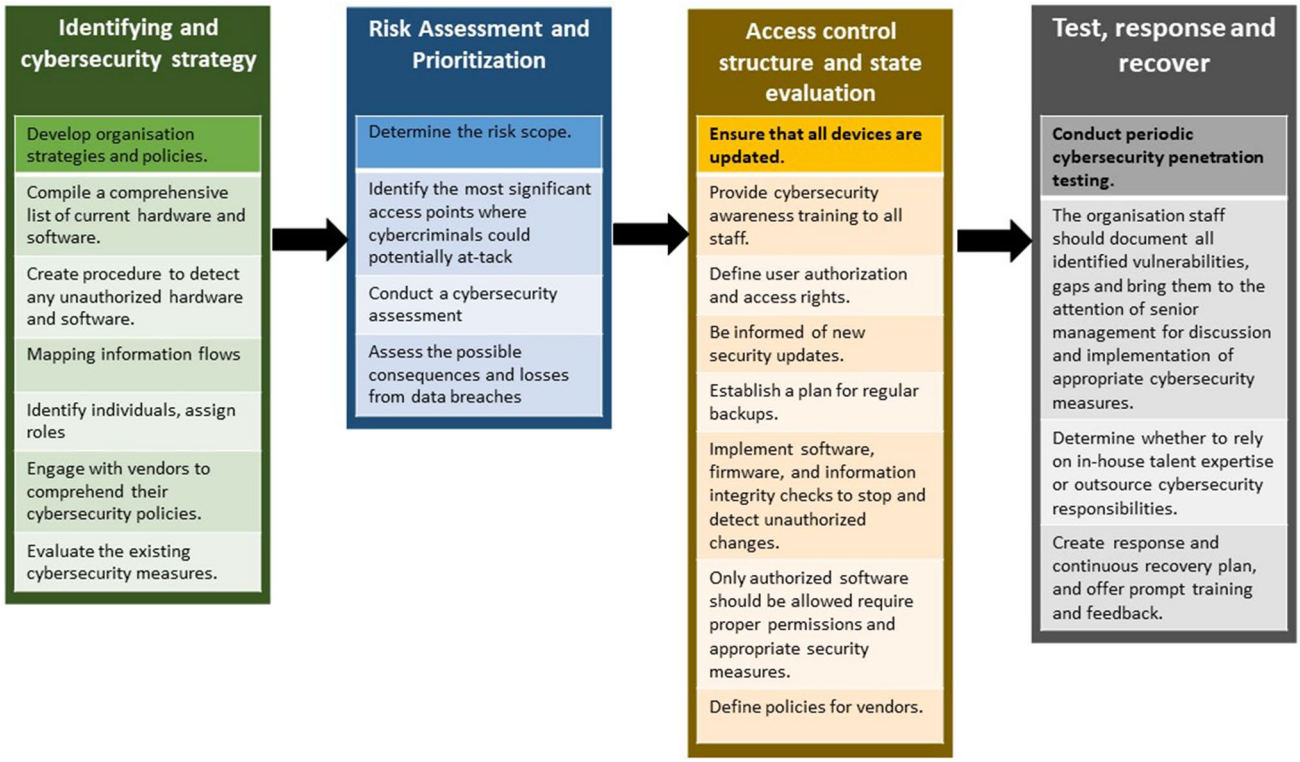


Fig. 12 Safeguarding through framework

an information technology department with dedicated personnel responsible for information technology security, but mid-scale and small-scale enterprises lack this capability. Mid and small-scale food businesses are still using legacy systems, embracing Industry 4.0 technologies to improve productivity, but failing to safeguard those systems and devices from cyberthreats. In the UK, the food sector is predominantly composed of 97% of small and medium enterprises [31, 39]. Although this recommendation is applicable to all food companies, it is particularly relevant for small and mid-scale food companies to defend against cyber-attacks and ensure effective cybersecurity implementation. The reasons for the emergence of cyber issues, as well as the suggested framework, are presented in Fig. 12.

5.1 Identifying and strategy

Setting up the policies identify the critical asset—In the food industry everything is interrelated, so the first step is to identify the critical assets that require protection within the organization. This provides clarity and helps formulate the appropriate cybersecurity strategy and tools.

a) All assets used in the organization should be named, labelled, and documented. This is an approach, therefore all personnel from various levels of management should be involved to ensure a comprehensive understanding of processes and approvals.
b) Compile a comprehensive list of current hardware and software used in the organization, such as IoT devices, robots, and computers. Determine how many of these devices are connected to the internet, and document details such as user information, device type, model, serial number, physical location, and data storage.
c) Developing procedures to detect any unauthorized hardware and software within the organisation environment.
d) Draw a diagram of the information flow between operational technology and systems.
e) Identify individuals, assign roles, and develop policies for allocation, including role definition and assignment, management support, interdepartmental coordination, and adherence to regulations.
f) Engage with vendors to comprehend their cybersecurity policies and ensure alignment with the organization's policies, as third parties often introduce cyber threats.
g) Evaluate the existing cybersecurity measures and assess their compatibility with the suggested framework to estimate potential costs.

5.2 Risk assessment and prioritization

It may also be proposed that the identification of vulnerabilities is a crucial step in the process. After classifying the asset, whether human or machine, it becomes imperative to uncover the associated threats. Comprehending the potential risks enables the formulation and application of suitable countermeasures.

a) Identify the types of assets that could be at risk from a cyberattack, including hardware, software, people, and third-party vendors.
b) Identify all the sensitive points that could be exploited by cybercriminals for attacks, manipulate data, or steal information. Secure all endpoints, such as laptops, desktops, and mobile devices, with antivirus software and firewalls.
c) Conduct a cybersecurity assessment for the food and agriculture company to evaluate its current security posture. This will help in identifying the most suitable security tools and technologies that align with the company's organizational goals, productivity requirements, and budget constraints. This process is commonly referred to as penetration testing.

5.3 Access control structure and state evaluation

Access control structure should be defined to protect the identified asset. It should define which system or process will be used to protect against cyber threats. This will help in laying a guideline for all to understand how to protect data and which control will be accessed to protect it and who will be responsible.

a) Ensure that all devices are updated with the latest software versions and implement access controls to restrict the flow of malware. Encrypt all files to prevent unauthorized access in case of interception. Encryption should be applied to all data, both at rest and in transit.
b) Provide cybersecurity awareness training to all staff members, especially executives, to prioritize cybersecurity within the organization. Educate and train the workforce to recognize and address cyber threats effectively.
c) Define user authorization and access rights. Implement a strong password policy and maintain logs that are regularly monitored to prevent data theft and malware attacks.
d) Be informed of new security updates, versions and keep up with current development. For example, operating system suppliers continually update their systems to reinforce their security settings as new threats emerge, thus systems should be updated from time to time.
e) Establish a plan for regular backups of systems and store them securely on separate networks.
f) Implement software, firmware, and information integrity checks to stop and detect unauthorized changes to manufacturing system components during storage and transport as needed.
g) Only authorized software should be allowed, and exceptions should require proper permissions and appropriate security measures. Discourage the "bring your own device" policy whenever possible.
h) Define policies for vendors, including provisions for releasing third-party vendors from service level agreements in case of breaches.

5.4 Test response, and recovery

Once the structure is established, it should be periodically tested to ensure it effectively safeguards the identified assets. All well-defined policies and procedures should be documented to ensure smooth operation across the enterprise.

a) Conduct periodic cybersecurity penetration testing within the company to evaluate the effectiveness of the implemented cybersecurity measures.
b) The organisation staff should document all identified vulnerabilities and gaps and bring them to the attention of senior management for discussion and implementation of appropriate cybersecurity measures.
c) Determine whether to rely on in-house expertise or outsource cybersecurity responsibilities.
d) Create response and continuous recovery plan and offer prompt training and feedback.

6 Conclusion and future work

This research aimed to critically assess the state of cybersecurity in the food industry, a sector increasingly reliant on digitalisation yet lacking in cyber defense measures compared to industriessuch as finance, healthcare, information technology, and transportation. This is highlighted in this research, where it becomes evident that other sectors are investing significantly more in bolstering their cybersecurity measures. Our findings reveal a significant gap in cybersecurity preparedness within the food sector, emphasising the urgent need for enhanced security measures. The proposed specialized security framework, developed through extensive analysis, is customised to address the unique challenges and vulnerabilities of the food industry. The risk of hackers targeting vulnerable industries raises concerns, and without adequate precautions, cyber attacks could affect the food industry. Furthermore, this research underscores the risks linked to cybercrime within the food sector, along with the challenges encountered during its implementation. Consequently, it strongly advocates for the early integration of cybersecurity measures to mitigate associated risks and proposes the adoption of a comprehensive cybersecurity framework. The research also underscores the pivotal role of stakeholders in shaping and implementing cyber policies within their organizations to ensure uninterrupted business operations, emphasizing the urgency of this measure.

Future research should involve corporate interviews with stakeholders and owners of small and medium enterprises in the food industry.. Conducting these interviews will yield valuable insights into various perspectives on cybersecurity within the industry. The industry calls for further exploration to better comprehend existing cyber risks and to capture the attention of senior stakeholders. A comprehensive investigation is needed to identify companies that have fallen victim to cyberattacks, the challenges they have encountered, and the countermeasures they have employed. These cases will serve to underscore the critical importance of cybersecurity within the industry.

Acknowledgements We would like to express our sincere gratitude to all of the survey participants who took the time to complete our survey. Your insights and feedback were invaluable to the completion of this research project.

Author contributions AA: data curation, formal analysis, validation, investigation, methodology, writing—original draft, software, writing—review and editing, AK: data curation, investigation, write survey questions, SJ: data curation, formal analysis, investigation, methodology, software, supervision, writing—original draft, writing—review and editing. NW: formal analysis, investigation, project administration, writing—review and editing. MA: formal analysis, methodology, project administration, validation, visualization; writing—original draft, writing—review and editing. KS: project administration, resources, software, supervision, validation, visualization.

Funding This research received no external funding.

Data availability The authors confirm that the data supporting the findings of this study are available within the article.

Declarations

Competing interests 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.

References

1. National Cyber Security Strategy. Cyber Security Breaches Survey 2021. 2021. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021. Accessed 26 Jan 2023.
2. Laranjo M, Córdoba MDG, Semedo-Lemsaddek T, Potes ME. Food microbiology. Biomed Res Int. 2019;2019:837–8. https://doi.org/10.1155/2019/8039138.
3. Prasad R, Rohokale V. Cyber threats and attack overview. In: Prasad R, Rohokale V, editors. Cyber security the lifeline of information and communication technology. Cham: Springer; 2020. https://doi.org/10.1007/978-3-030-31703-4_2.

4. Noor Hasnan NZ, Yusoff YM. Short review: Application Areas of Industry 4.0 Technologies in Food Processing Sector. 2018 IEEE 16th Student Conference on Research and Development, SCOReD 2018. 2018; 1–6. https://doi.org/10.1109/SCORED.2018.8711184.
5. Antrum CJ, Waring ME, Cooksey Stowers K. Personal vehicle use and food security among US adults who are primary shoppers for households with children. Discover Food. 2023;3:9. https://doi.org/10.1007/s44187-023-00048-6.
6. Settanni, G., Shovgenya, Y., Skopik, F., Graf, R., Wurzenberger, M., & Fiedler, R. (2017) Acquiring Cyber Threat Intelligence through Security Information Correlation. 3rd IEEE International Conference on Cybernetics (CYBCONF), Exeter, UK, 2017, pp. 1–7, doi: https://doi.org/10.1109/CYBConf.2017.7985754.
7. Alqudhaibi A, Albarrak M, Aloseel A, et al. Predicting cybersecurity threats in critical infrastructure for industry 4.0: a proactive approach based on attacker motivations. Sensors. 2023;23:4539. https://doi.org/10.3390/s23094539.
8. Parker S, Wu Z, Christofides PD. Cybersecurity in process control, operations, and supply chain. Comput Chem Eng. 2023;171:108169. https://doi.org/10.1016/j.compchemeng.2023.108169.
9. Javaid M, Haleem A, Singh RP, Suman R. An integrated outlook of cyber-physical systems for industry 4.0: topical practices, architecture, and applications. Green Technol Sustain. 2023;1:100001. https://doi.org/10.1016/j.grets.2022.100001.
10. Cartwright A, Cartwright E, Edun ES. Cascading information on best practice: cyber security risk management in UK micro and small businesses and the role of IT companies. Comput Secur. 2023;131:103288. https://doi.org/10.1016/j.cose.2023.103288.
11. Barreto L, Amaral A. Smart Farming: Cyber Security Challenges. 9th International Conference on Intelligent Systems 2018: theory, research and innovation in applications, IS 2018 – Proceedings. 2018; 870–876. https://doi.org/10.1109/IS.2018.8710531
12. Tuptuk N, Hailes S. Security of smart manufacturing systems. J Manuf Syst. 2018;47:93–106. https://doi.org/10.1016/j.jmsy.2018.04.007.
13. Alqudhaibi A, Aloseel A, Jagtap S, Salonitis K. Identifying and predicting cybersecurity threats in industry 4.0 based on the motivations towards a critical infrastructure. Amsterdam: IOS Press; 2022. https://doi.org/10.3233/ATDE220599.
14. El Bilali H, Allahyari MS. Transition towards sustainability in agriculture and food systems: role of information and communication technologies. Inform Process Agric. 2018;5:456–64. https://doi.org/10.1016/j.inpa.2018.06.006.
15. West J. A prediction model framework for cyber-attacks to precision agriculture technologies. J Agric Food Inform. 2018;19:307–30. https://doi.org/10.1080/10496505.2017.1417859.
16. Perales Gómez ÁL, Fernández Maimó L, Huertas Celdrán A, et al. SafeMan: a unified framework to manage cybersecurity and safety in manufacturing industry. Softw Pract Exp. 2021;51:607–27. https://doi.org/10.1002/spe.2879.
17. Alawida M, Omolara AE, Abiodun OI, Al-Rajab M. A deeper look into cybersecurity issues in the wake of Covid-19: a survey. J King Saud Univ Comput Inform Sci. 2022;34:8176–206. https://doi.org/10.1016/j.jksuci.2022.08.003.
18. Mahajan N, Chauhan A, Kumar H, et al. a deep learning approach to detection and mitigation of distributed denial of service attacks in high availability intelligent transport systems. Mobile Netw Appl. 2022;27:1423–43. https://doi.org/10.1007/s11036-022-01973-z.
19. Michelena Á, Aveleira-Mata J, Jove E, et al. A novel intelligent approach for man-in-the-middle attacks detection over internet of things environments based on message queuing telemetry transport. Expert Syst. 2023. https://doi.org/10.1111/exsy.13263.
20. Wilson C. Cyber threats to critical information infrastructure. In: Chen T, Jarvis L, Macdonald S, editors. Cyberterrorism. New York: Springer; 2014. https://doi.org/10.1007/978-1-4939-0962-9_7.
21. Verma HC, Srivastava S, Ahmed T, Usmani NA. Cyber threats in agriculture and the food industry. Hershey: IGI Global; 2023. p. 109–22. https://doi.org/10.4018/978-1-6684-8133-2.ch006.
22. Mustard S. The NIST cybersecurity framework. INTECH. 2014;61:1–6. https://doi.org/10.4018/978-1-6684-3698-1.ch003.
23. Bracho A, Saygin C, Wan H, et al. A simulation-based platform for assessing the impact of cyber-threats on smart manufacturing systems. Procedia Manuf. 2018;26:1116–27. https://doi.org/10.1016/j.promfg.2018.07.148.
24. Khan R, McLaughlin K, Laverty D, Sezer S. STRIDE-based threat modeling for cyber-physical systems. In: 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe). IEEE. 2017; pp 1–6. https://doi.org/10.1109/ISGTEurope.2017.8260283.
25. Kozik R, Choraś M. Current cyber security threats and challenges in critical infrastructures protection. 2013 2nd International Conference on Informatics and Applications, ICIA. 2013; 93–97. https://doi.org/10.1109/ICoIA.2013.6650236
26. Kshetri N, Voas J. Hacking power grids: a current problem. Computer. 2017;50(12):91–5. https://doi.org/10.1109/MC.2017.4451203.
27. Liang G, Weller SR, Zhao J, Luo F, Dong ZY. The 2015 Ukraine blackout: implications for false data injection attacks. IEEE Trans Power Syst. 2017;32:3317–8. https://doi.org/10.1109/TPWRS.2016.2631891.
28. Mukrimaa SS, Nurdyansyah, Fahyuni EF, et al. Food Industry Cybersecurity Summit Meeting Report. Jurnal Penelitian Pendidikan Guru Sekolah Dasar 6:128. 2016. https://conservancy.umn.edu/handle/11299/217704. Accessed 26 Sept 2023.
29. Nikander J, Manninen O, Laajalahti M. Requirements for cybersecurity in agricultural communication networks. Comput Electron Agric. 2020;179:105776. https://doi.org/10.1016/j.compag.2020.105776.
30. Ghobakhloo M. Determinants of information and digital technology implementation for smart manufacturing. Int J Prod Res. 2020;58:2384–405. https://doi.org/10.1080/00207543.2019.1630775.
31. Food and Drink Federation. Our Industry at a Glance. 104. 2019. https://www.fdf.org.uk/globalassets/resources/public/general/industry-at-a-glance-may2021.pdf. Accessed 08 Sept 2023.
32. Lehto M. Cyber-attacks against critical infrastructure. In: Lehto M, Neittaanmäki P, editors. Cyber security. Computational methods in applied sciences. Cham: Springer; 2022. https://doi.org/10.1007/978-3-030-91293-2_1.
33. UK G. Public summary of sector security and resilience plans. Cabinet Office, London. 2017. https://assets.publishing.service.gov.uk/media/5c8a7845ed915d5c1456006a/20190215_PublicSummaryOfSectorSecurityAndResiliencePlans2018.pdf. Accessed 14 Sept 2023.
34. Gupta S, Joshi D, Jagtap S, Trollman H, Haddad Y, Atescan Yuksek Y, Salonitis K, Raut R, Narkhede B. From failure to success: a framework for successful deployment of Industry 4.0 principles in the aerospace industry. Int J Indus Eng Oper Manag. 2023. https://doi.org/10.1108/IJIEOM-04-2023-0042.
35. Alqudhaibi A, Deshpande S, Jagtap S. Towards a sustainable future: developing a cybersecurity framework for manufacturing. Technol Sustain. 2023. https://doi.org/10.1108/TECHS-05-2023-0022.

36. Bendovschi A. Cyber-Attacks – trends, patterns and security countermeasures. Proc Econ Finance. 2015;28:24–31. https://doi.org/10.1016/S2212-5671(15)01077-1.
37. Jackson E. New risks to the missing middle of global meat supply chains. Thousand Oaks: SAGE Publications; 2023. https://doi.org/10.4135/9781071920510.
38. GlobalData. Cybersecurity in Consumer Goods – Thematic Research. 2022. https://www.researchandmarkets.com/reports/5640098/cybersecurity-in-consumer-goods-thematic. Accessed 26 Oct 2023.
39. Alqudhaibi A, Krishna A, Jagtap S, Afy-Shararah M, Salonitis K. Safeguarding food industry: understanding cyberthreats and ensuring cybersecurity. Eng Proc. 2023. https://doi.org/10.3390/engproc2023040011.