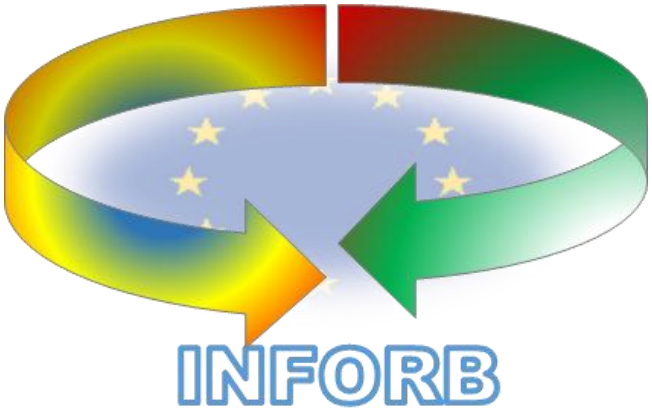

STUDY AND HANDBOOK REGARDING CYBER SECURITY AND SUPPLY CHAIN FOR THE FOOD SECTOR

DELIVERABLE D4.1

Version V1.0

EXECUTIVE SUMMARY

This document is structured in two parts, aiming to strengthen cybersecurity in the food sector in Romania and Bulgaria, in line with the NIS2 Directive and increasing digitalization.

Title I – **Study on Cybersecurity in the Food Sector** evaluates the maturity level of cybersecurity, highlighting digitalization trends, SME vulnerabilities, key cyber threats, and alignment with EU standards. Based on surveys, ENISA reports, and open-source data, it provides conclusions and targeted recommendations to enhance cyber resilience.

Title II – **Supply Chain Cybersecurity Risk Management Handbook** offers a practical framework for identifying and mitigating cyber risks across the digital supply chain. It incorporates international standards (ISO/IEC 27005, NIST RMF) and national legal frameworks, emphasizing technical safeguards, organizational responsibilities, and regulatory compliance.

Together, these components form a valuable tool for food sector organizations seeking to improve cybersecurity posture, ensure compliance, and foster operational resilience.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the European Cybersecurity Competence Centre can be held responsible for them.

Document control information

Settings	Value
Document title:	Study and Handbook regarding cyber security and supply chain for the food sector
Project number:	101128047
Project name:	Implementation of the NIS Directive in the food production, processing and distribution sector in Romania and Bulgaria
Project acronym:	INFORB
Author(s) of the document:	Gheorghiță Comăneci, Silviu-Nicolae Dorobanțu, Rozalia Parapuf, Diana Opriș, Gergana Rakova, Eli Kuyamova, Panayotka Panayotova
Deliverable identifier:	D4.1
Delivery deadline:	30.06.2025
Delivery date:	24.06.2025
Project Manager (PM):	Constantin Călin
Document version:	V1.0
Sensibility:	PU-Public
Date:	23.06.2025

Document evaluation and evaluators

Name	Role	Action	Date
Gheorghiță Comăneci	WP4 Coordinator	Draft document created	22.11.2024
Silviu Dorobanțu	Cybersecurity Expert	Original version (DNSC)	20.05.2025
Gergana Rakova	Project Coordinator	Update version (MGBEG)	20.06.2025
Eli Kuyamova	Project IT expert		
Panayotka Panayotova	BG Team Project Leader		
Advisory Board of Experts	Evaluation	Agreed version	23.06.2025
Constantin Călin	Project Manager	Final document assumed and delivered	24.06.2025

Document history

Review	Date	Created by	Brief description of the changes
V0	12.12.2024	Cybersecurity Expert	Draft document created. Documentation, analysis of sources. Documentation, analysis of sources.
V0.1	16.04.2025	Cybersecurity Expert & WP4 Coordinator	Rectification of updated document with information
V0.1.1	23.04.2025	Cybersecurity Expert	Updated document

V0.1.2	08.05.2025	Cybersecurity Expert	Update with information
V0.2	20.05.2025	Cybersecurity Expert	Update the document (Romanian language)
V0.3	23.05.2025	Cybersecurity Expert	Translated into English
V0.4	20.06.2025	Coordinator/Project Leader	Updated by Bulgarian Experts
V1.0	23.06.2025	WP4 Coordinator & Cybersecurity Expert	Final document version 1

Contained

TITLE 1. STUDY ON CYBERSECURITY IN THE FOOD SECTOR

Abstract

This part assesses the cybersecurity maturity of the food sector in Romania and Bulgaria, with a technical focus on digitalization levels, specific vulnerabilities of small and medium-sized enterprises (SMEs), key cyber threats, and the extent of compliance with EU cybersecurity standards. Drawing on structured surveys, ENISA threat assessments, and data from open sources, the study identifies gaps in technical controls, such as insufficient network segmentation, lack of endpoint protection, and limited incident response capabilities. The findings are used to develop targeted recommendations aimed at enhancing cyber resilience across the sector, including the adoption of standardized security frameworks, risk-based asset classification, and improved monitoring of critical digital infrastructure.

SECTION 1. INTRODUCTION

The food sector is undergoing an accelerated process of digitalization, integrating IT technologies and automated systems into the production, processing, storage and distribution of food. This digital transformation brings multiple benefits in terms of efficiency and traceability, but it also opens up new vulnerabilities in the face of cyber threats.

In recent years, significant incidents have been reported demonstrating the real impact of cyberattacks on the food chain: for example, in April 2021 a ransomware attack targeted a Dutch food distributor, blocking communication between warehouses and customers and leaving the shelves of a major supermarket chain without products for several days. Shortly after, the world's largest meat processor was forced to temporarily shut down its operations in the US, Canada, and Australia following another ransomware attack. Such incidents highlight the urgent need to strengthen cybersecurity in the food sector.

Cybersecurity in this area is not only about protecting company data, but also about ensuring the continuity of food production and distribution – an essential element of national and even global food security. The food sector is considered part of critical infrastructure, as its compromise can have serious consequences for the population (from food shortages to health risks). However, historically speaking, this sector has not received the same level of attention in cybersecurity policies as other sectors (such as finance or energy). That is why this study aims to assess the current state of cybersecurity in the food industry, identifying the main risks, challenges and specific protection measures, based on data collected from organizations in the field and guides provided by specialized bodies at European level.

Next, we will present the objectives and methodology of the study, the detailed analysis of the data of a survey conducted among companies in the food sector in Romania and Bulgaria, we will integrate current perspectives from ENISA (European Union Agency for Cybersecurity) publications on cybersecurity in the food sector or related sectors, and we will formulate conclusions and recommendations aimed at supporting the improvement of the level of cybersecurity in this critical sector.

Objectives of the study

Assessing the level of digital maturity and cybersecurity practices in food companies – by analysing the characteristics of organizations (size, location, activity profile) and the IT&C infrastructure used, including how they implement or outsource cybersecurity services.

Identifying the main perceived cyber risks and threats in the food sector – based on survey data and qualitative analyses (including open answers on security issues), as well as highlighting differences based on factors such as the size of the organisation or the geographical region.

Comparison of the situation in the food sector with trends and best practices at European level, from the perspective of ENISA – including recent statistics on cyber incidents in the food sector, regulatory provisions (e.g. extension of the scope of the NIS2 Directive) and forecasts on the evolution of cyber threats in this area.

Formulating specific conclusions and recommendations to improve cybersecurity in the food sector – addressed both to industry organizations (manufacturers, processors, distributors, etc.) and to decision-makers or technology partners, to reduce vulnerabilities and increase the cyber resilience of the food chain.

Methodologies

- **Survey data collection**

A questionnaire was carried out using the EU Survey platform, on behalf of the two counties separately (in BG, EN and RO version). These questionnaires were intended for organizations in the food sector in Romania and in Bulgaria, covering topics such as company profile, IT infrastructure and cybersecurity practices. The survey included both closed-ended questions (to quantify the use of certain technologies or services) and open-ended questions (to identify perceptions about cyber risks and challenges encountered). A total of 62 organizations in Romania in the field responded. Until 19.06.2025, in Bulgaria 38 entities responded the survey. The BG survey remains open for additional responses. The responses being anonymized and aggregated for analysis.

- **Data analysis**

The collected data were statistically analysed (descriptive and correlative analysis). The distribution of respondents by different criteria (type of organization, size, region, food sub-sector) was examined, the degree of adoption of cybersecurity solutions (internal vs. outsourcing) was assessed, and significant trends or correlations were identified (e.g., by organization size or geographic region). Also, a segmentation analysis (clustering) of organizations according to IT&C and security practices was applied, to highlight possible **distinct cyber maturity profiles**.

- **Qualitative analysis**

The responses to the open-ended questions in the survey were analysed to extract the main **themes and concerns related to cyber risks**. A *word cloud* of frequently mentioned terms was also created, to quickly identify the risks perceived as the most important. This textual analysis provided an overview of threat awareness among organizations.

- **Documentation and integration of ENISA sources**

In order to correlate the survey findings with the European context, recent publications by ENISA and other relevant bodies were consulted. Reports on the Threat Landscape, best practice guides and regulatory provisions (such as the NIS2 Directive) applicable to the food sector or related sectors (agri-food, supply chain, SMEs) were analysed. The relevant information from these sources was integrated into a separate chapter of the study, to highlight **the alignment of the situation in Romania with EU trends and recommendations**.

- **Delineation and structuring of the relationship**

The content of the study was organized in clear sections (introduction, methodology, analysis, conclusions, etc.) according to the requirements of a research report. The graphs and tables resulting from the analysis were included to visually support the conclusions, each figure being accompanied by a title and relevant explanations. At the end, a bibliography is provided listing the sources consulted and cited throughout the document.

SECTION 2. RESULTS OF SURVEY DATA ANALYSIS

Profile of respondent organisations

The survey involved 62 organizations in the food sector in Romania and until 19.06.2025 – 38 organizations in the food sector in Bulgaria, covering different links in the food supply chain. **The type of organization** indicates a predominance of private companies – all respondent entities being private firms. This can be explained by the economic structure of the sector, in which private initiative is predominant. Although state organisations or NGOs (e.g. health authorities, manufacturers' associations) are also active in the industry, they are poorly represented in the survey sample, suggesting the need to better understand their specific needs in the future.

Situation in Romania

From the perspective **of the food sub-sector** in which they operate, the respondents cover a wide range of activities. The majority (about 92%) have **food production** operations (from raw material processing to the manufacture of finished products), many of these companies also have **integrated distribution** (61%) or **storage** (52%) functions in the logistics chain. About 45% of respondents are also involved in **processing** (intermediate processing of food products). These cumulative percentages exceed 100%, as many companies have an integrated business model (e.g. they produce food and have their own warehouses and distribution networks). Thus, **the sample reflects a complex picture of the agri-food chain**, including both primary producers and processing units or wholesale distributors. This diversity allows us to capture cybersecurity challenges throughout the food chain.

Geographically, the organizations are spread across several development regions of the country, but not evenly. There is a significant concentration of respondents in **the Centre region** (which includes counties with an industrial-agrarian tradition, e.g. Mureș, Sibiu, Brasov), followed by **Bucharest-Ilfov**, which as a capital region acts as an economic and technological pole. The **North-West** (e.g. Cluj, Bihor) and **South-East** (e.g. Constanta, Galati) regions also have a notable presence, while the **South** and **North-East** areas are more modestly represented, and **the South-West (Oltenia) barely scores in the sample. This distribution partly reflects regional economic disparities: more economically developed regions with more solid IT infrastructure (such as Centre, Bucharest-Ilfov, North-West) were better represented, while those with less development appear with small shares. Figure 1 illustrates the distribution of respondents by development regions, highlighting the predominance of the Centre and Bucharest-Ilfov regions compared to others.**

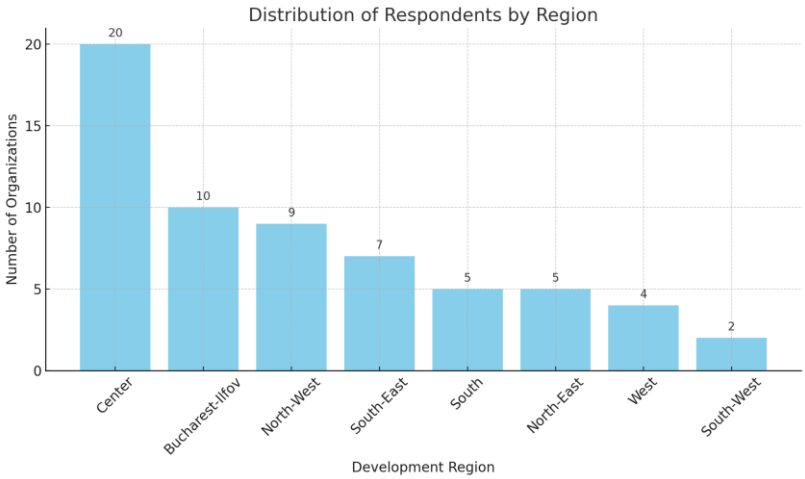

Figure 1. Romania - Distribution of respondents by development regions.

The Centre and Bucharest-Ilfov regions account for almost half of the sample, indicating a concentration of participating companies in the more economically developed areas. By contrast, regions such as the South-West or North-East have a much smaller number of respondent organizations, which may suggest both a lower number of food companies with a digital profile in these areas, as well as possible gaps in the degree of digitization and awareness of cybersecurity issues.

In terms **of company size**, small and medium-sized enterprises (SMEs) predominate. Around half of respondents classify themselves as **medium-sized enterprises** and a significant proportion as **large enterprises**. Only very few (isolated cases in the sample) are micro or small enterprises. This is in line with the overall structure of the national economy, where SMEs form the backbone of the food industry, while large companies (although far fewer in number) have a disproportionately large economic and logistical impact. The relevance of this structure for cybersecurity is major: SMEs usually have limited financial and human resources for investments in security, compared to large corporations that can afford dedicated teams and advanced technologies. Thus, supporting SMEs in adopting security solutions becomes critical for raising the overall level of protection in the sector.

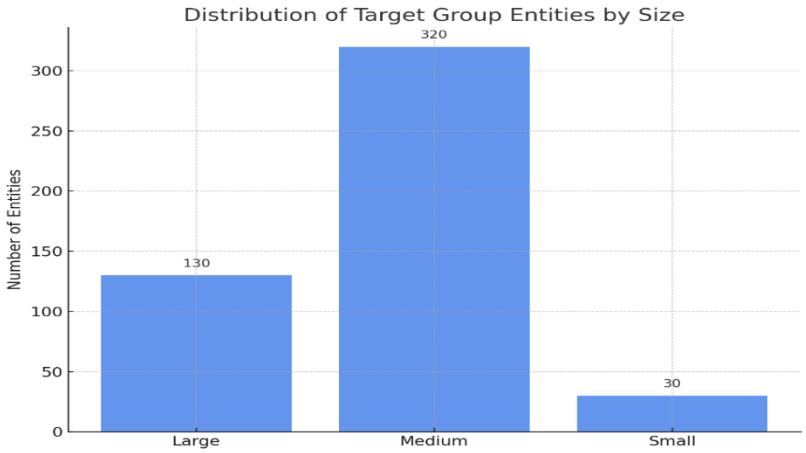

Figure 2. Romania - Distribution of respondents by company size.

Situation in Bulgaria

From the perspective **of the food sub-sector** in which they operate, the respondents cover a wide range of activities. The majority (about 87%) have **food production** operations (from raw material processing to the manufacture of finished products), some of these companies also have **integrated distribution** (13%) functions in the logistics chain. About 18% of respondents are also involved in **processing** (intermediate processing of food products). These cumulative percentages exceed 100%, as many companies have an integrated business model (e.g. they produce food and have their own warehouses and distribution networks). Thus, **the sample reflects a complex picture of the agri-food chain**, including both primary producers and processing units or wholesale distributors. This diversity allows us to capture cybersecurity challenges throughout the food chain.

Geographically, the organizations are spread across several development regions of the country. There is a significant concentration of respondents in **the North-Easter Region** (which includes regions with an industrial-agrarian tradition, (e.g. Varna, Dobrich), followed by **North-Central-region**. The Central-Southern, the **North-Western** and the **South-Western** (e.g. Sofia) regions also have a notable presence, while the **South-Eastern (Burgas)** area are more modestly represented. **This distribution partly reflects regional economic disparities: more economically developed regions with more solid IT infrastructure (such as Sofia, Varna) were better represented, while those with less development appear with small shares. Figure 1 illustrates the distribution of respondents by development regions, highlighting the predominance of the North-Easter and North-Central region compared to others.**

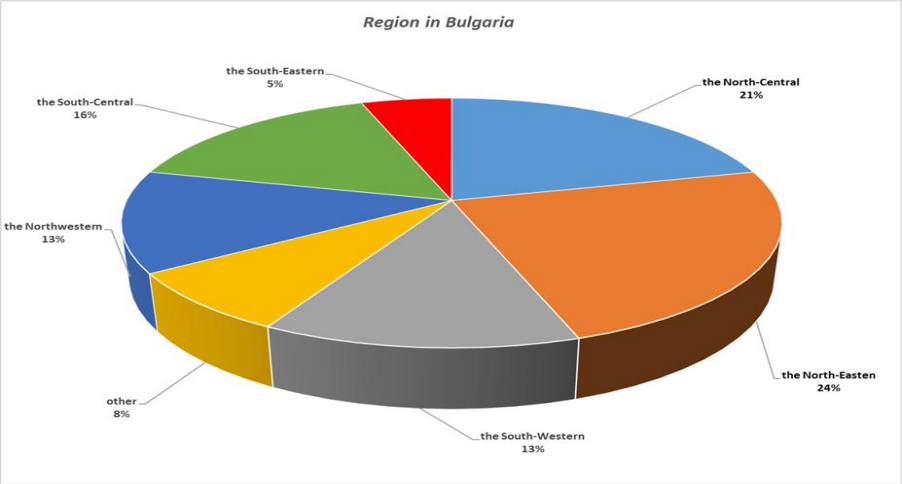

Figure 3. Bulgaria - Distribution of respondents by development regions.

In terms **of company size**, micro or small enterprises predominate. Only few are medium and large sized. This is in line with the overall structure of the national economy, where SMEs form the backbone of the food industry. SMEs usually have limited financial and human resources for investments in security, compared to large corporations that can afford dedicated teams and advanced technologies. Thus, supporting SMEs in adopting security solutions becomes critical for raising the overall level of protection in the sector. **Figure 3 illustrates the distribution of respondents by company size.**

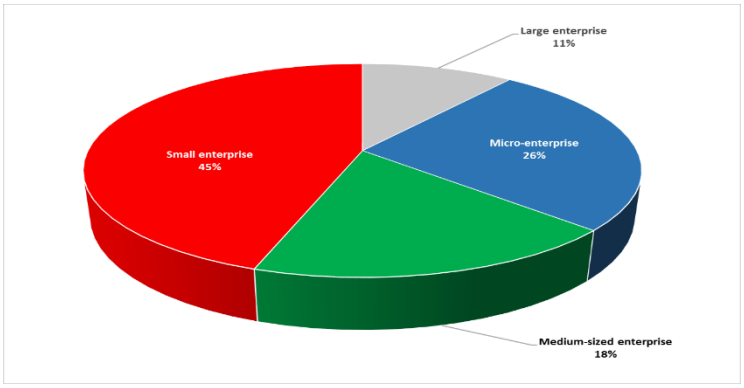

Figure 4. Bulgaria - Distribution of respondents by company size.

IT Services and Cybersecurity Practices

The analysis of the use of **IT&C services** by the organizations in the sample provides clues about their technological maturity and degree of concern for security. Basic services such as **system maintenance**, **network administration** and **technical support** appear to be the most frequently used – which is to be expected, as they are essential for the daily operation of any modern organization. Also, many companies indicate the use of services related to online presence, such as managing a **website** or **email services**. These elements constitute the fundamental level of digitalization, ensuring the company's continuous operability and communications.

On the other hand, **advanced IT services** – for example, cloud computing solutions, industrial process automation, business intelligence – are more the prerogative of large organizations or those in sectors perceived as technologically critical (such as transport or finance). Only a fraction of the

responding food companies (those with more substantial resources) mentioned the use of such advanced solutions, which indicates an **uneven degree of digitalization** among the sector: a few spearhead firms adopting cutting-edge technologies, while most remain at the level of the basic tools necessary to operate.

Specifically related to **the cybersecurity solutions and measures adopted**, we found significant variation between organizations. A central aspect is the way **of managing the cybersecurity function**: internal (with its own staff and local resources) or outsourced (by contracting specialized suppliers). The results for Romania show that there are four major situations (see Figure 4):

- Organizations that **do not have a dedicated cybersecurity function** (either do not consider applicable or do not have any specialized services) – about a third of the sample (34%) are in this situation, which may indicate a latent risk, these companies likely relying only on the minimum measures implemented by general IT teams.
- Organizations that manage **security exclusively internally** – in ~34% of cases, companies rely on their own IT staff to ensure security (installation of antiviruses, firewall, security maintenance, etc.), without resorting to external services.
- Organizations that **fully outsource** cybersecurity services – representing about 11% of respondents, they have contracts with specialized providers (MSPs/MSSPs) that deal with the protection of their infrastructure.
- Organizations that have a hybrid approach **(internal and outsourced mix)** – about 21% of respondents use a combination: they keep some security duties in-house, but outsource certain critical services (e.g., 24/7 monitoring, vulnerability auditing or incident response).

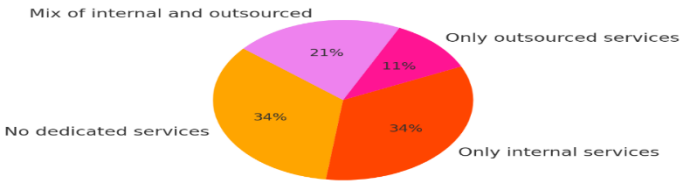

Figure 5. Romania - How cybersecurity services are managed in the respondent companies.

It can be seen that only a small part (about 11%) relies exclusively on outsourced services, while most prefer either in-house solutions (own staff) or a combination of the two. Notably, a third of companies do not have dedicated security services, which indicates a potential vulnerability – either these companies are very small and did not consider it necessary, or there is a lack of awareness of cyber risks. At the same time, the high percentage of those who use **only in-house solutions** reflects SMBs' preference for low-cost options and local control, but these in-house solutions are often **basic solutions** (e.g. free antivirus, default firewall) that may be insufficient against advanced threats.

Regarding **the security technologies implemented**, the data show that **the basic measures are relatively well represented**:

- Almost all organizations reported using an **antivirus** on their workstations – in fact, 98% confirmed that all their computers and laptops are protected with up-to-date antivirus solutions. This shows that the minimum level of endpoint protection is ensured in most cases.
- As for network **firewalls** (or Next-Generation Firewall solutions), ~84% of organizations have such a solution (either in the form of dedicated hardware or as a virtual appliance or cloud service). Only 16% indicated that they do not have a firewall at all, especially very small entities or probably in the early stages of computerization.

- **Backups** are also an almost universal practice: 92% of companies have implemented a regular backup solution for important data, either locally or in the cloud, thus ensuring that they can recover their data in case of incidents (failures or ransomware attacks).
- Other security solutions mentioned: **access control** systems (including domain/Active Directory control in the cases of larger companies), email security solutions (e.g. anti-spam filters, secure email gateway), IDS/IPS tools for detecting network intrusions, and to a lesser extent data loss prevention (DLP) or **WAF (Web Application Firewall)** solutions for the protection of public web applications.

However, the adoption of these more advanced security technologies (IDS/IPS, DLP, WAF, etc.) is **uneven**: large companies and those with a more complex technological profile tend to have them implemented, while traditional SMEs in the food industry are usually limited to antivirus, firewall and backup. The main reason given in informal discussions is related to **costs and the necessary expertise** – many small companies consider that the minimum set of measures is sufficient and do not have the staff or budget for Enterprise solutions. This highlights a potential **exposure to advanced threats** of a significant part of the sector: malicious actors can exploit the lack of advanced protections in SMEs to launch more sophisticated attacks (such as network penetration and undetected lateral movement in the absence of an IDS, or exfiltration of sensitive data if there is no DLP).

On the other hand, outsourcing security to specialized firms provides access to cutting-edge expertise and technologies (24/7 monitoring, threat intelligence, rapid intervention), but it is not without challenges. Respondents who opted for outsourcing mention benefits such as periodic vulnerability audits and strategic consulting but also recognize **the associated risks**: lock-in, possible delays in response due to service-level contracts, as well as long-term costs that can become substantial. The solution to which our conclusions converge is the mixed one: **a strategic combination of internal and external solutions** seems to be the optimal approach, allowing the organization to maintain control over critical issues and at the same time benefit from the contribution of external expertise where needed.

The relational analysis of the data highlighted some **important correlations**:

- **Organization size vs. technological complexity:** There is a clear trend that **larger organizations** (large enterprises) use a **wider range of IT technologies and security solutions** than SMEs. This is to be expected, as large companies have more complex operations (requiring automation, enterprise applications, interconnection with partners, etc.) and at the same time have more consistent resources for IT investments. In contrast, **SMEs**, although constrained by budgets, are also gradually starting to adopt more advanced technologies as they become more accessible, a sign that there is an **increase in digitization** including among medium-sized companies in the food sector. This slow but sure progress indicates that more and more SMEs are aware of the importance of technology (including security) for competitiveness.
- **Size vs. security outsourcing:** Large enterprises tend to **outsource** more cybersecurity components (for example, a manufacturer with thousands of employees may use an outsourced Security Operations Centre), while SMEs rely mostly on internal efforts or none at all. Medium-sized companies seem to frequently choose the mixed model (they keep the basic management in-house but outsource certain specialized services). This distribution underscores the need for category-specific security offerings: SMBs could benefit from outsourced bundled services or easy-to-use platforms (due to a lack of dedicated staff), and

large companies are emphasizing the integration of vendors into their complex security strategy.

- **Geographic region vs. technology adoption:** The regional differences identified in the respondents' profile are also reflected in the degree of adoption of advanced solutions. In developed regions such as **Bucharest-Ilfov** (and partly centre or West), companies have easy access to IT service providers and better infrastructure, leading to a **higher adoption of state-of-the-art technologies** and outsourced services. For example, many companies in Bucharest mention the use of cloud services or collaboration with local security consultants, while in regions such as the South-East or North-East, companies rely almost exclusively on their own IT teams and traditional solutions. Thus, **less technologically developed regions** have a different risk profile: they tend to be more exposed to common threats (due to the predominance of basic solutions and the lack of specialists), while companies in advanced regions face a more diverse spectrum of threats (being targets for more sophisticated attacks, according to the technologies used).
- **Region vs. perceived risks:** An interesting result from the qualitative analysis indicates that respondents from highly digitized areas (e.g. Bucharest) mentioned concerns about complex threats such as **advanced ransomware attacks**, industrial espionage or supply chain attacks, while respondents from less developed regions more often mentioned "basic" problems – such as, **regular phishing** or lack of internal IT skills. This suggests a **differentiated awareness**: where companies have already been exposed to an environment with more complex attacks, the perception of risk is more acute and nuanced, while elsewhere an attitude of "something serious cannot happen to us, we are small" still prevails.

The analyses for Bulgaria show significant differences between the organizations regarding the adopted cybersecurity decisions and measures. A key aspect is the way the cybersecurity function is managed: internal (with own staff) or outsourced (by subcontracting). The results show that there are three main situations:

- Organizations that manage security exclusively internally – in about 50% of the cases, companies rely on their own IT staff to ensure security (installing antivirus programs, firewall, security maintenance, etc.), without using external services.
- Organizations that completely outsource cybersecurity services – representing about 37% of respondents, they have contracts with specialized providers who deal with the protection of their infrastructure.
- Organizations that apply a hybrid approach (mix of internal and external specialists) – about 13% of respondents use a combination: they maintain some internal security responsibilities but outsource certain critical services.

Concerning the actual security technologies implemented, the data in Bulgaria shows that **the main measures are:**

- Almost all organizations report using antivirus software on their workstations – around 95% confirmed that all their computers and laptops are protected by up-to-date antivirus solutions. This shows that a minimum level of endpoint protection is ensured in most cases.
- Regarding network firewalls: approx. 53% of organizations have such a solution (in the form of dedicated hardware, software solution or cloud service). A significant share - 47% - indicate that they do not have a firewall at all.

- Data backup: 63% of companies regularly back up important data, locally or in the cloud, thus ensuring that they can restore their data in case of incidents (failures or ransomware attacks).
- Other security solutions mentioned: access control systems (including domain/active directory control in the case of larger companies), email security solutions (e.g. anti-spam filters, secure email gateway), IDS/IPS tools for network intrusion detection and, to a lesser extent, data loss prevention (DLP) or WAF (Web Application Firewall) solutions for protecting public web applications.

However, the uptake of these more advanced security technologies (IDS/IPS, DLP, WAF, etc.) is uneven: large companies implement them, while traditional small and micro-enterprises in the food sector are usually limited to antivirus programs, firewalls and backups. The main reason may be related to the cost and expertise required - many small enterprises consider the minimum set of measures sufficient and do not have the staff or budget for enterprise solutions. This highlights the potential threat exposure of a significant part of the sector: attackers can take advantage of the lack of advanced protection to launch attacks.

On the other hand, outsourcing security to specialized companies provides access to state-of-the-art expertise and technology (24/7 monitoring, threat intelligence, rapid response), but sometimes comes with challenges. Respondents who have chosen to outsource activities cite benefits such as periodic vulnerability audits and consulting, but also acknowledge the associated risks: dependency, possible delays in response due to service level agreements, and long-term costs that can become significant.

Overall, these analyses underline the need for **context-sensitive policies and strategies**: support for SMEs (and especially those in lagging regions) to increase their security capabilities, while also providing advanced approaches for economic hubs where digitalisation brings more sophisticated risks. Without differentiated attention, the cybersecurity gap between different categories of organizations in the food sector can widen.

Organization segmentation and cyber maturity profiles

Based on the characteristics analysed (size, technologies used, level of outsourcing, etc.), we identified three **main segments of organizations** in terms of cybersecurity maturity:

1. **SME segment with basic solutions** includes micro and small enterprises (but also some medium-sized ones) that mainly use basic IT and security solutions. These organizations have relatively simple infrastructures (personal computers, local network, possibly a website) and rely on free antivirus or basic licenses, firewalls built into commercial routers, and occasional backup. They do not have specialized security personnel and, in case of need, delegate IT tasks to the system administrator or a general support company. This segment is the most **vulnerable to common attacks** and has limited visibility into threats.
2. **The segment of medium-sized organizations with a mix of internal and external solutions:** here we find medium-sized companies and a few large companies that have adopted a hybrid approach – they have developed certain capabilities internally (e.g. an IT department with 1-2 people with some expertise in security) but also use external services for critical aspects (audit, monitoring, compliance). These organizations have already implemented standard security measures (AV, firewall, regular backup, password policies) and are trying to keep up with new requirements (e.g., implementing multi-factor

authentication where possible or network segregation for production systems). Their level of maturity is **medium**, awareness of risks is present, but often the capacity for response and prevention is limited by resources. They represent the most dynamic segment, being able to evolve positively if they benefit from guidance and support.

3. **Large, technologically advanced organizations segment** includes large companies (and a few medium-sized companies) that have invested heavily in technology and security. They use advanced solutions (interconnected ERP systems, SCADA for industrial automation, IoT for product traceability), have implemented state-of-the-art security measures (IDS/IPS, SIEM, integrity monitoring tools, incident response teams or service) and usually outsource critical services to top providers (e.g. SOC services, annual penetration testing, compliance consultancy). This segment has a **proactive view** of security, integrating it as part of organizational risk management. However, these companies are not invulnerable either – the high complexity of the infrastructure and the dependence on external partners open up other risk vectors (e.g. attacks on third-party providers, configuration errors in complex systems, etc.).

This **segmentation** is useful to understand the diversity of the food sector in terms of cybersecurity. At the same time, it can guide IT&C solution providers to customize their **offer**: from simple, turnkey packages for segment 1 (which needs easy-to-implement and low-cost solutions) to specialized services for segment 3 (which needs niche expertise and complex integration). Thus, initiatives to improve security in the sector should be calibrated according to the target segment.

From a sectoral point of view, it is worth noting that there are differences in emphasis between industries, even when we talk about cybersecurity. Sectoral profiling suggests that **the industrial and transport sectors** (partially included in the survey) have highly critical cybersecurity needs (due to reliance on industrial control systems and just-in-time logistics), while the **food sector**, although becoming increasingly digitalised, still places a strong emphasis on **core IT maintenance and operational** support, seeing security as a support component rather than a strategic one. This does not mean that food companies ignore security, but that, relative to other sectors, their investments and concerns are still focused on keeping systems running (uptime, IT service) and less on protecting against complex cyber threats. This finding can guide the adaptation of awareness messages: for example, by highlighting the direct link between security and **business continuity** (avoiding stopping production or distribution), it can better capture the attention of decision-makers in the food industry.

The main cyber risks and threats identified

The open-ended questions in the survey, corroborated with discussions and analyses, made it possible to identify a set of **major cyber risks** that concern (or affect) the food sector. Summarizing the answers and performing a *word cloud* analysis of the terms mentioned by the respondents, the following central problems emerge:

Figure 6. Word cloud.

• **Technological vulnerabilities and lack of updates:** Many organizations have cited **vulnerabilities** (of operating systems, applications used or industrial equipment) as a source of risk. In particular, **failure to apply security updates and patches on time** was flagged as a problem – either due to lack of time/staff or fear of disrupting production through updates. Thus, outdated software and older equipment (legacy systems) remain in operation, creating a known attack surface for hackers. This aspect is aggravated by companies that use old SCADA systems or custom software, for which updates are rarely or difficult to apply.

- **Lack of advanced protections:** Many respondents indicated that they do not have advanced protection solutions (such as next-generation firewalls, intrusion detection systems, continuous monitoring mechanisms), explicitly mentioning their absence as a vulnerability. Phrases such as *"we don't have a dedicated firewall, only what the router offers"* or *"we only use free antivirus, nothing advanced"* have been encountered. This **lack of advanced protection** is correlated with budget constraints or the mistaken belief that those companies would not be targets of interest to attackers.
- **Security breaches and data leaks:** The fear of **data breaches** (compromising business information or customers' personal data) is present, even if not all companies have experienced such a thing. In the food sector, breaches may concern data on production recipes/formulas, on contracts with suppliers or customer identification data. A major breach can lead to **financial losses, legal penalties (if it involves personal data, according to GDPR), and loss of trust** from partners and consumers. Although less publicized, there have been incidents of this type – for example, a hypothetical example given by a respondent: *"leaking the details of contracts with suppliers could put us in an unfavourable situation in future negotiations"*. This shows the awareness of the reputational and competitive impact of information security.
- **Phishing and social engineering attacks:** Almost all respondents are aware of **phishing** attacks – fraudulent emails that try to trick employees into disclosing credentials or downloading malware. This type of threat is perceived as very common. The food sector, not necessarily having highly trained IT employees, is vulnerable to **human error**. A common scenario mentioned: attackers posing as suppliers by sending fake invoices or links to phishing pages, with the aim of gaining access to internal systems or fraudulent payments. Employee education about phishing is often insufficient, which means that this risk remains high.
- **Malware and ransomware attacks:** More and more organizations in the sector have heard about or even suffered **ransomware** attacks – in which data is encrypted by attackers, who then demand a reward. The impact of ransomware in the food industry can be particularly serious, as it stops production and distribution (any hour of downtime can lead to the loss of batches of perishable food). One respondent gave the example of a cold storage: *"ransomware*

that would block our systems would mean that we can no longer manage refrigerated stocks, we risk losing the goods" – a scenario also confirmed by real incidents that happened internationally. In general, malware attacks (including classic viruses and Trojans) are seen as a constant threat, against which many companies rely only on standard antivirus, which is not always enough if employees are not vigilant.

- **Risks in the digital supply chain:** Some firms, especially the largest ones, have expressed concerns about **the security of the partners and suppliers** with whom they are digitally integrated. For example, a manufacturer that relies on a software solution provider for inventory management is vulnerable if that provider is compromised. Supply chain attacks are an emerging threat: food companies can be indirectly affected by breaches at logistics, transport or IT partners. An example: if a food carrier's IT systems are attacked, deliveries can be delayed or rerouted, affecting producers. Also, smart industrial equipment (IoT) used in factories can serve as an attack vector if the suppliers of this equipment do not properly secure it.

At a glance, **SMEs seem to be the most exposed** to the above risks, due to limited resources and the use of security solutions only at the basic level. In contrast, large companies, while more attractive targets for sophisticated attacks, usually also have better means of protection and response. The regional differences discussed above are also making their mark: less developed regions report simpler but frequent incidents (viruses, basic phishing), while **diversified and complex** threats (APT attacks, next-generation ransomware) also appear in developed regions.

It is important to note that many companies in the food sector also face **operational risks** that may have cyber causes: for example, an interruption or malfunction of the SCADA air conditioning system in a cold storage facility can be caused by a cyber-attack or an IT failure and has direct consequences (material losses). Thus, cyber risks are intertwined with operational risks in this area. Any **business interruption** (whether caused by an attack or a technical incident) can lead to missed delivery deadlines, financial losses and even food safety regulations (e.g. if the 'cold chain' is compromised).

In conclusion, **the food sector is exposed to a diverse range of cyber risks**, amplified by technology dependence and operational interconnectedness. In the next chapter, we will place these findings in the broader European context, looking at ENISA's perspectives and recommendations on cybersecurity in the food sector, as well as recent regulatory and threat developments.

SECTION 3. ENISA'S PERSPECTIVES AND THE EUROPEAN CONTEXT

To better understand the position of the food sector in the European cybersecurity landscape, we will examine information and conclusions from **ENISA** (European Union Agency for Cybersecurity) sources and other relevant reports. This section discusses incidents at European level, statistics on threats in the agri-food sector, regulatory initiatives (such as NIS2) that explicitly include the food industry, as well as forecasts about the evolution of risks in the future. The aim is to provide a **comparative benchmark** for the situation in Romania and to identify **good practices** or applicable recommendations.

Cyber threats and incidents at international level in the food industry

According to data aggregated by ENISA in recent years, the agri-food sector was not among the first targets of reported cyberattacks, but its importance is growing. ENISA's threat landscape reports highlight that in 2023, **the agri-food sector accounted for around 1% of all cybersecurity incidents reported** at EU level. This percentage may seem small compared to sectors such as finance or health, but it should not be interpreted as a lack of risk – on the contrary, ENISA points out that **the accelerated digitalisation of agriculture and the food industry, combined with low security maturity, could arouse the increased interest of attackers**. In other words, as the sector adopts Industry 4.0 technologies (automation, IoT, cloud data), the attack surface is increasing, and malicious actors could take advantage of **existing security gaps**.

Globally, there have already been a number of **majors cyberattacks on targets in the food and agriculture sector**, which serve as lessons on what can happen and what to watch out for:

- In 2021, a **major meat producer (JBS Foods)** suffered a ransomware attack that severely affected operations in several countries, forcing a temporary halt to production in the US, Canada and Australia. This incident has attracted attention at the government level, being even considered national security issues (protection of the food supply chain).
- The so-called **"cheese hack"** – the attack on the Dutch cheese distributor in April 2021 mentioned above – demonstrated the direct impact on the market of a cyberattack empty shelves in stores, bottlenecks in the logistics chain from producers to retailers. The attack targeted the distributor's ERP system, disrupting communication with stores and inventory records.
- **Agricultural cooperatives and irrigation infrastructures**: Also in 2021, an agricultural cooperative in Iowa (USA) was hit by a cyberattack that disabled its IT networks used to coordinate animal feeding and grain deliveries. And in 2023, one notable incident targeted Israel's automated irrigation system, causing crop losses and a shift to manual watering. Such attacks show that **not only food processors are targeted, but also modern farms and smart farming systems**.
- **Demonstration attacks on agricultural equipment:** A novel case was the compromise of John Deere tractors in 2022, when hackers managed to install a video game (DOOM) on tractor displays, as a protest against the poor security of these connected equipment. Although it did not cause direct damage, the incident highlighted vulnerabilities in the area of agricultural equipment and the concept of **smart farming**.

These examples highlight the diversity of attack vectors: from classic profit-oriented ransomware to **sabotage of physical processes** (watering, air conditioning, food processing) to **agricultural IoT**

exploitation. For the food sector in Romania, the lessons are that **the threat is real and growing**, and the effects can be major (financial losses, market disruptions, food safety issues).

ENISA, together with other authorities (such as CISA in the US), recommends monitoring the evolution of these threats and continuously adapting food security strategies, precisely to **mitigate risks proactively. Although large-scale incidents are still relatively rare in this sector, the underlying trend is an increase in the level of attacks**, both in frequency and sophistication.

A number of specific factors also highlighted by ENISA and INCIBE (*Spanish National Institute of Cyber Security*) experts in an analysis dedicated to the agri-food industry contribute to the vulnerability of this sector:

- **Extensive integration into the supply chain** makes an attack on a link have a domino effect. For example, a manufacturer depends on transport logistics and packaging suppliers – attacks against them affect it indirectly, but severely. This high interconnectedness makes them an attractive target for attackers who want maximum impact.
- **Low maturity in cybersecurity**: the food sector is traditionally oriented towards productivity, low costs and volume, which has led to the neglect of cybersecurity. The lack of security procedures and policies at many companies makes them more susceptible to attacks. Also, many companies are **SMEs or micro-enterprises** without dedicated security staff, so vulnerabilities can remain unaddressed for longer.
- **Adoption of new technologies without adequate security**: The deployment of IoT, smart sensors and automation in agriculture and food production has often exceeded protective measures. Communications between devices can be unsecured, default configurations – vulnerable, services exposed online – unprotected and unprotected. In short, the sector is still in a phase where **technology is being introduced before security is fully understood and integrated**.
- **Dependence on outdated equipment and software**: many food factories use decades-old machinery, partially modernized with IT systems. These **legacy technologies** are difficult to secure – they do not support updates, communicate through legacy protocols, and can be easily compromised. On the other hand, modern smart equipment, if not configured correctly, can provide attackers with entry points into the industrial network.

In the face of these realities, **ENISA recommends a set of safeguards tailored to the food sector** to counter both current and emerging threats. We will detail these recommendations in the Recommendations subchapter, but we mention here that the priorities highlighted include: **staff training** (employees being the weak link in many attacks, such as phishing), **multi-factor authentication** where possible (especially when accessing sensitive data), **regular backups** (to mitigate the ransomware effect), **clear security policies and procedures** (so that employees know how to act and prevent incidents), as well as **updating and securing industrial equipment** (hardening, closing unused ports, segmenting OT networks).

European regulatory framework (NIS2) and the importance of the food sector

From a legislative and policy point of view, at the European Union level there has been until recently a certain gap in the coverage of the food sector in cybersecurity legislation. The first NIS Directive (Network and Information Security Directive, adopted in 2016) focused on a limited set of sectors considered essential (energy, transport, finance, health, drinking water, etc.), explicitly not including the food industry in the list of essential services. However, some Member States have extended the list at national level: for example, **some EU countries have designated food industry operators as ESOs (Essential Services Operators)** under the NIS1 umbrella, recognising that the security of the food chain is critical. However, at European level there was no uniform obligation for the food sector.

Things have changed with the updating of the legislation. The **NIS2 Directive**, adopted at the end of 2022 and to be transposed by Member States (deadline October 2024), considerably extends the scope. NIS2 **explicitly includes the food industry as a sector with important entities** from a cybersecurity perspective. Specifically, the directive adds **food producers, processors and distributors** to the list of regulated sectors, classifying them as "important entities" that will have to implement security measures and report incidents. Furthermore, NIS2 removes the old criterion based on national importance and replaces it with a size criterion: **all medium and large entities in the food supply chain will be covered by the new directive (micro and small enterprises being exempted by default, unless a Member State specifically declares them critical).**

This is a major development: basically, large food processors, food retail chains, large food distribution companies in the EU will have strict legal security obligations (risk assessments, technical and organizational measures, notification of significant incidents, etc.). The NIS2 Directive thus recognises that **access to food is essential for society**, similar to access to safe drinking water, and that the food chain is sufficiently dependent on network and information systems that a cyber disruption could have serious effects.

For Romania and Bulgaria, the transposition of NIS2 will probably mean the identification and inclusion of large players in the food industry on the list of essential/important entities supervised by the competent cybersecurity authorities. This should lead to an **overall improvement in the level of security**, as the companies concerned will have to align with minimum requirements (which will be detailed through standards and implementing acts of the directive).

In addition to NIS2, there are other related regulations that, although not specific to the food industry, have an impact on safety in this sector:

- **General Data Protection Regulation (GDPR)** – imposes personal data security requirements. Any food company that processes personal data (e.g. data about employees, customers, partners) must implement appropriate technical and organizational measures for the protection of such data. The GDPR does not cover the security of industrial equipment if it does not handle personal data, but the *"security by design"* principle promoted by the GDPR still encourages manufacturers of IT equipment (including those used in agriculture/food industry) to integrate security into the product, which also helps end users.
- **EU product safety legislation** – for example, the Radio Equipment Directive and delegated regulations emphasise the obligation of manufacturers to ensure that internet-connected equipment does not compromise the network and its operation is safe. This also concerns IoT equipment used in agriculture (sensors, smart cameras, agricultural drones) – their manufacturers must take cybersecurity measures, which, if respected, will increase the resilience of the food chain as a whole. However, there are still gaps – for example, the Machinery Directive that regulates industrial machinery covers more the physical safety of the machine, not necessarily the security of the network in which it is integrated. There is discussion of revising these legislations to explicitly include cybersecurity requirements.
- **Certification and standardisation initiatives** – ENISA is working on cybersecurity certification schemes for various products and services. In the future, we may see certifications for agricultural IoT devices or for software used in critical infrastructures, which would provide a level of assurance. Also, international standards such as ISO/IEC 27001 (information security management) or food industry practices (e.g. food safety standards that could incorporate IT elements) will play a role.

All in all, **the cybersecurity of the food sector is receiving increasing attention in the EU's legislative and policy framework**, moving from the '*neglected' to 'regulated and monitored'* stage. Our food companies should actively prepare for compliance with the new requirements (NIS2), which involves conducting risk assessments, adopting a set of security policies, preparing incident response

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the European Cybersecurity Competence Centre can be held responsible for them.

procedures and, last but not least, **raising** awareness among management about the importance of this topic.

Looking Ahead: Emerging Trends and Threats

ENISA, in its *foresight* exercise, tried to anticipate how cyber threats could evolve by 2030. One of the scenarios identified as having a medium-high probability and a significant impact is directly related to the food sector: **cyberattacks aimed at disrupting the food production chain**. The ENISA *Foresight 2030* report describes the possibility of threats such as **malware insertion into food production systems** or denial-of-service attacks on critical processing infrastructures, with the aim of stopping operations or even sabotaging food safety. For example, it has been speculated that attackers could target automated packaging or ingredient mixing lines, causing malfunctions that lead to **factory closures or unauthorized changes in food composition**. The consequences of such actions could be dramatic: from **food shortages** and economic disruptions to the risk of **intentional contamination of food** (if recipes or dosages are maliciously altered). ENISA warns that, against the backdrop of increasing automation and robotisation of food production, these scenarios are becoming increasingly plausible, and serious safeguards are needed to prevent them.

An example of future risk from the ENISA analysis is the one called *"Malware insertion to disrupt food production supply chain",* where it is pointed out that attackers with medium to high resources could **manipulate industrial food systems** in ways that have a physical impact. For example, a DoS attack on packaging systems can stop the shipment of products, and compromising production equipment can lead to the complete shutdown of the operations of some food processing facilities. In the worst case, such attacks can cause **food sabotage** – for example, changing the settings of some machines could contaminate products (imagine an extreme scenario: changing temperatures in a pasteurization or sterilization process, making products unsafe). Although these situations have not yet been reported, preparedness for them is being discussed in cyber resilience plans.

In addition, **the convergence between physical food security and cybersecurity** will become increasingly pronounced. In addition to direct attacks, there can also be **digital disinformation campaigns** targeting the food industry (for example, spreading fake news about the contamination of a product, by hacking a company's communication channels), which is another facet of risk in an increasingly interconnected world.

In order to counter emerging threats, there is intense discussion at European level about the need for **public-private partnerships** and more efficient information exchange in sectors that have so far been less addressed, such as agri-food. Initiatives such as **ISACs** (Information Sharing and Analysis Centres) specializing in food or agriculture can help companies stay up to date with recent tactics and indicators of compromise. Already in the US, the Food and Ag-ISAC has been formed, which issues threat reports for the food industry and agriculture, a model that could also be replicated at European level.

Another aspect of the future is the growing role of **artificial intelligence** – both as a tool for defence and as an attack vector. On the one hand, AI systems can help detect anomalies in food industrial processes (signalling possible cyberattacks or malfunctions), but on the other hand, attackers could use AI to more effectively identify vulnerabilities or launch automated attacks at scale.

In conclusion, the **European perspective highlights both progress – stricter regulations and growing awareness – and the challenges of the future – increasingly sophisticated threats to the food chain**. The food sector is starting to be treated as a critical sector that needs to be protected, and companies in the field will have to evolve from a reactive (or even passive) approach to a proactive one in managing cyber risks.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the European Cybersecurity Competence Centre can be held responsible for them.

Conclusions

The food sector is at an inflection point in terms of cybersecurity. On the one hand, **accelerated digitalization** brings considerable economic and operational benefits – production automation, efficient supply chain management, quality monitoring and food traceability – but on the other hand, it **exposes the industry to unprecedented cyber threats**. The results of our studies indicate that in Romania and in Bulgaria food companies are increasingly aware of these risks, but the level of preparedness and protection varies greatly depending on size and resources. Food SMEs remain vulnerable to common attacks (malware, phishing) due to limited resources and the use of only basic security measures, while large companies implement more advanced solutions but also become targets for more complex attacks.

We have identified **the main cyber risks**: from the lack of updates and advanced protections, to direct (phishing, ransomware) and indirect (on the supply chain) attacks. The fact that many the organizations analysed do not have dedicated security services shows that there is still a long way to go in this industry to achieve a satisfactory level of cyber maturity. At the same time, international examples show us that the stakes are very high – a successful attack can stop production, cause losses of millions and even endanger public safety. Fortunately, we did not find any major incidents among the companies analysed, but the absence of incidents should not lead to complacency, but to **proactivity**.

At European level, **the food sector has officially entered the focus of security regulations** (through NIS2) and threat analysis (ENISA highlighting risks specific to agri-food). This means that companies in Romania and in Bulgaria will also be pushed by the context to raise their security standards, which is a positive thing. Implementing robust cybersecurity strategies in the food sector is not only important for individual companies but becomes a matter of **national security and societal resilience**: continuous access to food, prevention of possible food crises caused by cyber disruptions, protection of consumers from possible dangers.

The present study provides an integrated look at the current situation and the direction of evolution. In conclusion, **the cyber protection of the food chain requires a combined approach**: investments in technology (advanced protections, modern IT infrastructure), **employee education and awareness**, strengthening security throughout the supply chain (including partners) and cooperation between companies and authorities. Only through such a holistic approach can the food sector ensure its **operational continuity and prevent emerging threats**, while maintaining public confidence in food safety.

The food sector of the future will be a high-tech, interconnected and efficient one, but for it to be safe, **cybersecurity must be organically integrated into all processes**. Organizations in this field are encouraged to treat security not as a compliance burden, but as a **key factor in business quality and sustainability**. Finally, robust cybersecurity means food products delivered on time, without incidents that compromise safety or quality – which is exactly the essential promise that this sector has to fulfil to society.

External correlations

Recent data and reports from ENISA (European Union Agency for Cybersecurity) confirm and complement many of the observations drawn from the national study conducted in Romania and Bulgaria. The following graphs illustrate how European trends directly reflect on the situation in the food sector:

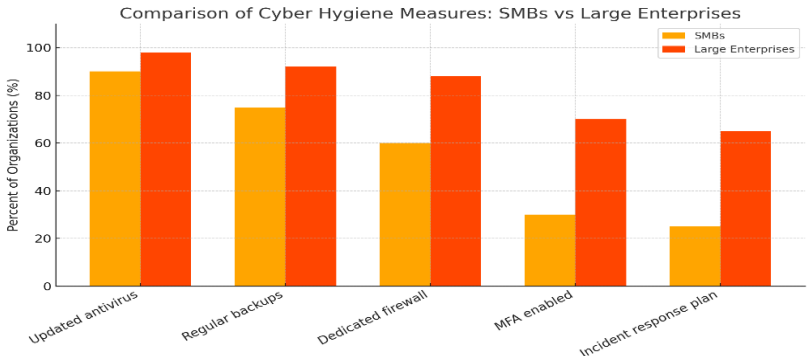

Figure 8. Comparison of Cyber Hygiene Measures – SMEs vs Large Enterprises.

SMBs mainly apply basic measures (antivirus, backup), but they lag far behind large companies in terms of multi-factor authentication (MFA) and incident response plans. ENISA highlights the same problem: the lack of basic cyber hygiene in SMEs is one of the biggest structural vulnerabilities in the EU.

The discrepancy between self-reported incidents and the estimated reality shows that SMEs, in particular, **do not detect or recognise many of the incidents suffered**. ENISA warns that this behaviour leads to repeated exposure to the same vulnerabilities.

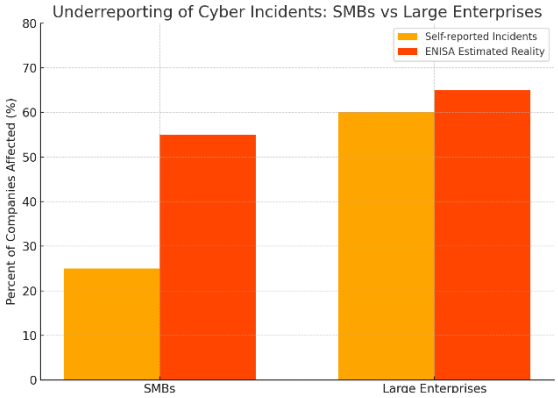

Figure 7. Underreporting of cyber incidents.

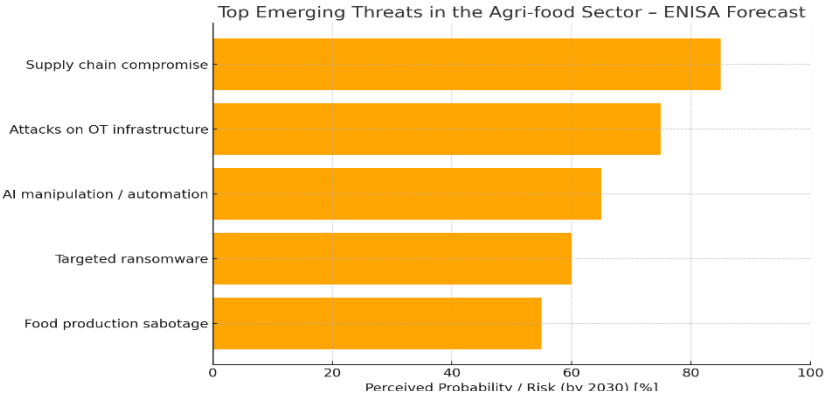

Figure 9. Top emerging threats by 2030 (according to ENISA).

According to the *ENISA Threat Landscape & Foresight 2030* report, the most likely and impactful threats for the coming years include: supply chain compromise, attacks on OT equipment in the industry, specialized ransomware, and the use of AI for attacks. **All these risks are already signalled or anticipated in the Romanian and Bulgaria food sector**, according to our study.

SECTION 4. RECOMMENDATIONS

In light of the findings, we make a number of recommendations to improve cybersecurity in the food sector. These recommendations are aimed at both companies in the industry (from SMEs to corporations) as well as decision-makers and technology partners:

1. Increasing staff awareness and training: Given that human error is a major attack vector (e.g. phishing, malicious attachments), companies should invest in **regular training programs** for employees. Awareness sessions on phishing emails, safe password usage practices, and USB device handling can dramatically reduce the risk of incidents caused by inattention. Organizational culture must promote **cyber vigilance** at all levels, from factory operators to management.

2. Implementation of essential technical measures (cyber hygiene): Every organization, regardless of size, should ensure that it has at least **basic cyber hygiene** measures in place: updated antivirus solutions on all stations, **network firewall** (including correct configuration of routers), **periodic** backup mechanisms offline for critical data, and timely updating of all software systems. These measures, although they seem basic, constitute the first line of defence and can prevent most unstructured attacks.

3. Adoption of multi-factor authentication (MFA): Wherever possible (email access, VPN, privileged accounts, cloud platforms), enable **two-factor authentication**. MFA adds an extra layer of security that can stop attacks even if passwords have been compromised. With credential phishing rampant, MFA is becoming a minimal necessity for protecting accounts.

4. Updating and maintaining industrial systems: For companies with automated production equipment, it is recommended **to audit the security of the OT (Operational Technology) infrastructure**. This includes identifying all connected devices (inventory), applying security patches where vendors offer them, **network segmentation** (separating production and office networks), shutting down unused services and ports, and changing default device credentials. Old equipment that cannot be upgraded should be isolated in the network and closely monitored.

5. Development of internal security policies and procedures: Companies should develop **clear cybersecurity policies** – simple documents that establish the ground rules (use of devices, access to data, password policies, incident reporting protocol, etc.). These policies provide employees with **guidance on safe behaviour** and reduce chaos in the event of an incident. In addition, procedures such as incident response plans and business continuity plans should be prepared and tested through periodic simulations so that the organization reacts effectively if an attack occurs.

6. Combination of internal and external solutions (hybrid model): SMEs that do not have sufficient internal capacity should consider **outsourcing security services** to specialised providers (e.g. 24/7 infrastructure monitoring, firewall administration, incident response services). An external partner can bring expertise that the company does not have in-house. However, even in this case, companies should keep a **minimum of control and knowledge** in-house – for example, an internal security officer (even if part-time) who liaises with the supplier and ensures that the company's policies are followed. This avoids total dependence on third parties and maintains long-term resilience.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the European Cybersecurity Competence Centre can be held responsible for them.

7. Supply chain collaboration: Large companies should require their partners and suppliers to hold minimum **security standards** – for example, contractual clauses on data protection and incident notification. At the same time, they can initiate collaborations (such as **consortia or sector alliances**) to exchange threat intelligence and implement joint solutions, especially at local or regional level. For example, companies in an industrial park or industry association can share the cost of security courses or build a local monitoring centre together.

8. Compliance with legal requirements and standards of good practice: As the NIS2 Directive will impose obligations, the companies concerned must prepare for **compliance audits**. Even those that are not legally obliged (e.g. SMEs below the threshold) should be inspired by the requirements of NIS2 as a **security standard**. It is also recommended to align with recognized standards (e.g. ISO 27001) to structure the information security management system. Also, participating in initiatives such as the national cybersecurity programme (if any) or accessing available funds for secure digitalisation (e.g. European funds for SMEs in the field of cybersecurity) can accelerate improvements.

9. Monitoring the evolution of threats and updating strategies: Security is an ongoing process. Companies should keep track of threat reports (including sectoral ones, such as Food-ISAC reports or CERT-RO bulletins) and regularly update their risk assessment. As new risks emerge (e.g. threats to recently introduced technologies such as AI or autonomous internal transport vehicles), strategies must be adapted. The idea is to move from a reactive approach to a **proactive and anticipatory** one. Investing in **early detection capabilities** (log monitoring, alerting systems) can make all the difference in stopping an attack before it causes major damage.

10. Improved resilience and continuity plans: Given that not all attacks can be 100% preventable, it is essential for businesses to have backup plans in place to continue their work in the event of a serious cyber incident. For example, maintaining manual emergency procedures (workarounds) for temporary operation without IT, establishing **clear recovery grounds** (RTO/RPO) for critical systems, as well as ensuring that backups are tested and can be restored quickly. Good **cyber resilience** ensures that even if an attack is partially successful, the company will quickly return to normal functionality and minimize losses.

Putting these recommendations into practice will require effort and, in many cases, a change in mindset among food company management, who need to see **cybersecurity as a strategic investment, not just a cost or compliance requirement**. In the long run, the benefits – preventing costly incidents, protecting reputation, ensuring business continuity and regulatory compliance – far outweigh the initial investments. In the context in which cyber threats will not disappear, but on the contrary, will intensify, **only proactive and prepared organizations will be able to thrive without** interruptions.

Taking a proactive stance towards cybersecurity in the food sector will contribute not only to the safety of those companies, but also to the **food safety of the population** and overall trust in the food supply chain. Therefore, all stakeholders – industry, authorities, security experts – must work together to strengthen this crucial area of the economy. In the digital age, **cybersecurity has become synonymous with quality and safety** in the food sector.

Bibliography

- Burcu Yasar – *"Securing European Cyberspace: Is the Food and Agriculture Sector Critical?"*, CiTiP Blog KU Leuven, 10 May 2022. [Online]. Disponible la: <https://www.law.kuleuven.be/citip/blog/securing-european-cyberspace-is-the-food-and-agriculture-sector-critical/#:~:text=Security%20rules%20also%20emanate%20from,or%20animals%20would%20presumably%20increase>.
- INCIBE-CERT (Spania) – *"Cybersecurity in the agri-food industry",* 2023. [Online]. Available: <https://www.incibe.es/en/incibe-cert/blog/cybersecurity-agri-food-industry>.
- ENISA – *"Foresight Cybersecurity Threats for 2030"* (report 2024). <https://www.enisa.europa.eu/publications/foresight-cybersecurity-threats-for-2030-update-2024-extended-report>.
- Industrial Cyber (2023). *"Farm and Food Cybersecurity Act…"*. <https://industrialcyber.co/reports/food-and-ag-isac-cyber-threat-report-provides-actionable-intelligence-on-cyber-threats-ransomware-tactics/#:~:text=Food%20and%20Ag,on%20cyber%20threats%2C%20ransomware%20tactics>.
- Reports and conclusions extracted from the internal analysis on an anonymized document of the survey data conducted among organizations in the food sector in Romania: company profile, degree of digitalization, main perceived risks, differences by region and size, level of security outsourcing, etc.
- ENISA (2024). *State of Cybersecurity in the Union – Condensed Report*. <https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union>.
- ENISA (2023). *Cybersecurity Threat Landscape 2023*. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023>.

TITLE 2. SUPPLY CHAIN CYBERSECURITY RISK MANAGEMENT HANDBOOK

Abstract

This part analyses the cyber risks associated with the food supply chain in Romania and Bulgaria, in the context of the implementation of the NIS2 Directive. In this regard, major threats are identified, such as ransomware attacks, vulnerabilities in IT/OT systems and the exposure of small and medium-sized enterprises to the accelerated process of digitalization. The manual proposes a cyber risk management framework, aligned with international standards (ISO/IEC 27005, NIST RMF), and recommends technical and organizational measures, such as network segmentation, the use of EDR solutions, multi-factor authentication (MFA) and business continuity plans. The national legislative frameworks are also analysed – GEO no. 155/2024 in Romania and the amendments to the Law on Cybersecurity in Bulgaria –, with a focus on incident reporting obligations and managerial responsibility. The manual emphasizes the importance of an integrated approach to cybersecurity, focused on compliance, regional cooperation, and operational resilience in the agri-food sector.

SECTION 1. INTRODUCTION

Cybersecurity risk management is part of the cybersecurity area of governance and is of fundamental importance for how cybersecurity risks are managed at all levels, including cybersecurity risks related to the digital supply chain. Cybersecurity risk management must be an integral part of the set of activities associated with an economic entity and includes interaction with the parties, including the component entities of the digital supply chain (hardware & software).

The food supply chain is the physical infrastructure through which food is produced, processed, distributed, and delivered to consumers. The accelerated digitalization of the food sector in the last decade – from automated systems in the production area to IT platforms for logistics, promotion and advertising – has brought efficiency, substantial increases in production and sales, but also increased exposure to cybersecurity risks.

In recent years, significant cybersecurity incidents have highlighted sector-specific vulnerabilities, vulnerabilities that have been exploited and led to the materialization of the risks associated with these vulnerabilities, thus, in 2021 a ransomware attack paralyzed a food distributor in the Netherlands, blocking communication with warehouses and transport and leaving the shelves of a large supermarket without products (known as the "cheese attack").

Shortly after, the world's largest meat producer was forced to halt its operations in the US, Canada, and Australia due to another ransomware. Also, leading companies in the food industry – such as Campbell Soup, Dole Foods, Heineken or Krispy Kreme – have fallen victim to recent cyberattacks. These examples clearly demonstrate that the agri-food sector can no longer treat cybersecurity as a secondary issue, as the consequences can be severe: considerable financial losses, partial or total interruption of activity, impairment of food safety and even animal welfare.

The strategic importance for society of the food supply chain is comparable to that of other essential sectors (such as energy or drinking water). Access to safe and continuously available food is vital for the well-being of the population and the smooth running of the economy. However, until recently, European cybersecurity policies have not explicitly covered this sector. The NIS Directive (2016) did not include food as an EU-wide essential service, although several Member States have voluntarily registered certain entities operating in the food business as essential service operators (ESOs). This administrative loophole has been remedied by the new NIS2 Directive, which extends the scope to the food sector (food producers, processors and distributors), recognizing it as an 'important sector' with important entities requiring increased cyber protection.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the European Cybersecurity Competence Centre can be held responsible for them.

This handbook addresses cyber risk management in the digital supply chain in the food sector, with a focus on the concrete situation in Romania and Bulgaria in the context of initiating the implementation process of the NIS2 Directive. This paper is addressed both to professionals (IT managers, NIS compliance managers, cybersecurity consultants) and to the academic environment (students, master's students in cybersecurity and industrial IT). In the following pages, a solid theoretical framework is presented along with guides and practical tools.

The content of the handbook is structured on thematic chapters, covering from legislative and regulatory aspects to risk management processes, the particularities of cybersecurity in the digital supply chain, business continuity planning, cybersecurity incident management and international cooperation, as well as good practices and model policies/procedures. Each chapter expands and deepens the initial sections, integrating both European perspectives (ENISA, European Commission, ISO standards, BSI/ANSSI/CERT recommendations, etc.) and concrete examples from Romania and Bulgaria, including useful tools (risk matrix, checklist for evaluating providers and services provided by them, policy templates, cybersecurity incident notification forms, continuity plans).

The purpose of the introduction is to outline the context and necessity of such a manual. The increasing complexity and sophistication of cyberattacks and the increasingly close interconnection of supply chains mean that no one is out of the woods. "No one owns the entire risk. If you have valuable data or systems, attackers will always look for the weakest link, often a partner placed in the supply chain," the experts point out. Therefore, organizations in the food industry must adopt an integrated vision of cybersecurity, which includes both internal protection and collaboration with suppliers and distributors. The manual provides guidance in this regard, aligned with the requirements of the NIS2 Directive – the new European standard that requires a systematic approach to cyber risks. Next, we will present the relevant legal framework, before moving on to the concepts of risk management and measures specific to the food sector.

SECTION 2. LEGAL FRAMEWORK

European legislative framework – NIS2 Directive

In order to strengthen the cyber resilience of critical infrastructures at European Union level, **Directive (EU) 2022/2555 (NIS2)** on measures for a high common level of cybersecurity in the Union was adopted in December 2022. The NIS2 Directive replaces and updates the first significant NIS Directive scope, imposing increased security requirements and tougher penalties for non-compliance. One of the key purposes of the NIS2 Directive is precisely **to address the risks related to digital supply chains**, a lesson learned from the wave of attacks on third-party providers and services that have taken place in recent years.

The NIS2 Directive classifies entities into two broad categories of operators: **essential entities** (in very critical sectors) and **important entities** (in critical sectors). The food sector – defined as *the production, processing and distribution of food* – is included in the category of critical sectors, with entities in this field of activity being considered important entities. This means that all medium and large economic entities (over 50 employees or turnover over €10 million) in the food supply chain automatically fall under NIS2. (Unlike NIS1, where states identified ESOs based on criteria, NIS2 introduces the so-called "size-cap" rule – inclusion by size and sector, ensuring uniform coverage of a much larger number of operators.)

The obligations imposed by NIS2 on essential and important entities are substantial. The Directive provides for a minimum set of **security risk management** measures that each entity must apply, according to the principle of "**all-hazards**" (targeting any type of risk, not just cyber-specific). These include carrying out regular risk analyses and adopting policies for the security of information systems; measures for **the security of the digital supply chain** and supplier relations; vulnerability management and updating programs; use of security tests (audit, pentesting) and appropriate cryptography; plans to respond to cybersecurity incidents and ensure operational continuity. The Directive also introduces **the responsibility of the management of economic entities** – the management of the entity is responsible for complying with cybersecurity measures and can be personally sanctioned in case of gross negligence. For uniform treatment, NIS2 requires Member States to establish *harmonized penalties*: the maximum level of fines cannot be less than **€10 million or 2% of overall turnover** (applies to core entities) or **€7 million or 1.4% of turnover** (for large entities), whichever is greater. These sanctions aligned with those of the GDPR illustrate the importance given to cybersecurity at a strategic level.

A central aspect of NIS2 is **the reporting of cybersecurity incidents**. The Directive establishes a two-stage mechanism for the notification of significant incidents: initially, the transmission of an **early warning within 24 hours** of the occurrence of the incident (with preliminary information on potential malicious causes and cross-border impacts); then, a **detailed notification within 72 hours**, with an initial assessment of severity and impact, including known indicators of compromise. In addition, within one month of the incident, the entity must submit a **final report** with the results of the investigation and remedial measures. The purpose of this step-by-step reporting regime is to enable CSIRT authorities and networks to react promptly and provide support, while ensuring a subsequent in-depth analysis of the incident. It is worth mentioning that the NIS2 Directive distinguishes between essential and important entities also in terms of supervision: critical entities are subject to a **proactive supervision regime** (periodic checks by the authorities), while important entities will be supervised mainly **reactively, post-incident**. However, both categories are required to comply with the same security requirements and may receive similar penalties if serious non-compliance is found.

Also at the European level, the NIS2 Directive strengthens the cooperation mechanisms **between states**. It mandates the existence of an *NIS Cooperation Group* (for the exchange of policies and good practices) and the *CSIRTs Network* (for operational coordination between national incident response teams). NIS2 also formalizes *EU-CyCLONe* – the European cyber crisis management network – meant to ensure coordination in major incidents or crises with an impact on several states. These aspects of cross-border cooperation will be detailed in the dedicated chapter, but it is worth mentioning that the directive also provides for the possibility of carrying out **coordinated risk assessments on critical supply chains** at EU level. An example would be the risk assessments carried out at European level for 5G infrastructure – a model that can be extended to other critical technologies for different sectors.

Implementation of NIS2 in Romania – GEO 155/2024

In Romania, the initial NIS legal framework was established by Law no. 362/2018, which transposed the 2016 NIS directive. The emergence of NIS2 required the updating of national legislation, materialized by **Emergency Ordinance no. 155/2024**, adopted on December 30, 2024. GEO 155/2024 repeals Law 362/2018 (except for some transitional provisions) and establishes a new framework for the security of networks and information systems in civil national cyberspace, aligned with the extended requirements of NIS2. This normative act marks a defining moment in Romania's efforts to strengthen its resilience to increasingly complex cyber threats.

The new legislative framework clarifies aspects that had remained unclear under the old law and introduces additional elements to the European directive. In particular, **the scope has been considerably broadened**: GEO 155/2024 takes the extensive list of critical/very critical sectors from NIS2 (listed in Annexes 1 and 2 of the ordinance) and applies *the size rule*, which means that **thousands of Romanian companies** now become obliged to comply with the new requirements. If under the old NIS only a few dozen essential service operators (ESOs) were identified, now practically any medium or large organization in sectors such as energy, transport, finance, health, water, waste, digital, etc., but also **in the food industry**, falls under GEO 155/2024. Thus, the food supply chain – from agri-food producers and processors to storage and wholesale distribution – is formally recognized as a critical sector, the entities in this field being classified as important entities that must implement security measures and report incidents according to the law.

The ordinance establishes clear deadlines and mechanisms for implementation. For example, the companies concerned must **register** with the competent authority (DNSC – National Directorate of Cyber Security, which acts as a Single Point of Contact NIS and national authority) within a certain interval, and the DNSC will manage the record of essential/important entities and incidents. At the time of the adoption of the ordinance, the registration process was not yet operational, requiring the development of platforms and procedures – the authority announced that it will issue secondary orders and methodologies in the first part of 2025 to clarify practical aspects. Until then, the provisions of the ordinance apply, and operators must start compliance procedures.

The security and reporting obligations provided for by GEO 155/2024 are in line with NIS2: carrying out periodic risk analyses, adopting internal security policies, technical and organizational protection measures proportionate to the risks, continuity and incident management, notifying significant incidents within a given period, cooperating with the authorities and CSIRT teams, etc. The **certification of IT security auditors is also provided for**, which will assess the compliance of companies (a process that is being updated compared to the regime of Law 362/2018). A notable element is that the ordinance introduces *some additional measures compared to the European framework*, in order to adapt to the local context. For example, the responsibilities of public institutions and internal notification procedures are clarified, and the DNSC is empowered to issue specific regulations (guidelines, regulations) for different sectors, where necessary. Contravention fines for violations reflect the levels imposed by NIS2 (up to 2% of global turnover), underlining that

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the European Cybersecurity Competence Centre can be held responsible for them.

cybersecurity is becoming a legal obligation as important as the protection of personal data or food safety.

In conclusion, through GEO 155/2024, Romania has aligned its legislation with the NIS2 Directive, extending cyber protection to the food chain. In 2025, the authorities (DNSC) will issue the implementing rules and actively start monitoring compliance. Entities in the food industry must treat these requirements seriously, investing in security and risk systems, otherwise they risk severe sanctions and, worse, incidents with an impact on the population.

Implementation of NIS2 in Bulgaria – Cybersecurity Act (update)

Bulgaria adopted a Cybersecurity Law in 2018 that transposed the original NIS directive, establishing a framework for identifying operators of essential services and regulating security measures. The existing Bulgarian law provides for a governance structure with a Cybersecurity Council, a National Coordinator and Incident Response Teams (CERT Bulgaria at national level, plus sectoral CSIRTs in energy, finance, transport, etc. Sectoral regulatory authorities also have the role of designating essential operators and overseeing compliance with requirements in those areas. Until the implementation of NIS2, key sectors in Bulgaria included energy, transport, banking, health, water, digital infrastructure, etc., and the list of OES entities was narrower.

In anticipation of NIS2, the Bulgarian authorities have prepared a **draft amendment to the Cybersecurity Act**, sometimes referred to as the "*Cybersecurity Act*". This bill was submitted to Parliament in July 2024, with the aim of transposing the new NIS2 requirements into national law. By the European deadline (October 17, 2024), Bulgaria had not completed the adoption of the amendments, so at that date the transposition was still unfinished, and the draft was under parliamentary debate, which led to the proposal of **substantial amendments to** the original text. The legislative process continuing towards the end of 2024 and the middle of 2025, as amended law is expected to be passed in 2025, bringing the country into line with NIS2 standards.

The changes envisaged in the new Bulgarian law include the extension of the scope to more sectors and categories of companies. Basically, it will move from the narrow OES list to the inclusion of all medium and large entities in the critical and very critical sectors defined by NIS2. Thus, in Bulgaria as well, the food industry (producers, processors, food distributors) will officially come under the legislation, as a *critical sector* with important entities that must implement security measures and notify significant incidents. The new rules will impose **increased risk management and incident reporting obligations on the entities concerned**, similar to the GEO 155/2024 discussed above. In addition, the management of the companies will be held accountable for non-compliance, and the financial penalties will be increased up to the thresholds harmonized by NIS2 (millions of euros or percentages of turnover).

Until the entry into force of the NIS2 amendments, Bulgaria continues to apply the provisions of the existing law (NIS1). Even under the old law, some requirements were very strict. For example, **the obligation to report incidents** in Bulgaria requires essential operators to notify the CSIRT national team **within 2 hours** of becoming aware of a serious incident, followed by a full report within 5 working days. This 2-hour deadline for initial notification is much more demanding than the NIS2 standard (24 hours) and was set precisely to ensure an immediate reaction at national level. Bulgarian law also requires entities to **fully cooperate with authorities and response teams** in the event of an incident, including by providing the necessary information and, if the incident may constitute a crime, coordinating with law enforcement bodies (e.g. the cybercrime unit).Ensuring **continuity of services**: companies must take measures to maintain the continuity of essential or digital services in the event of cyber disruptions, through contingency plans, redundancies and other means of resilience. Failure to comply with the obligations entails sanctions: Bulgarian law provides for administrative fines which, although in the old form they were lower (orders of thousands of euros), will increase under the NIS2 regime. Civil or even criminal liability can also be incurred for serious incidents caused by

negligence (the Bulgarian criminal code provides for up to 8 years in prison for computer crimes that affect national security).

In conclusion, Bulgaria is in the process of legislative update to implement the NIS2 Directive, a process that involves the extension of cybersecurity obligations to the food chain as well. Until the new law is finalized, Bulgarian companies in the sector should anticipate the requirements that will come – practically similar to those in Romania and the rest of the EU – and start strengthening their security practices. The Bulgarian authorities, led by the Ministry of e-Governance (NIS national coordinator) and CERT Bulgaria, will step up their surveillance and support efforts, ensuring the transition to the new framework. By harmonizing legislation, Romania and Bulgaria will be able to cooperate more effectively in securing the cross-border food supply chain, as we will discuss in the following chapters.

SECTION 3. RISK MANAGEMENT

Risk management is the foundation of any effective cybersecurity strategy. Essentially, it is a systematic process by which an organization **identifies, assesses and treats risks** that could compromise the achievement of its objectives, in this case the continuity and integrity of the food supply chain. International standards, such as **ISO 31000:2018**, provide reference frameworks for risk management in general, also applicable to the industrial cybersecurity context. Also, specific standards such as **ISO/IEC 27005** (information security risk management) or methodologies such as **EBIOS** (developed by ANSSI in France) or **NIST SP 800-30** (USA) detail the steps and techniques for risk assessment in the IT/OT field. The NIS2 Directive requires essential and important entities to implement **risk analysis and security policies for information systems** that are regularly updated, which basically translates into the existence of a formal risk management process at the level of the organization.

Risk management process

Effective risk management is an essential process in any organization, including the food industry, where threats can affect both food safety and business continuity. The risk management process is a systematic approach by which organizations identify potential hazards, assess their impact and likelihood, implement control measures and continuously monitor the effectiveness of these measures. This process is cyclical and iterative, constantly adapting to changes in the organizational environment and the emergence of new threats.

The classic elements of risk management include:

- **Identification of risks**

The first step is to recognize all the potential risks that could affect the achievement of the organization's goals. At this stage, a list (risk register) is created that includes the identified risks, from human error or technological failures to cyber-attacks or natural disasters.

- **Risk analysis**

After identification, each risk is analysed to understand its causes, the affected assets, as well as how it could manifest itself. The analysis involves determining exploitable vulnerabilities and the factors that could trigger the risk. In the cyber context, for example, risk analysis would examine attack vectors (phishing, malware, exploits) and the degree to which IT/OT systems are exposed.

- **Risk assessment**

The next step is risk assessment or assessment, i.e. the estimation of the potential impact and the probability of materialization of each risk. Qualitative methods (scales from "low" to "critical") or quantitative methods (financial calculations of expected losses) can be used to determine the level of risk. The purpose of the assessment is to **prioritize risks** – that is, to determine which risks are unacceptable and require immediate treatment, compared to those that can be tolerated in the short term. In practice, many organizations use **risk acceptance criteria** – for example, a financial or security threshold above which the risk must be treated.

- **Treatment and control of risks**

Once critical risks have been identified and assessed, the organization develops and implements **risk treatment measures**. There are four general risk response strategies: avoidance (eliminating the activity that generates the risk, if it is too dangerous), transfer (insurance or outsourcing so that a third party takes on the financial impact of the risk), mitigation (implementing security controls to reduce

the likelihood or impact), and acceptance (assuming the remaining risk, if it is at a tolerable level). For example, faced with the risk of a ransomware attack, a food company could choose mitigation measures (offline backups, advanced antivirus solutions) and transfer (a cyber insurance policy) instead of passively accepting the risk.

- **Continuous monitoring and review**

Risk management does not stop after the implementation of controls; continuous monitoring of the effectiveness of the actions taken and regular reassessment of the risk landscape is essential. The security environment is evolving rapidly – new vulnerabilities are emerging, cyber threats are changing – so organizations need to **regularly review risks** and adjust strategies. An effective risk management process is a dynamic one, a repetitive "life cycle" in which monitoring feedback leads to the identification of new risks or the reassessment of existing ones.

*The figure above illustrates the cycle of the risk management process, including the stages of **Identification**, **Analysis**, Assessment, Treatment and **Continuous Risk Monitoring**. This cycle is repeated periodically to ensure continuous improvement in security.*

In the food industry, the implementation of this general risk management process must be adapted to the specifics of the field, which includes both classic IT infrastructures (computer networks, databases) and operational technologies (industrial equipment, SCADA/ICS) and strict food safety requirements. Next, we will delve into how **cyber risks in the food sector** can be managed through this process.

Cyber risks in the food sector: identification, analysis and prioritization

The agri-food industry has been facing a growing wave of cyber threats in recent years, as digitalization and process automation have expanded **"from farm to fork".** The specificity of the food sector – which combines complex supply chains, industrial production control systems and sensitive recipe or customer data – makes cyber risks unique. In this section we will examine the main digital threats to the food sector, as well as ways to identify and prioritize these risks through recognized frameworks (ex. ISO 27005, NIST RMF, OCTAVE).

Specific characteristics of cyber risks in the food industry

A peculiarity of this sector is the interdependence between **operational technology (OT)** and **information technology (IT).** Food processing plants use SCADA systems and programmable logic

controllers (PLCs) to automate ingredient mixing, packaging, and preservation of environmental conditions (temperature, humidity). These systems, once completely isolated from external networks, are now often connected (directly or indirectly) to IT networks to optimize production and the logistics chain. This convergence exposes industrial equipment to cyberattacks. For example, *"the perception that there is an airgap between automated food systems and the internet is often false – they are rarely completely isolated and need regular updates, which introduces attack vectors",* as a US report pointed out. A **false sense of security** can increase the risk, if managers believe that their industrial systems are protected just because they are not apparently online.

In addition, the food sector often operates with **very strict time frames** (e.g. perishable products that need to be processed and delivered quickly). Thus, a cyberattack that stops production or logistics even for a few days can lead to massive losses and even **food shortages in the market**. This gives attackers a pressure advantage – food companies may be more willing to pay ransoms to restart critically affected operations, for fear of disrupting the population's supply. At the same time, compromising quality or food safety data (e.g. laboratory results, HACCP certifications) can have consequences for public health, which makes certain cyber risks take on a **food safety dimension** in addition to the economic one.

Examples of relevant cyber threats: Among the most common cyber risks in the food industry are:

- **Ransomware attacks on IT and OT systems:** Ransomware is currently considered the biggest digital threat to companies in agriculture and food. A notorious incident is the one suffered by the JBS Foods company in June 2021, when a ransomware attack forced the closure of all of the company's US beef processing plants (about 20% of the national supply), with JBS paying an amount of **$11 million** to criminals to resume activity. This case showed how cyberattack can have a systemic impact on the food chain. In 2023, another cyberattacks targeted Dole Food, disrupting operations and leading to **delays and shortages of products** in stores. Recent statistics confirm the trend: in 2024 alone, there were 212 ransomware incidents in the food and agriculture sector, up from 167 in 2023. Such attacks block access to critical data (recipes, orders, production planning) and can paralyze both food production and distribution on a large scale.
- **Attacks on industrial infrastructures (SCADA/PLC):** A distinct threat is the infiltration of OT networks and the takeover of industrial processes. If a hacker gains access to PLCs in a food factory, the consequences can be **catastrophic**. For example, changing additive dosage or sterilization parameters can lead to **product contamination** or entire batches of food unsafe for consumption. Imagine a scenario in which in a cannery, an attacker raises the temperature in sterilizers below the safe level: the resulting products might look normal, but they would harbor pathogens. Such risks combine the cyber aspect with traditional food safety risk. In 2021, there was even an attempt to poison a municipal drinking water network through unauthorized access to the control system (in Oldsmar, Florida) – an incident that shows that attacks on critical infrastructure can directly target public health.
- **Fraud and phishing in the operational context:** Attackers often exploit the human vector through context-sensitive phishing campaigns. In food companies, an email that appears to be sent by a packaging supplier or logistics partner may contain malware. A single click on a malicious attachment of an employee in the purchasing department can give intruders access to the network. It should be noted that the complex supply chain increases the attack surface through social engineering: there are many partners, suppliers and customers, so many vectors through which an attacker can pose as "someone trustworthy". A Verizon report showed that **15% of security breaches involve a third party** – often attackers first compromise a smaller partner, then use their access to break into the target network.
- **Software and hardware supply chain attacks:** Food companies use niche software solutions for farm, inventory, or distribution management. If these software vendors are attacked (such

as the Blue Yonder incident in 2024, when a ransomware attack on a supply chain technology provider affected major retail customers), the effects trickle down to all of their customers. Also, unsecured IoT devices deployed on farms or factories (environmental sensors, process controllers) can act as a **Trojan horse**: compromised equipment from a supplier can introduce malware into the food company's network when connected. Thus, **due diligence** in the acquisition of IT/OT systems is critical – each new component must be checked from a security perspective before integration.

- **Sensitive data leaks and industrial espionage:** The food industry also includes intellectual property aspects (secret recipes, formulas, technological processes) that can be targets for espionage. A cyberattack can target **the theft** of a beverage manufacturer's recipes or the formula of a natural preservative, which would affect competitive advantage. In addition, customers' personal data (e.g. in retail – card numbers, purchase history) can be stolen if point of sale systems or store databases are compromised. These breaches cause significant damage to their image, with customers losing trust if they hear that their data has fallen into the hands of hackers. In November 2024, a U.S. supermarket chain (Stop & Shop) suffered a cyber incident that disrupted delivery operations and resulted in **empty shelves** for fresh produce in several states – an example that underscores how retail data and IT systems are an integral part of the food chain and can cause visible disruptions for the population.

Identifying and prioritizing cyber risks – reference frameworks.

To effectively manage these threats, food organizations can turn to internationally recognized cyber risk management frameworks. **ISO/IEC 27005** is a standard dedicated to information security risk management, which provides guidance on the identification of information assets, threats and vulnerabilities, risk assessment and their treatment. Although not specific to the food sector, ISO 27005 can be applied to structure a cyber risk analysis in a dairy factory, for example, helping to identify all elements (servers, PLCs, wireless networks in the warehouse, etc.) and the risks associated with each. The standard recommends establishing **risk criteria** from the outset (what level of impact is considered serious, what probability is negligible, etc.), in order to be able **to later classify the risks** and decide which require immediate action.

Another valuable framework is **the NIST Risk Management Framework (RMF),** developed by the U.S. National Institute of Standards and Technology. NIST RMF describes a 7-step process (Preparation, Categorization, Control Selection, Implementation, Evaluation, Authorization, Monitoring) that integrates risk management into the information systems lifecycle. In the industrial (OT) context, FMR is often used alongside specific guidelines such as NIST SP 800-82 (security of industrial control systems) to ensure that cyber risks are identified and mitigated from the design phase of automation systems. For example, by applying NIST RMF in an automated grain silo, managers would **categorize the system** according to impact (e.g., very high availability), **select appropriate controls** (e.g., network segmentation, strict access control), and **continuously monitor** security status (through periodic audits).

Last but not least, the **OCTAVE** (Operationally Critical Threat, Asset and Vulnerability Evaluation) methodology offers an approach focused on the assessment of security risks at the level of the organization and critical assets. OCTAVE emphasizes the involvement of internal staff in identifying threats and vulnerabilities, assessing both technological and process and policy aspects. In a food company, the use of OCTAVE would mean, for example, organizing workshops with mixed teams (IT, production, quality) to map possible attack scenarios (from refrigeration equipment failure to the theft of data about the distribution network) and establish **treatment priorities** based on the impact on the business. The result would be an **action plan** that combines technical measures (e.g. implementation of intrusion detection systems in the industrial network) with organizational measures (e.g., training employees in phishing, reviewing back-up procedures).

Interim conclusion

Cyber risks in the food sector are varied and can cause both financial damage and food safety and public trust issues. By rigorously applying the risk management process – identifying relevant threats, analysing specific vulnerabilities (from the processing plant to the supermarket), assessing the potential impact, and prioritizing interventions – organizations can build resilience. The use of reference frameworks such as ISO 27005, NIST RMF or OCTAVE provides **structure and consistency** to this approach, ensuring that no critical issue is overlooked. In the next chapter we will explore in more detail the **concrete cybersecurity measures** that can be applied along the food supply chain, as part of the treatment of the identified risks.

Cybersecurity in the food supply chain

The agri-food supply chain is a complex ecosystem, comprising raw material producers, processors, transporters, distributors and retailers. Every link in the chain – from farm to shelf – increasingly relies on technology for efficiency and traceability, opening up new attack surfaces for cybercriminals. In this chapter we focus on a **technical and operational** approach to cybersecurity in the food supply chain: we will describe the vulnerabilities specific to each segment of the chain, possible attack vectors, as well as the recommended protection measures (technologies, policies, audits). We will also highlight good practices tailored to both small and medium-sized enterprises (SMEs) and large economic operators in the food industry.

Cyber vulnerabilities and risks in the agri-food chain segments

The food chain can be divided, simplified, into four main segments: **food production processing**, **transport and logistics**, **wholesale distribution** and **retail** (retail). Different types of providers and operators correspond to each, but they are all based on interconnected digital technologies. We will analyze these segments in turn, highlighting the specific cyber risks.

- **Food production and processing (suppliers/processors)**

This includes factories and facilities where agricultural raw materials are transformed into finished food products (from slaughterhouses and sausage factories, to canneries, dairy products, bakeries, etc.). Characteristics of this segment: the intensive presence of **industrial control systems** (PLCs, SCADA) governing production lines, industrial robots, packaging systems and safety equipment (e.g. sensors for quality control). Specific vulnerability:

  - **Old or outdated OT equipment:** Many factories use equipment with long lifecycles (10-15 years) that can run outdated software with known vulnerabilities. For example, a *SCADA system* that controls the temperature in an industrial furnace could run on an outdated, unpatched, unpatched version of Windows, representing a gateway for malware.
  - **Insufficiently segmented networks:** If the production network is connected to the corporate IT network without segmentation, an attack that starts from a simple computer in the office can directly affect the machines in the plantation. A report by industry experts points out that segmenting ICS (Industrial Control Systems) networks should be part of an in-depth security strategy to prevent attackers from moving uncontrolled within the network. The lack of segmentation allows an adversary who has penetrated through the classic perimeter (corporate firewall) to move laterally to critical OT areas.
  - **Unsecured remote access:** Many factories have remote access options for equipment maintenance (suppliers can diagnose machines remotely). If these VPN/RDP connections aren't protected with multiple authentication (MFA) and strict restrictions, they can be compromised. Real cases show that attackers take advantage of reused weak credentials – as was the case at JBS, where the initial breach apparently occurred after an employee used the same passwords at work and on an external website.

- **Human error and lack of awareness:** Manufacturing personnel, focused on volume and quality goals, may not be sufficiently trained in cybersecurity practices. An infected USB stick inserted into an industrial computer or technology workstation can launch an attack. Security culture is still in its infancy in many food factories, where the historical focus has been on physical work safety and food safety, not IT security.

- **Transport and logistics (transport providers, warehousing)**

This segment includes companies that transport raw materials and finished goods, as well as warehouses and logistics centres where goods are stored and redistributed. Technology plays a major role: **connected vehicles** (refrigerated trucks with telemetry, GPS, temperature sensors in trailers), **fleet management systems**, **smart warehouses** (e.g. automated warehouses with robots or computer-controlled conveyor belts). Vulnerabilities and risks:

- **Unsecured IoT systems:** Modern transport vehicles have integrated IoT – from sensors that monitor temperature to devices that transmit position and status in real time. These devices, if not secured (default passwords, unencrypted protocols), can be hacked remotely. An attacker compromising the sensors of a refrigerated truck could shut down the **cooling system** or modify the sensors so that the driver does not notice the temperature rising, resulting in the cargo being damaged on the road. Similarly, unauthorized access to a warehouse's system can allow fans to shut down, increasing humidity and destroying batches of stored grain.
- **Logistics IT platforms:** The entire logistics flow is usually orchestrated by specialized software (transport management systems, stock management systems – WMS). If these platforms are hit by ransomware or DDoS, operations stop. A hypothetical example: a ransomware attack hits the central warehouse management system of a supermarket chain, encrypting the stock database and delivery routes; The result would be **major delays in deliveries and unstocked shelves** until backups are restored. Such attacks have even happened – for example, the 2024 attack on software provider Blue Yonder disrupted the supply chains of retailers such as Sainsbury's, forcing them to temporarily resort to manual procedures.
- **Reliance on third parties and their integration:** Transportation and storage are often outsourced to third-party firms. This means IT links between companies – data exchange, common portals, APIs. If either of these partners is compromised, **attackers can use trusted connections** to penetrate further. A concrete example: an attacker breaks into the system of a small transport company, then uses the digital certificates stolen from there to access the portal of a major manufacturer where that company had access for orders. Attacks through the supply chain are on the rise (Verizon estimating ~15% involves third parties), which makes the security assessment critical when onboarding (contracting) new suppliers.
- **Interference with navigation and communications systems:** An often-overlooked aspect is that logistics fleets depend on GPS and mobile networks. Sophisticated attackers could use GPS jamming or spoofing to disorient delivery trucks or drones, or intercept unencrypted radio communications. These actions are more related to communications security, but they are becoming part of the cyber risk landscape of food logistics.

- **Distribution and wholesale (distributors, regional hubs)**

This segment connects manufacturers and retailers, usually through large distribution centres where products from multiple sources are consolidated, sorted, and sent to stores. From a technological point of view, it resembles the logistics segment (large, automated warehouses, IT inventory management systems), but it also has peculiarities: large volumes of transaction data, direct links with retailers'

systems for demand forecasts, and sometimes **financial systems** (invoicing, EDI – Electronic Data Interchange with suppliers). Specific risks include:

- **Attacks on data and financial systems:** A distributor handles thousands of invoices and payments. A Business Email Compromise (BEC) attack could intercept an important payment or redirect funds (e.g., changing a provider's bank account in the database after a fraudulent email). Also, compromising EDI systems can disrupt orders to manufacturers, which has a direct effect on emptying stocks on the shelf if orders are no longer transmitted correctly.
- **Critical centralized IT infrastructure:** Distribution centres rely on central IT infrastructure (servers, databases). Often there is **a single ERP** that coordinates the entire flow. This becomes a *single point of failure* from a cyber perspective – any successful attack here (ransomware, internal sabotage) can completely stop the ability to ship products to hundreds of stores. That is why continuity plans (disaster recovery), and **offline back-up** are vital at this level.
- **Physical vulnerabilities with cyber impact:** Wholesale centres can be targets for unauthorized physical access (warehouse intruder) that can connect an unauthorized device to the network or steal a server from the premises. Physical access control and video monitoring are becoming integral parts of cybersecurity, because a determined attacker can combine methods (physical + cyber) to exploit an organization.

- **Retail (food retail)**

The last link, consisting of supermarkets, hypermarkets, small grocery stores and online food commerce platforms. The technologies involved include **modern POS (Point of Sale) systems** and cash registers, Wi-Fi networks for customers, mobile online shopping applications, customer loyalty systems and IT infrastructure in stores (terminals, self-checkout kiosks, etc.). Examples of vulnerabilities and risks:

- **Compromising POS systems:** In-store, payment terminals and checkouts are often targeted by specialized malware (e.g., **POS malware** that extracts data from the magnetic stripe of cards). If the retailer doesn't keep these systems up-to-date and doesn't use end-to-end encryption for transactions, criminals can steal **customers' credit card data** directly from memory. There have been famous breaches in retail (e.g. the attack on Target in the US in 2013) that, although not food-specific, show what reputational and financial damage exposure millions of customers can have.
- **Attacks on digital infrastructure in stores:** As retail becomes omnichannel, brick-and-mortar stores are integrated with online platforms, mobile apps, and home delivery systems. A cyberattack can involve **DoS (Denial of Service)** on a supermarket's online shopping site, paralyzing online orders, or compromising the mobile product scanning app (if communication with the server is not secure). Also, because many stores rely on VPN connections to the center for inventory and pricing, ransomware that affects the headquarters can **also block physical stores** (which can no longer scan products or process payments if they can't access the central servers).
- **Risks to consumer data:** Food retailers collect names, addresses, purchase history (via loyalty cards), and payment information. This data is attractive to attackers either for resale on the black market or for blackmail (e.g., a supermarket chain could be blackmailed with public exposure of customer data). A landmark incident occurred at **the Krispy Kreme** company in 2024, when a cyber-attack disrupted the online ordering system during a peak period, affecting customers and revenue. Even if it did not involve data theft, the case highlights retail's dependence on digital platforms.

POS system in a modern supermarket – an example of essential digital technology in the food supply chain. Such systems, if not properly protected, can become targets for cyber attackers, compromising customers' payment data or disrupting sales operations. Implementing security updates and segmenting the store network helps reduce these risks.

Supply chain-specific attack vectors

From the above examples, it appears that many risks are propagated through the links between segments. Two sectors are worth highlighting:

- *Third-party attacks*: Whether it's a raw material supplier, a carrier or an IT service provider, the weakest link in the chain can be the gateway. A breach at a small local manufacturer supplying ingredients can provide access to a large processor's system, if the two have interconnected systems for orders. That is why assessing **the security of suppliers** and imposing minimum security requirements in contracts has become essential in supply chain management (we will elaborate on the measures).
- *Attacks on data and trust systems*: the food chain relies on the accuracy of data (e.g. HACCP test data, quality certificates, or even product labels). An attacker who manages to falsify or delete such data can cause chaos. For example, if a plant's HACCP plan (which indicates critical food safety checkpoints) is stolen and published, attackers could identify **weaknesses** (as shown by the example of the HACCP plan exposure mentioned by TXOnetxone.com) or blackmail the company with their disclosure. The integrity of the information in the chain (including batch traceability) is therefore a cybersecurity concern, not just a quality one.

Recommended cyber protection measures in the agri-food chain

Given the multitude of risks, companies in the food sector must adopt a **multi-layered** cyber defence strategy, applying the **defence-in-depth** principle. We will further outline a number of key technologies, policies and recommended practices to protect the supply chain, from manufacturing to retail:

- **Segmentation and securing of OT and IT networks: As** mentioned, network segmentation is fundamental. Basically, the corporate IT network (computers, offices, internet) must be strictly separated from the OT operational network (SCADA, PLCs, factory sensors), allowing only the necessary communications through secure gateways and industrial firewalls. Segmentation limits **the lateral spread** of an attack – for example, even if a desktop PC is infected with malware, it shouldn't end up controlling ovens or bottling lines. ISA specialists recommend segmentation as part of security best practices for centuries in the physical domain and decades in IT, showing that it offers a much more robust level of security than a single perimeter defence. In addition, **micro-segmentation** within OT networks (zoning and cell division according to ISA/IEC 62443) can even stop the movement of an attacker who has penetrated OT – for example, packaging PLCs are in a separate area from cooking PLCs, with minimal communication between them, supervised and filtered.
- **EDR (Endpoint Detection and Response) solutions:** EDR is a technology that monitors activity on workstations and servers in real time, in order to detect abnormal behavior (indicative of malware or attacks) and respond automatically (isolation, blocking). In the context of the food chain, EDR should be installed on all critical IT systems: servers hosting the ERP, employee workstations with access to sensitive data, even on certain factory systems running Windows/Linux (e.g. HMI – Human Machine Interface – HMI stations). A well-

configured EDR can quickly catch ransomware before it spreads or an attacker attempting lateral movements. For example, if an employee clicks on a malicious file receiving a backdoor, EDR can detect suspicious execution and **stop the malicious process** immediately, sending an alert to the security team.

- **SIEM (Security Information and Event Management) systems:** A SIEM collects and correlates event logs from across the entire infrastructure – firewall, servers, controllers, applications – to identify potential incidents. In the food supply chain, a SIEM can be configured to monitor events such as unauthorized connections between the manufacturing network and the internet, multiple authentication failures on PLC access accounts, unexpected changes in HACCP configuration files, etc. By correlating these signs, the SIEM can generate **early warnings**. For example, the simultaneous detection of an unusual volume of data traffic from a database server and a VPN connection opened at unusual times could indicate data exfiltration – the SIEM can alert and trigger response procedures. The implementation of SIEM is especially recommended for large operators, who have SOC (Security Operations Centre) resources and can promptly analyse alerts, but SMEs can also resort to managed SIEM variants (MSSP).
- **Multi-factor authentication (MFA) and robust access management:** A seemingly simple measure, MFA, has proven highly effective in preventing accounts from being compromised even if passwords are stolen. All access to critical systems (remote VPNs, administrator accounts, access to cloud management platforms) must require two or more authentication factors (password + hardware token or mobile application). Implementing MFA could have prevented some big breaches (e.g., the aforementioned JBS attack, started from reused stolen credentials). In addition, the Zero **Trust** principle – "Trust no one by default, always verify" – should be adopted as a general policy. This means that every request for access to a system, even from an employee in the network, is treated as potentially unauthorized until it is verified. Basically, Zero Trust translates into: segmentation (which we have already mentioned), MFA everywhere, continuous verification of the integrity of the devices that connect (e.g. a computer with antivirus disabled cannot access internal servers) and the principle of least privilege (each account or application has access only to the resources strictly necessary).
- **Update and patch management:** A significant number of incidents are based on the exploitation of known vulnerabilities for which patches already exist. That's why a rigorous **patch management** program is vital. The challenge is major especially in the OT area: many industrial systems do not support frequent shutdowns for updates or use equipment that goes out of support. The solution involves planning – immediate patches on IT systems (servers, PCs) and scheduled patches on ICS in maintenance windows, possibly combined with compensatory measures (isolation, increased monitoring) until the patch is applied. For example, if critical vulnerability affects a PLC and cannot be patched immediately because it would stop production, the company can temporarily implement a firewall rule that blocks access to the ports used by that vulnerability and intensify monitoring of traffic to that PLC until it can be safely patched. **Updating firmware** to IoT devices on farms or warehouses is again essential, as many IoT attacks are based on old versions of firmware.
- **Regular backups and disaster recovery plan:** Many small businesses only realized the importance of backups after suffering a ransomware attack. A good practice is to apply the **3-2-1** rule: three copies of the data, on two different media, one off-site (disconnected). For production, this means having backups for both IT data (recipe databases, accounting systems) and OT configurations (PLC programs, SCADA configurations). These backups should be tested periodically. A disaster recovery plan should detail how operations are quickly restored in the event of a major incident. For example, if the distributor's ERP system goes down, what is the procedure? (maybe temporary switching to manual order processing, using backup files, etc.). The plan must be practiced, not just written.

- **Continuous monitoring and intrusion detection:** In addition to EDR and SIEM, which are active solutions, it is recommended to use IDS/IPS (Intrusion Detection/Prevention Systems) also for industrial networks. There are specialized OT monitoring solutions that can detect, for example, unauthorized commands on an industrial protocol (Modbus, OPC-UA) or unprogrammed changes in the logic of a PLC, and alert immediately. Some may even **block suspicious command** (IPS). Monitoring network traffic in the factory and warehouse area (e.g., monitoring wireless sensor networks) can reveal abnormal activity (a new device communicating strangely, possibly a compromised device). Investing in such technologies is more suitable for large companies, but SMEs can also adopt simpler versions or outsourced monitoring services.
- **Security policies and procedures (organizational framework):** Technology cannot cover everything without clear and respected rules. Companies must have written policies for password security (e.g. periodic change, complexity), use of mobile devices, access to data (who and under what conditions can copy sensitive data). A supplier **access control policy** is also crucial: for example, there should be procedures in place to grant temporary access to an OT maintenance technician so that after the work is completed the account is immediately deactivated. **Due diligence in supplier onboarding** means the prior evaluation of new partners in the chain: security questionnaires, on-site audits or the request for certifications (ISO 27001 for IT suppliers, for example) before connecting them to internal systems. Contracts should include cybersecurity clauses and prompt notification in the event of an incident (so as not to find out late that a supplier has been hacked). Another element is **the management of external media**: the policy should prohibit the use of unauthorized USB sticks in industrial environments and provide for the scanning of any newly introduced equipment (modelled after the portable scanners that were talked about in TXOne solutions – a device for inspecting new equipment for malware before connecting).
- **Training and awareness (Cybersecurity awareness):** The human factor often remains the weak link, but it can also become the strongest defence if staff are properly educated. All employees, from factory workers to top managers, should take regular cybersecurity awareness courses. These must be adapted to the context: workers will be explained why they should not connect personal devices to the machine network and how to recognize a phishing email claiming to be from a boss; transport drivers can be shown how to react if the telematics device in the truck behaves strangely; IT staff – hardening and incident response policies. A strong security culture means that employees **immediately report** suspicious incidents (a computer that "struggles" after opening a file, a foreign device spotted in the factory, etc.), which allows the response team to act before the damage escalated. The company's management must be involved in promoting this culture, so that the safety rules are followed as rigorously as the food safety rules.
- **Security audits and penetration testing:** It is difficult to know how effective the measures are implemented without practically checking them. **Periodic audits** (internal or third-party) can assess compliance with policies (e.g. an audit may find that, despite the policy, some critical servers have not been patched for 6 months). More thoroughly, **penetration tests** simulate real attacks to find breaches. For example, a pentesting team hired by a beverage manufacturer might try to break into the company's network through various means: phishing employees, scanning the network for open ports, even covert physical access to the premises. The results of these tests highlight **weaknesses** before real criminals discover them. It is recommended to include OT components in the test scope, with caution (non-intrusive tests, so as not to disrupt production). A useful test scenario is a **red team – blue team exercise** where a group simulates a complex attack on the entire chain (including the compromise of a fictitious supplier) and the internal security team must detect and respond. These exercises reveal both technical vulnerabilities and gaps in procedures or reaction times.

Best practices and tailored recommendations (SME vs. large companies)

The implementation of the above measures can vary significantly depending on the size of the organization and the resources available. We will point out some distinct recommendations for **small and medium-sized enterprises (SMEs)** in the food industry, respectively for **large economic operators**:

- **SMEs (small factories, processing farms, local warehouses, independent stores):** These often have limited IT resources and lack dedicated security teams. However, they are not safe from attack – criminals may consider them easier targets. Good practice for SMEs:
    - *Outsourcing and managed services:* If they cannot afford an IT security department, SMEs can turn to **MSSP** (Managed Security Service Providers) or consultants to configure and monitor their basic security (firewall, antivirus, backup). An MSSP can provide EDR/SIEM solutions on a subscription basis, more affordable than in-house deployment.
    - *Focus on fundamentals:* The good thing is that many SMEs have simpler infrastructures. The priorities should be regular offline backup for critical data (especially prescriptions, HACCP forms, financial data), up-to-date updates for all PCs and systems (using automatic updating where possible), and minimum awareness training for staff (not fall into obvious phishing traps). Also, using cloud solutions for email, storage, or ERP (Software as a Service) can shift some of the security responsibility to specialized vendors (who have security teams). Of course, reliable assessments must be made for these providers.
    - *Simple network segregation:* Even with limited resources, things such as separate router and separate Wi-Fi network for production vs. office equipment, changing default passwords on all devices (surveillance cameras, routers, etc.), disabling unused services can be achieved. These actions do not cost much, but they reduce the attack vectors.
    - *Simplified incident response plan:* SMEs should at least have a **response plan in case of** a cyberattack: who is called (IT provider, police, national CERT?), how to isolate infected systems quickly (who removes the cable from the server), how to communicate internally and externally (notify customers if applicable). Repeating this plan once a year (at least on paper) will help enormously in the real case.
- **Large companies (food groups, retail chains, processors with dozens of factories):** These organizations have extensive infrastructures and are attractive targets for sophisticated attacks. Good practice for them:
    - *Alignment with recognized standards and frameworks:* It is advisable for large companies to implement an **ISMS (Information Security Management System)** according to ISO 27001, which includes periodic risk assessments (according to ISO 27005) and documented controls. Also, specific standards such as **ISA 62443** for industrial environments can guide OT security practices. Adherence to such standards provides a **holistic framework** and can also improve the company's image in front of partners (demonstrate maturity on security).
    - *Investments in advanced technologies:* In addition to EDR and SIEM, large companies can adopt solutions such as **advanced industrial monitoring** (e.g. OT security platforms that map all assets in factories and detect anomalies in traffic), **user behaviour analysis** (UEBA – User and Entity Behaviour Analytics, which would catch abnormal activities of a legitimate account), or even artificial intelligence for detecting Threats. They can also deploy redundant and availability-centric systems

(e.g., synchronized backup data centers, in case one is attacked, the other quickly takes over).

- *Dedicated teams and partnerships:* Large operators should have an internal **CSIRT** (Computer Security Incident Response Team) or a blue-team team that monitors and responds to incidents 24/7. Collaboration with specialized bodies is also useful: for example, in the global food sector there is the Food and Ag-ISAC (threat intelligence sharing centre) that provides alerts about emerging attacks. Large companies should be active members of such initiatives in order to be aware of the new tactics used by attackers.
- *Complex testing and continuous evaluation:* A large company can afford and should periodically execute **crisis management** exercises simulating major attacks. The involvement of top management in **table-top exercises** will ensure that, in the event of a real incident, decisions (e.g. to stop production temporarily, to make public notifications, or to pay/not pay a ransom) are made quickly and informed. An example of good practice is the organization of national or sectoral training exercises – in 2024 CISA (the US cybersecurity agency) conducted the **Cyber Storm exercise** focused on the food and agriculture sector, bringing together large companies to test their coordination and response to simulated attacks. Participating in such exercises (or replicating them internally) prepares organizations for real-world situations.

Final conclusions

The cybersecurity of the supply chain in the food sector can no longer be ignored – recent incidents have shown that from farms to supermarkets, every component can be disrupted by digital attacks, with consequences for food for the population, consumer confidence and economic stability. A proactive approach, combining **technical practice** (implementing appropriate controls and technologies), **narrative storytelling** (understanding possible attack scenarios and preparing for them) and **academic rigor** (aligning with recognized standards and methodologies, based on studies and reports) is necessary to ensure the resilience of this critical sector. Essentially, companies need to build an environment where risks are known and kept under control, where a potential cyber incident can be quickly isolated without harming the end consumer. By implementing the measures discussed and cultivating a culture of security, the agri-food sector can protect its **supply chain** against increasingly sophisticated cyber threats, while ensuring food safety and continuity of supply.

Operational continuity

Business continuity refers to an organization's ability to maintain its essential functions during and after a major incident (be it cyber, technological, or even physical, such as a natural disaster). In the context of the food supply chain, **continuity planning** is crucial, as disruptions can have immediate consequences on the supply of the population. The NIS2 Directives and national legislation underline the importance of this: entities must take **measures to ensure the continuity of essential services** in the event of cyber disruption. This chapter looks at how to prepare for such situations and the planning tools available.

Continuity planning

The first step in ensuring continuity is to carry out a Business Impact Analysis (BIA). Through BIA, the company identifies which processes and activities are critical, which are the dependencies, dependencies, etc. For example, a milk processor may determine that stopping the pasteurized line leads to the spoilage of the raw material, hence the RTO for the pasteurization control system; also, the loss of traceability data for more than the last hour of production (RPO = 1 hour) would compromise the ability to make accurate recalls, so data backups must be done at least hourly.

Once the recovery requirements have been identified, **continuity strategies** can be developed. These include: redundancy of infrastructure (duplicate systems or backup servers), safety stocks (of raw materials or finished products) to cover delays, diversification of suppliers (to have an alternative if the main one is unavailable), plans for temporary relocation of production (if one factory goes down, another can partially take orders), manual work procedures (for example, issuing manual invoices if the computer system is turned off), etc. A special emphasis is placed on **data backup and recovery**: all critical data (recipes, orders, equipment configurations) must be copied periodically and stored securely, testing their recovery. Many cyber incidents (such as ransomware) can be overcome faster if there are valid backups and a quick recovery plan.

Business Continuity Plan (BCP)

The central tool is the development of a **Business Continuity Plan (BCP).** This is a comprehensive document that describes *how* critical functions will be maintained or restored in the event of a major disaster or incident. For NIS (essential/important) organizations, the existence of an updated and tested BCP is a practical necessity and, implicitly, expected by the authorities as part of the security measures. A specific BCP for the food chain will contain:

- **Purpose and scope:** what scenarios it covers (e.g. severe cyberattack, extended power outage, unavailability of a key supplier, pandemic, etc.) and which units of the organization are involved.
- **Crisis and responsibilities team:** a nominal list of the members *of the continuity/crisis management team*, with the roles of each one (team leader, communication, IT, production, logistics, customer service, etc.) and emergency contact details (alternate phone, personal email if the corporate network is down, etc.). For example, the operations director can be the head of the crisis committee, the CIO responsible for IT restoration, the production manager for manufacturing resumption, etc.
- **Immediate response procedures:** the measures to be taken immediately after a serious incident is detected. This can include *short action plans (playbooks)* such as in case of ransomware – disconnect the affected systems from the network, start the backup servers if they exist, notify the security team; in case of a SCADA system crash – put the installations on manual control according to procedure X, inform the shift supervisors, etc. These immediate actions have the role of limiting the impact and preparing the ground for recovery.
- **Continuity plans for each critical function:** detailing how each critical process identified (through BIA) will be maintained. For example, continuity plan for **order processing**: if the IT platform for receiving online orders goes down, orders will be received by phone/fax at a backup number, sales staff will be reassigned to take them manually, they will be noted in a register and then entered into the system when they return. Another example is a production continuity plan: if the main factory is non-functional for 24 hours, delivery from existing stocks will be prioritized, production will be temporarily subcontracted to a partner (if there is an agreement) or it will be delivered from another location. These plans must be as concrete and operational as possible.
- **Necessary and logistical resources:** what resources are critical and how are they provided in the event of an incident – from emergency power supply (generators for cold storage, for example), to backup internet access, to alternative transport vehicles. If, for example, the truck routing system fails, drivers must have a communication procedure (by phone, SMS) in order to receive delivery instructions.

- **Communication in case of crisis:** the plan must include predefined messages and communication channels both *internal* (to employees: what to do, where to present themselves, how to continue the activity) and *external* (to customers, suppliers, authorities, media). In the food chain, prompt communication with retailers or distributors is essential if deliveries are delayed. Also, if there is a risk that unsafe products have reached the market, recall communication and public information must be prepared, in coordination with the health authorities.

- **Disaster recovery procedures (IT):** although it is sometimes a separate plan (DRP – Disaster Recovery Plan), the BCP includes concrete measures to restore the IT infrastructure and resume normal operations. This includes: the sequence of restoring servers from backup, reconnecting networks, verifying the integrity of recovered data, testing critical applications, etc., in the order set by business priorities. For example, it is established that the ERP (enterprise resource planning system) must be restored within 8 hours, the public website can wait 48 hours, and so on.

- **Stand-down plans:** once the crisis has passed and systems are restored, the plan must cover how to transition from provisional to normal procedures, reinstatement of standard controls, assessment of the state of the business (e.g. inventory of delays, delivery arrears, resumption of production at capacity). This is also where **the lessons learned** come in: organizing a post-incident debriefing and updating plans based on what is found.

A **short continuity plan** (or *summary version*) is often used as a practical guide for crisis situations – a condensed document, of a few pages or even a poster, containing the essential information: emergency contacts, immediate steps to follow, recovery priorities. It is easily accessible and understandable to all key employees, serving as a *checklist* in times of high tension. For example, a **checklist of actions in the event of a major incident** can look like this: 1) Make sure that the staff is safe; 2) Confirms the nature of the incident (cyber, IT, physical); 3) Informs manager X and the crisis team; 4) Activate the continuity plan – consult the relevant section (IT/production); 5) Communicates internally the activated "emergency mode"; etc.

On the other hand, **the complete continuity plan** is the detailed document that we have described above, which provides all the necessary information to manage the crisis step by step. It is good for organizations to have both versions: the complete plan, updated annually or whenever changes occur (e.g. new systems, reorganizations), and operational statements (short) for quick use.

A critical aspect is **testing and updating plans**. A continuity plan is only valuable if it has been tested beforehand, otherwise there may be undetected gaps. Testing can be of several kinds: *desk-check exercises* (theoretical team review of the plan), *simulation exercises* (for example, you simulate that the ERP system is unavailable and see how the team reacts for a few hours by working according to alternative procedures), *failover technical tests* (starting backup servers, running systems on the generator, etc.). ENISA and good practices recommend testing plans **at least annually** and whenever major changes occur in the organization.

In Romania and Bulgaria, companies in the essential/important food sector will have to include continuity plans in their overall security measures. The authorities may require records of the tests carried out or organize sectoral exercises. For example, we can expect the DNSC (RO) or the equivalent in BG to initiate **cyber crisis exercises** in the food sector, similar to those organized in sectors such as energy or finance, to check the level of readiness.

In conclusion, operational continuity is *the safety net of* the supply chain. No matter how robust the prevention measures are, a severe incident can still occur, and then the difference between a minor impact and a disaster will be made by the degree of preparedness and the ability to react quickly. Companies that have well-developed plans will be able to overcome incidents, protecting both their

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the European Cybersecurity Competence Centre can be held responsible for them.

business and consumers. The others risk not only legal penalties, but also the irreparable loss of confidence in the market. Continuity must be seen as an indispensable investment in **the resilience** of the food chain.

Incident response

Even with robust risk management and robust preventive measures, no system is foolproof. Therefore, the ability to **respond effectively to cyber incidents** is a critical component of the security strategy. Incident Response consists of a set of processes and procedures through which an organization detects, investigates, limits and recovers from security incidents, minimizing their impact. The NIS2 Directive requires essential and important entities not only to prevent, but also to **manage incidents in a professional manner**, including by notifying the competent authorities within a strict timeframe. This chapter addresses how to organize the response to incidents in the food supply chain, both internally within companies and in interaction with authorities and partners.

Organization of the incident response team (internal CSIRT)

The first step is to establish an **incident response team** within the organization. This is often referred to as CSIRT (Computer Security Incident Response Team) or IRT. In smaller companies, it can be an ad-hoc group of employees with IT skills, under the coordination of the IT manager or security officer. In large companies, there are dedicated security teams (SOCs – Security Operations Centre) that continuously monitor and react to alerts. Regardless of the size, it is important that the roles are well defined: who analyses the alerts, who decides to escalate a major incident, who communicates externally, etc. An **Incident Response Plan (IRP)** documents these aspects, similar to how BCP documents continuity.

The standard steps of the incident response cycle, according to NIST and other best practices, are **Preparedness, Detection and Analysis, Containment and Eradication, Recovery, Lessons Learned**.

- **Preparation:** includes all the preliminary activities that ensure that the team is ready to intervene. This includes defining incident policies (what types of events constitute an "incident" and how severe they can be), implementing detection systems (network monitoring, IDS/IPS systems, alarms on servers), preparing investigation tools (malware analysis software, access to centralized logs), as well as training the team. In the food sector, training must take into account the specifics of the ICS: the response team should include or be able to call on automation engineers who know industrial systems, not just IT experts, because analysing an incident on a PLC or SCADA requires OT knowledge.
- **Detection and analysis:** the moment when a suspicious event occurs and is identified. The sources can be automatic (a monitoring system detects abnormal traffic, an antivirus endpoint alerts about malware, a compromise indicator received from CERT shows the presence in the systems) or human (an employee reports strange PC behaviour, a partner announces that he has been attacked and maybe problems have propagated). The initial analysis determines whether it is a *real incident*, what type (data exfiltration, ransomware, DoS, account compromise, etc.), which systems are affected and estimates the impact. This phase is crucial and difficult – statistically, many organizations discover incursions late (days or weeks can pass between compromise and detection). That's why practices like *proactive threat hunting* or close surveillance of logs are valuable. In the food chain, an alarm sign could be a PLC server that restarts unscheduled, an unjustified increase in traffic between the office and industrial networks, a user account that launches unusual orders at inappropriate times, etc.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the European Cybersecurity Competence Centre can be held responsible for them.

- **Contain, eradication:** Once an incident is confirmed, the immediate priority is **to limit the damage**. This can mean isolating the affected segment (disconnecting a network, shutting down a compromised server), blocking the attacker's access (changing passwords, blocking suspicious accounts), and preventing it from spreading (e.g., if malware is detected on a PC, the PC is disconnected and everything else is checked). In the case of file-encrypting ransomware, containment means stopping the spread on the network as quickly as possible – which sometimes involves the difficult decision to temporarily shut down certain critical systems preventively. In parallel, **the eradication of the cause** begins: identifying and eliminating malware, closing exploited vulnerabilities (e.g. applying a patch if a known vulnerability has been entered), eliminating persistence (backdoors left by the attacker). This stage must be done carefully: if you act too slowly, the attacker can cause more harm; If action is taken too quickly or unprepared, important evidence for investigation can be lost. Sometimes companies specialized in incident response are used, especially for serious incidents – in Romania and Bulgaria there are such services, either provided by internal teams of integrators, or by international teams that can intervene on request.

- **Recovery:** Once the immediate threat is neutralized, the focus shifts to recovering systems and returning to normal, safe operations. If a server has been affected, it can only rebuild from the backup and reintegrate into the network after we are sure that it will not be reinfected. In the event of data theft, recovery also means restoring data integrity and managing the consequences (e.g., resetting compromised credentials). The Continuity Plan (BCP) discussed earlier is closely related to this phase: if it has been activated, the transition from temporary to restored systems is now being made. A special aspect: in the food industry, if the incident has affected production processes, recovery involves quality checks. For example, if the production lines have stopped suddenly, when restarting it must be tested that the quality parameters are within the parameters, and the final product is safe (according to food standards). Therefore, the food quality and compliance team are involved with the IT team in validating the return to normal.

- **Post-incident/lessons learned:** The last formal step is to analyse the incident after resolution, to document what happened, how it was responded, and what can be improved. A detailed **incident report** is drawn up, which includes the chronology, attack vector, impact (affected assets, downtime, losses), measures taken and recommendations. This report is useful internally (to prevent future similar incidents) but also externally – it is basically the information that will be the basis for the final notification to the competent authority, according to NIS2 (the report that must be sent 1 month after the incident). Also, this post-mortem analysis may reveal investment or policy change needs (e.g., if the incident was possible due to the lack of rigorous patch management, addressing this gap will be prioritized).

Incident notification and cooperation with authorities

According to the NIS2 Directive (and associated national legislations, such as GEO 155/2024 in RO), companies in the food chain classified as important entities must **notify the authorities** (DNSC in Romania, the future designated authority in Bulgaria - the national competent authority and CERT-BG) when they suffer an incident with a significant impact. The definition of a 'significant incident' takes into account several factors: the number of beneficiaries affected, the duration, the geographical scope, the severity of the disruption of the service, the economic or societal impact. An attack that halts production for a few hours may be insignificant, but one that makes it impossible to deliver food in a day to a wide region would be considered significant and therefore notifiable.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the European Cybersecurity Competence Centre can be held responsible for them.

The reporting mechanism was previously detailed: ideally an initial alert within 24 hours, full notification within 72 hours and final report after 30 days. In practice, companies must establish *a protocol internally*: who has the authority to notify (usually the head of the NIS or CISO, with the approval of management), what information is sent and how. To facilitate this, it is recommended to prepare an **incident notification form** (or template) containing the necessary fields. An example of an **incident notification form** would include:

- **Reporting entity details:** Name of organization, contact person (NIS officer), contact data (phone, email).
- **Type of entity and sector:** Major entity, food sector (production/processing/distribution).
- **Date and time of incident detection:** ... (hour/minute accuracy).
- **Brief description of the incident:** e.g. "Ransomware attack that affected production servers and inventory management systems".
- **Initial impact assessed:** affected systems (e.g.: "SCADA at factory X, ERP unavailable"), disrupted services ("production stopped for 8 hours, delayed deliveries"), estimated share of damage (e.g.: "~30% of the daily production volume delayed").
- **Potential cause:** if it is known or suspected – e.g.: "suspicion of a phishing cyber-attack (ransomware); encrypted files and observed ransom note."
- **Measures taken immediately:** e.g.: "Network segmentation, infected systems isolated, continuity plan activated – deliveries honoured from stocks".
- **Possible cross-border impact:** e.g. "Yes – deliveries to two partners in another Member State (Bulgaria) may be delayed" or "No, localized impact".
- **Need for assistance:** optional, if the company requests assistance from the authorities/CSIRT.
- **Other relevant information:** any technical details (known indicators of compromise, attacking IPs) or context.

This form would correspond to the initial notification/within 72 hours. Subsequently, the final report would contain the complete analysis: confirmed vector, exploited vulnerabilities, the exact volume of the impact (e.g.: "12,000 tons of delayed production, later recovered", "no data exfiltration detected", etc.), as well as the corrective measures implemented (patches applied, practices changed). The purpose of the notification is not to sanction the reporting entity for having suffered an attack (victimization is not fault), but to allow the authorities to monitor threats and, if necessary, to alert other operators or provide support. At the same time, **cooperation with the authorities** implies that, if necessary, the company will provide additional information, allow investigations (whether the attack is of national or criminal interest) and implement the recommendations received.

In Romania, the DNSC centralizes notifications. It is possible that the DNSC will provide an online reporting platform or dedicated addresses. In Bulgaria, CERT Bulgaria will play a similar role. It should be noted that NIS2 legislation prohibits the use of information obtained through notifications to incriminate the reporting entity – so the purpose is cooperation, not blaming the victim.

European best practices in risk management and supply chain security

To support entities in implementing NIS2 requirements and increasing the level of security, the European institutions and standardization bodies have developed a number of **relevant standards, guides and best practices**. The adoption of these common benchmarks facilitates a uniform level of protection and ensures the interoperability of security measures across cross-border chains. Below,

we summarize the most important sources of good practices at European and international level applicable to risk management in the food supply chain:

- **ISO/IEC international standards:** The ISO 27000 family of standards provides a general framework for information security (ISO/IEC 27001 sets out the requirements for an information security management system – ISMS, and ISO/IEC 27002 provides guidance for implementing controls). These standards include requirements related to risk assessment and risk treatment at suppliers. Of particular interest is the **ISO/IEC 27036 series – Security management in supply relations**: this series covers the stages of the relationship with suppliers (planning, selection, contracting, management, termination) from a security perspective. By adopting ISO 27036, an organization structures its supply chain security program, having policies and controls for each phase (e.g.: imposing security requirements in contracts, periodic supplier evaluations, secure off-boarding procedures upon termination of collaboration). Also, **the ISO 28000** standard (security management for the supply chain) provides a general framework for risk management in supply chains, although it has a broader perspective (including physical risks) and does not specifically address cybersecurity. For the food sector, the combination of ISO 22000 (food safety) with ISO 27001/27036 (information security) can provide an integrated risk management system of all kinds.

- **ENISA Guidelines:** The EU Agency for Cybersecurity (ENISA) has an active role in disseminating good practices. The report **"Good Practices for Supply Chain Cybersecurity" (ENISA, 2023)** is an essential reference. It presents the findings of a study on current practices in key and important entities in the EU and makes recommendations on five areas: strategic approach, chain risk management, supplier relationship management, vulnerability management, product quality assurance and security practices at suppliers. Some concrete good practices highlighted by ENISA include: *integrating chain risks into corporate governance* (assuming responsibility at top management level and allocating dedicated resources), *maintaining an up-to-date inventory of all outsourced suppliers and services*, *classifying suppliers by risk categories* (critical, medium, low) and applying proportionate controls to each category, *the inclusion of security requirements in procurement processes* (from RFPs to specific contractual clauses), *the continuous monitoring of the security performance of critical suppliers* (possibly through security rating services or independent audits), as well as the *establishment of communication channels for security incidents with suppliers*. ENISA also recommends adopting a *collaborative approach*: rather than unilaterally imposing requirements on small suppliers, larger companies can provide them with assistance and know-how to improve their security (on-chain 'mentoring' relationship model).

- **NIST Framework for Supply Chain Risk Management (Cyber SCRM):** Although originating in the US, NIST SP 800-161 (revision 1, 2022) has become an international benchmark in practice. It proposes a multi-level on-chain risk management model, aligned with NIST SP 800-53 controls. Many multinational companies, including in Europe, are inspired by NIST to create rigorous SCRM (Supply Chain Risk Management) programs. Some NIST principles: involvement of all relevant functions (not only IT, but also the procurement, legal, financial department, etc. in the assessment of supplier risks), assessment of both **cyber** and **operational resilience** risks (e.g. the supplier's ability to deliver in case of disruptions), the requirement that critical suppliers also have robust security practices and continuity plans, and the lifecycle chain approach (from design – ensuring that secure equipment/software is purchased – to scrapping – ensuring the safe destruction of data and devices).

- **Practices of national agencies (BSI, ANSSI, etc.):** The national bodies in Western European countries have published guides that can serve as a model. For example, **BSI (Germany)** has a number of recommendations on the *assessment of cloud providers* and *minimum-security requirements in contracts*, which can also be adapted for other providers. **ANSSI (France) promotes the** EBIOS Risk Manager **methodology**, used by many French organizations for risk analysis, which includes the identification *of external stakeholders* and the risks arising from their relationships. ANSSI has also issued sectoral security guidelines, and some principles (e.g. the need for strong authentication and logging in industrial systems) are universally applicable. **CERT-UK** (before Brexit) developed a set of 10 steps to secure the supply chain, emphasizing on-boarding due diligence and annual risk reviews. Through cooperation networks, this knowledge has been propagated: ENISA compiles such good national practices in its reports.

- **Cybersecurity certification and quality assurance:** Voluntary security certification schemes (EU Cybersecurity Certification Framework, according to the Cybersecurity Act) are being developed at EU level. For example, there is a certification scheme for cloud services (EUCS) being adopted, which includes supply chain requirements. In the future, the purchase of certified products and services at EU level will become a good practice – companies in the food chain will be able to choose suppliers with recognized security certifications. In addition, **the Cyber Resilience Act is envisaged**, which will require manufacturers of digital products (including industrial IoT equipment) to comply with minimum security requirements and provide support (patches) for the lifetime of the product. This initiative will raise the overall quality of equipment used in the industry, reducing the risks in the chain caused by vulnerable or unsecured products.

- **Security culture and the human factor:** A general good practice, but worth emphasizing, is *investing in awareness and training*. The European Union Agency ENISA stresses that organizations should run tailored training programs for different categories of staff – from management (to understand risks at business level, according to NIS2 requirements on management accountability) to operational employees (to recognize phishing attempts and comply with security procedures). Studies show that *human error remains the leading cause of incidents*, so no technical measure fills the need for a robust security culture. Advanced companies set up *"cyber hygiene"* programs with periodic checks (e.g. phishing simulations sent internally for training, prizes for the teams with the fewest mistakes, posters and reminders in factories regarding connection rules, etc.).

- **Collaboration and sharing of intelligence information:** At the European level there are platforms for the exchange of indicators (Threat Intelligence) such as MISP instances in which private entities also participate. A good practice is to join such communities – for example, in Romania, the DNSC centre facilitates the exchange of alerts with companies through channels such as Traffic Light Protocol (TLP) or through platforms such as RO-CSIRT. In Bulgaria, CSIRT facilitates the exchange of alerts with companies through channels such as Traffic Light Protocol (TLP). Within the Directorate for Network and Information Security at the Ministry of Electronic Governance, an Information Sharing and Analysis Centre (ISAC) has been established. This centre plays a crucial role in:

    - Analysing cyber threats on a national level;
    - Sharing Indicators of Compromise (IoCs) with the other key cybersecurity authorities;
    - Supporting national coordination on cyber threat intelligence.

- Information sharing is conducted in accordance with the Traffic Light Protocol (TLP) to ensure appropriate handling and dissemination of sensitive data. The Centre also handles classified information, including NATO and EU classified material, in compliance with applicable security regulations and protocols.
- Additionally, the Directorate operates a Security Operations Centre (SOC) responsible for monitoring malicious cyber activities and proposing the inclusion of relevant IoCs into blocklists maintained internally by each institution.
- The National CERT (Computer Emergency Response Team) is also situated within this Directorate. It collaborates with domestic and international stakeholders to respond to incidents and share critical threat intelligence. The CERT operates a MISP (Malware Information Sharing Platform) instance to facilitate the structured exchange of threat data with partners and support proactive cybersecurity efforts.

Large companies can also use commercial cyber intelligence services to be alerted if, for example, hackers' forums are discussing targeting the food sector or zero-day exploits appear that could affect their infrastructure.

In summary, good European practices call for a **holistic approach**: combining international standards with agency guidelines, adapting them to their own context, and actively participating in the security ecosystem (through certification, exchange of information, cooperation). Entities in the food supply chain in Romania and Bulgaria should aspire to implement a **cybersecurity framework** equivalent to those of companies in Western European states. NIS2 sets a mandatory minimum, but in practice companies can and should go beyond it – every proactive measure (be it additional auditing of suppliers, or doubling training for maintenance technicians) can prevent a costly incident. And alignment with recognized standards (ISO, NIST, etc.) also has business benefits: it makes it easier to demonstrate compliance, gains the trust of partners and can be an advantage when accessing international markets.

Model policies and procedures (practical tools)

In order to move from theory to practice, organizations need to translate requirements and good practices into internal operational documents – policies, procedures, standards, formulations. These tools guide the concrete actions of the staff and ensure the repeatability of security processes. Next, we present **indicative models** of policies and procedures relevant to risk management in the food supply chain. These models can serve as a starting point in developing your own documentation, which will then be adapted to the specifics of each organization.

Supply Chain Cybersecurity Policy (Example Structure)

Such a policy defines the organization's commitments to the security of relationships with suppliers and partners and establishes the framework for the assessment and control of external risks. Key elements can be:

- **Purpose and scope:** E.g. *"This policy sets out cybersecurity requirements applicable to XYZ Company's supply chain, including relationships with suppliers, distributors, IT service providers, and other third parties that manage critical data or systems."*
- **Responsibilities:** Nomination of a *Supply Chain Security Officer* (maybe CISO or a risk manager) who oversees the implementation of the policy. Also, the involvement of the Procurement (for the inclusion of security requirements in contracts), Legal (for clauses) and Operations departments.

- **Security requirements for suppliers:** List of the main expectations from suppliers. Example: *"All critical suppliers must be ISO/IEC 27001 certified or demonstrate an equivalent level of security controls. Providers accessing the company's internal networks must comply with our password and MFA policy. Software vendors will periodically provide attestations on vulnerability management (patch management) and promptly notify us of any security breach that may affect us."*.

- **Supplier risk assessment process:** Commitment to conduct on-boarding and periodic (e.g. annual) security assessments for suppliers in critical and important categories. Specifying that assessments are based on a *standard security questionnaire* (see supplier checklist below) and possibly on independent audit for highly critical ones.

- **Classification of suppliers by risk levels:** E.g.: Tier 1 (critical) – services without which operations stop, Tier 2 (significant) – medium impact, Tier 3 (non-critical). The policy may say that *"For Tier 1 suppliers, audit records and continuity plans are mandatory, for Tier 2, a response to the security questionnaire is required, Tier 3 – standard minimum requirements."*

- **Security contractual clauses: Ex:** *"Contracts with suppliers who process sensitive data or have access to our systems must include confidentiality agreement, clause for notification of security incidents within 24 hours of discovery, our right to audit or request penetration tests, the obligation of the supplier to implement specified security measures (e.g.: encryption of data in transit and storage)."*

- **Third-party access management:** The policy may establish that remote access by providers (e.g., equipment maintenance) is only done through a secure VPN and with prior approval; accounts granted to third parties are reviewed quarterly; providers do not receive access to data beyond the minimum necessary (principle of least privilege).

- **Monitoring and review:** The company's commitment to monitor supplier compliance (e.g. *"We will review the security performance of critical suppliers annually and discuss issues for improvement at regular meetings")* and to review the policy itself every 2 years or at legislative changes (e.g. the appearance of a new regulation).

This policy would be approved by management and communicated both internally (to the departments involved) and externally (to suppliers, as an annex to contracts for example, to understand their expectations).

Supplier Security Assessment Checklist (Sample Checklist)

A standardized checklist or questionnaire used to evaluate suppliers (especially before contracting, but also periodically):

- **Security management system:** Does the vendor have documented security policies? Is it ISO 27001 certified or another recognized standard?

- **Governance and resources:** Is there a clear security officer at the vendor? Which team/structure manages security?

- **Access control:** How does the provider manage employee access to customer systems and data? Does it use two-factor authentication? Does it have procedures for immediate revocation of access when employees leave?

- **Infrastructure protection:** Does the provider have perimeter protection measures (firewall, IDS/IPS)? Does it encrypt sensitive data in transit and storage? Does it use antivirus/EDR solutions on workstations and servers?
- **Vulnerability management:** What process does it have for applying security updates (patch management)? How long does it take to apply critical patches after issuance? Does it periodically scan its systems for vulnerabilities?
- **Backup & Recovery:** Does it have a regular backup plan for critical data? Does it test data recovery? In the event of an attack, does it have the ability to restore its operations (is there a continuity/DR plan)?
- **Incident response:** Does the vendor have an incident response team or procedures? Has it had significant incidents in the past and how has it resolved them? Is it willing to promptly notify the affected beneficiaries?
- **Data protection and legal compliance:** If the provider processes personal or confidential data, does it comply with the GDPR and other regulations? Did they have data breaches reported to the authorities?
- **Training and awareness:** Does the supplier train its own employees in security (e.g. phishing, cyber hygiene)? How often are the training courses?
- **Data localization and sub-vendor access:** Where is the data stored (on-premises data centre, cloud, EU/non-EU)? Does it use other subcontractors for the services offered? If so, is there a flow of security requirements for them as well?
- **Additional Audit and Certifications:** Has it recently undergone a third-party security audit? Does it have SOC 2 reports (for services), or food industry-specific certifications with a safety component (e.g. a certified SCADA system for safety, etc.)?

This checklist can be sent as a form to suppliers or used internally by the evaluation team to score the supplier. The goal is to identify gaps: if, for example, the supplier does not have an incident response plan, it becomes a topic of discussion and a condition for remediation. Not all suppliers will be able to achieve 100% of the requirements, but the checklist helps *to calculate a supplier risk score* and make an informed decision (do we collaborate or not, what compensations do we need if we collaborate – e.g. we take out additional cyber insurance if the supplier is weak in a chapter).

Incident response procedure (short model)

Although we detailed the process in the previous chapter, here we present a clear, step-by-step procedural format that can be included in the internal manual:

1. **Incident detection:** Any employee or automated system that observes a suspicious event (security alerts, abnormal equipment behaviour, unusual error messages, etc.) must immediately inform the IT/CSIRT team (internal emergency phone, e-mail security... or the ticketing platform dedicated to incidents). The time and nature of the observation will be noted.
2. **Initial assessment and classification:** The CSIRT (or IT on-call) quickly evaluates the information to determine if it is a **confirmed security incident** and associates it with a severity (Critical, Major, Minor) based on the potential impact. If it is a *critical incident* (e.g. production system stopped by malware, unauthorized access to recipe data, ongoing attack), the CSIRT manager and the relevant management (operational management) are immediately alerted.

3. **Containment:** The CSIRT team executes the necessary isolation actions according to *predefined Playbooks*. Ex: in case of ransomware – disconnecting the factory network from the central VPN, turning off specific switches; in case of detected exfiltration – blocking connections from the respective IP, suspension of compromised account, etc. The safety of personnel and equipment is taken into account (e.g. do not suddenly stop an industrial system if it can cause physical damage – switch to controlled manual mode).

4. **Internal notification and extended team activation:** An internal incident message (e.g. via SMS or phone) is sent to the members of the response team (including production, IT, management representative). If the incident disrupts production or deliveries, the logistics/sales department is also notified to activate its continuity measures (e.g. informing customers of possible delays – synchronization with BCP's plan).

5. **Investigation and eradication:** Technical specialists analyse the causes: collect logs, malware samples, identify the intrusion vector. At the same time, malicious components are eliminated – malware deletion, vulnerability patching, compromised password change. If internal resources are exceeded, an external incident response partner is contacted (if there is a contract) or help is requested from the national CERT. All actions and discoveries are documented.

6. **System Recovery:** Once the threat is deemed to have been removed, it restores the affected systems from clean backups (or rebuilds from scratch, as the case may be). The functionality and integrity of the data are tested. These systems are intensively monitored after recommissioning to detect any signs of attacker persistence.

7. **External communication and notifications:** If the incident is significant (NIS2 criteria), in parallel with the above steps, the NIS officer prepares the notification to the competent authority (DNSC/CERT) according to the established form. Communications can also be issued to chain partners if they are directly affected (e.g. "supplier X – announcement: our systems are temporarily unavailable, you cannot send us orders electronically, use your phone"). For the media/public, only the communication department issues statements approved by management, if applicable, maintaining transparency and control of information.

8. **Incident Closure and Post-Incident Report:** The CSIRT team leader decides when the incident can be declared closed (criteria: systems are restored, there is no more malicious activity, operations are back to normal or close). A debrief meeting is convened in which the share price is analysed. The final report of the incident is completed, which includes description, impact, root causes, timeline, measures taken, costs, and lessons learned. The report is sent to top management and, if required by legislation (NIS2), to the authorities. Any recommendations (e.g. "firewall upgrade required", "additional personal training") are recorded and transformed into concrete improvement actions.

9. **Documentation update and follow-up:** Security procedures, response or continuity plans are updated according to what is found (if an unforeseen situation has occurred in the current plan, it is now added). The team responsible follows the implementation of all corrective measures (e.g. if additional network segmentation has been decided, the project must be completed and verified).

This procedure shall be distributed to the relevant personnel and practiced periodically (through incident simulations). Each team member thus knows what to do when a real incident occurs.

Business continuity plan (condensed structure)

Although the chapter on continuity has extensively detailed the contents of a BCP, here is a **typical skeleton structure** that can be used as a checklist when drawing up the plan:

- **Title & Purpose:** Business Continuity Plan for [Organization] – Ensuring the continuation of critical operations (food production and distribution) in the event of a major incident.
- **Crisis Team (BCM Team):** Name, role, contact (includes Leader – Operations Director, IT Co-leader – CIO, Security Manager, Production Manager, Logistics Manager, PR Communication).
- **Impact Analysis – Critical Processes:** (Table with) Essential Processes, RTO, RPO, Responsible Team. Ex: Milk processing – RTO 4h, RPO 1h, Production team; Retail delivery – RTO 8h, etc.
- **Continuity Measures per Process:**
  - *Production:* backup electric generator 250 kW per location; raw material stock 2 days; possibility of redistributing production to the factory in another county (50% capacity).
  - *IT (ERP, SCADA):* real-time replication servers in a secondary center at 100 km; DNS failover plan; manual procedure for issuing commands if ERP is unavailable.
  - *Logistics:* contract with backup carrier if own fleet unavailable; alternative routes in case of blocked infrastructure.
  - *Sourcing:* list of alternative suppliers for key ingredients (cocoa powder, packaging), check and pre-approved; minimum safety stock 7 days for packaging.
- **Immediate Procedures at the Onset of the Incident:** Checklist of actions in the first 0-2 hours:
  1. Ensuring the physical safety of staff.
  2. Convening the Crisis Team (phone/WhatsApp).
  3. Initial assessment of the situation – what process is affected, estimated duration.
  4. Decision to activate alternative plans (e.g. move production).
  5. Notifications: internal staff (shifts), critical partners, authorities (if major incident).
- **Crisis communication:** Message templates:
  - Internal employees: "Due to [incident], factory X is operating at a reduced capacity. Shift 2 staff are asked to stay home until further notice. We will come back with updates at 14:00."
  - To customers: "We are experiencing temporary operational difficulties and deliveries may be delayed by 1 day. We assure you that our team is continuously working on the fix. Thank you for your understanding."
  - Media (if public): Message approved by PR and management, emphasizing the control of the situation and the absence of risks to consumers (if applicable).

- **Critical Resources & Emergency Contacts:** List of generator provider, external IT technician contact, fire/police contact, DNSC contact (if major cyber incident), etc.
- **Detailed plans by major scenario:** (Annexes) Ex: Total IT Outage Plan, Factory Unavailability Plan due to physical causes, Cyber Attack Plan, Supply Chain Interruption Plan. Each with its own specific steps.
- **Procedure for returning to normal:** How to switch from fault mode to normal: reconnection of systems to the main network, synchronization of data from temporary systems, "business as usual" notification to everyone, debrief.
- **Review and testing:** When was the last test of the plan, results, when the next update is coming.

This complete plan could have dozens of pages with appendices (including standard forms, inventory lists, etc.), but the skeleton above helps with structuring. A **short roadmap plan is also recommended** – example: an A3 poster in the factory control room with "In case of a major incident: 1) call the manager; 2) turn off the power supply after procedure X if necessary; 3) etc." – simplified for immediate reaction, and the detailed plan will be consulted by the crisis team along the way.

Incident Notification Form (Template)

As we exemplified in the previous chapter, a standardized internal form helps to quickly collect the information necessary to report an incident:

- Date, time of discovery:
- Who originally reported:
- System/Department affected:
- Brief description of what is happening (symptoms):
- Actions taken so far:
- Current impact (which processes are stopped/slowed down, how many locations affected, damage estimate):
- Potential impact if it continues (risk assessment):
- Internal severity classification: (Critical/Major/Minor, according to procedure)
- Security incident? (Yes/No/Requires investigation) – If yes, the NIS notification process also starts.
- Coordination manager (name of the incident manager):
- External notifications required? (NIS Authority, Police, customers...):
- Management approval for external notification: (name, time of approval).

The form filled in in the first hours becomes the basis for subsequent communications. It can be a simple internal web page or a standard document that the security team fills in and keeps updated for the duration of the incident. It is important that this form is accessible and known by all those who may notice incidents – for example, a production shift leader should know how to fill in the basic sections (what they see, when, where) and then the IT staff add the rest.

The above models are not exhaustive, but they provide a **pragmatic starting point**. Each organization should detail them and adapt them to its own context. For example, in a smaller company, some roles overlap (the same person may also be responsible for continuity and security), so the policy and procedures will be more concise. In a large corporation, separate documents can be developed on sub-topics: General Information Security Policy, plus Supplementary Policy for Supply Chain Security; Company-wide continuity plan plus IT continuity plans and department plans, etc.

The important thing is that these documents do not remain formal, but that they are **effectively implemented**: the staff trained according to them, the processes calibrated according to them, periodically reviewed. A policy that is beautifully written, but not applied, has zero value in the face of a real attack. Instead, a set of clear procedures, practiced and understood by all, can drastically reduce confusion and chaos at critical moments, thus protecting the business.

SECTION 4. COOPERATION

Cooperation with partners and lessons to share

A particular aspect of incident response in the supply chain is **coordination with supply chain partners**. If the incident in a company has direct repercussions on partners (e.g. a supplier cannot deliver or a distributor does not receive order data), it is essential to inform them quickly and collaborate to mitigate the effects. Even when the incident does not propagate by itself (it is not malware that infects other companies), the business effects may require a synchronized reaction. Good practices recommend including communication **protocols with critical partners** in incident response plans. For example, a processor has an agreement with its major suppliers: "in the event of a cyber incident that affects your ability to deliver, please inform us as soon as possible through channel X so that we can activate our contingency plans." And vice versa, the processing company undertakes to inform suppliers if it suffers an attack that will affect its orders.

An ENISA study showed that in a significant percentage of supply-chain attacks, affected customers knew more about how the attack took place than the initially compromised suppliers (93% vs 38%), highlighting a **maturity deficit in reporting incidents at the supplier level. In other words, often vendors either don't realize how they've been** hacked or don't communicate well with customers about it, which compounds the problems. As such, there is a need for improvement in this area: the flow of incident information needs to flow better in both directions along the chain.

At European level, there are initiatives to create **sharing communities** for incidents and threats specific to the food sector. For example, in other sectors there are ISACs (Information Sharing and Analysis Center) – centers through which companies in a field confidentially share information about incidents and indicators of compromise, in order to help each other. A pan-European Food-ISAC is not yet well defined, but ENISA and national authorities encourage informal cooperation mechanisms. In Romania and Bulgaria, essential food companies can participate in meetings of the NIS Cooperation Group or sectoral round tables organized by the authorities, where the exchange of experience related to incidents is very valuable.

Incident notification form (example) – to recap, below is a brief model that can be used by food entities:

- Date/time of finding: 10.04.2025, 08:30.
- Entity: XYZ Dairy Processing Plant (Important Entity – food sector).
- Rapporteur contact: Ioan Popescu – IT Security Manager, tel..., email...
- Incident description: Ransomware detected on production servers; The operators' stations display a ransom message.
- Impact: Production in the yogurt section completely stopped (line blocked); ERP system unavailable; estimated deliveries delayed by 1 day.
- Immediate actions: Production line safely stopped manually; servers disconnected from the network; notified the internal response team; Continuity plan activated (delivery from stock).
- Suspected cause: Phishing email received the day before, possibly opened by a technician – ongoing investigation.
- Cross-border impact: Possible – deliveries to 2 BG customers will be delayed (information sent to them).
- Support required: Yes – we request known indicators about this ransomware from DNSC/CERT.

- Remarks: The name of the displayed ransomware appears to be 'XYZLocker'; No indication of exfiltration data so far.

This type of initial report would be promptly submitted to the authority. Subsequently, the company will follow internal procedures and keep the authority informed of developments (e.g.: if it discovers that quality data or recipes have been stolen, it will update the notification, especially if it involves personal data – where it falls under the GDPR, requiring notification to the data protection authority separately).

In the end, a well-managed incident response makes the difference between an unpleasant but outdated event and a devastating crisis. It is essential that entities in the food chain have prepared response plans and teams, do not hesitate to cooperate with the authorities (this can even reduce possible penalties, demonstrating good faith), and learn from each incident to strengthen their defences. Incident response is also an opportunity to test in practice the robustness of continuity plans and to strengthen relationships with partners: by going through a crisis together, the entire chain can emerge stronger and more resilient.

Cross-border cooperation

Food supply chains often operate across national borders: products and raw materials flow between countries, and companies may have a regional presence. Thus, the cybersecurity of the food chain takes on a cross-border dimension – incidents and risks do not stop at the border, and their effective countering requires international cooperation. The NIS2 Directive recognizes this reality, with a focus on **cooperation and information sharing** at EU level between Member States in order to achieve a high common level of cybersecurity. In this section, we examine the cross-border cooperation mechanisms relevant to Romania and Bulgaria in the context of the food supply chain, and how private entities can benefit from them.

European cooperation framework (NIS Cooperation Group, CSIRT Network, EU-CyCLONe)

At the strategic-political level, there is **the NIS Cooperation Group**, composed of representatives of the Member States, the European Commission and ENISA. This group develops guidelines, exchanges policy information, discusses emerging threats and can carry out **coordinated risk assessments on critical chains. For example, if there is a wave of attacks on the food sector at a European level, the Cooperation Group could initiate a joint analysis and formulate sectoral recommendations applicable in all states. Although the group operates at the government level, the results of its work (reports,** best practices) also reach private entities in the form of guides and alerts.

At the operational-technical level, the **CSIRT Network** operates, which brings together the national incident response teams (CERTs). DNSC and CERT Bulgaria are part of this network, facilitating the rapid exchange of information about incidents, indicators of compromise, attack tactics, etc. For companies, this mechanism translates into the fact that by notifying the authorities about a serious incident, the information can be shared (anonymously, if sensitive) to the CSIRT network, alerting other countries as well. In a real situation, if an attack simultaneously targets several food companies in the region (plausible scenario with ransomware or targeted attack), the CSIRT network allows coordination: for example, the DNSC can notify CERT Bulgaria and the other CERTs that threat X has appeared, transmitting the IoC (Indicators of Compromise). Thus, companies in those countries can be warned in advance. This exchange takes place in almost real time, by virtue of the relationships of trust built in the network.

A new component brought by NIS2 is **the EU-CyCLONe** (EU Cyber Crises Liaison Organization Network) – a structure designed to facilitate the high-level management of major or multiple impact cyber crises. EU-CyCLONe involves representatives at the level of national authorities (decision-makers, not just technicians), who, in situations of severe crisis (e.g. a concerted attack on food supply

chains in several countries, leading to shortages) communicate and coordinate response measures. This ensures that, if needed, there is an overall vision at EU level, mutual support is allocated (perhaps even logistically, not just informational), and coherent public messages are sent to avoid panic. Of course, EU-CyCLONe is rarely activated, only at incidents of very high magnitude, but its existence highlights the concern to treat cybersecurity in the food sector as a security of supply issue at European level.

Bilateral and regional cooperation (Romania-Bulgaria case)

Romania and Bulgaria, as neighbouring countries and EU members, have multiple reasons to work closely together in the field of cybersecurity, including for the protection of regional food chains. There are some concrete directions:

- **Direct exchange of CERT-to-CERT information:** Regardless of official EU channels, CERT National Teams have direct relations. For example, if a company in Romania reports an attack that appears to originate from infrastructure in Bulgaria, DNSC may contact CERT Bulgaria for further investigation and vice versa. Such cooperation takes place routinely within the Balkan network of CERTs.

- **Joint projects and exchange of best practices:** Romania and Bulgaria can collaborate in European projects (e.g. programs funded by the Connecting Europe Facility, Horizon Europe or cross-border cooperation funds) focused on increasing cybersecurity in the food sector. There are already initiatives such as the pilot project carried out by the DNSC in 2023-2024 on the implementation of the NIS Directive in the food production and distribution sector, in which experts from both countries participated. Such projects allow for **joint risk assessments**, simulations of cross-border incidents and the development of sectoral guidelines, benefiting from the combined expertise. At the same time, it ensures the creation of direct contacts between Romanian and Bulgarian companies in the field, facilitating the exchange of technical information or defensive tactics.

- **Regional exercises and military-civilian cooperation:** As NATO members, both countries take part in cyberattack simulation exercises (e.g. the annual Cyber Coalition exercise) where food infrastructure scenarios can also be included. In addition, there is cooperation in a regional format (Three Seas Initiative, EEA cooperation) that also addresses resilience at the infrastructure level. Cybersecurity authorities can organize *bilateral workshops* with the participation of the private sector, where they can discuss lessons learned from incidents and prevention measures. An example of good practice would be a simulated joint Romania-Bulgaria exercise on the topic "Ransomware attack on a cross-border food producer", in which to test mutual notification procedures, burden-sharing (who informs joint customers, how alternative deliveries are ensured) and coordination with the authorities of both states.

The benefits of cross-border cooperation are obvious: it increases the speed of response to regional threats, avoids duplication of efforts (each country can learn from the other's experience instead of repeating mistakes), and supply chains – which often operate in an integrated manner across borders – receive a coherent level of protection. The NIS2 Directive encourages states to communicate to each other **the identification of essential/important entities** when they have operations in more than one country, as well as to conclude mutual assistance agreements. Romania and Bulgaria, having a significant volume of bilateral agri-food trade, could establish a direct consultation channel between the DNSC and the Bulgarian equivalent for incidents affecting food chains. For example, if a large Bulgarian meat producer, an important supplier for the Romanian market, suffers an attack, the

Romanian authorities could offer analytical support or resources, knowing that the impact will also be felt internally.

In conclusion, **cross-border cooperation** acts as a force multiplier in cyber risk management. The food supply chain, as a European critical infrastructure, benefits from a common Romania-Bulgaria front in the face of threats. Whether it is harmonized policies, coordinated responses to incidents or simply information sharing, this joint effort strengthens the security of both countries and contributes to the EU's strategic objective of ensuring an uninterrupted and secure food supply for all citizens.

SECTION 5. CONCLUSIONS

The food supply chain today is at the intersection of traditional critical infrastructures and the new challenges of the digital age. On the one hand, its importance for society is unquestionable – ensuring food constantly and safely is a fundamental prerequisite for stability. On the other hand, the growing dependence on technology and the extensive interconnection makes this sector vulnerable to cyber threats that, until recently, were not on the list of major risks. This handbook highlighted that the **cybersecurity of the food chain can no longer be treated separately from operational risk management**, but must be integrated organically, from the farm and factory to the store shelf.

The adoption **of the NIS2 Directive** and its transposition in Romania (GEO 155/2024) and Bulgaria (the law being updated) represents a qualitative leap in addressing these issues. For the first time at European level, the food sector is formally recognized as part of the cybersecurity ecosystem, and operators in the field – whether they are producers, processors or distributors – are obliged to implement rigorous security measures and collaborate with the authorities in case of incidents. This legal framework provides a strong **boost**: if until now some companies were hesitant to invest in security for cost reasons, it is now becoming a requirement for compliance and even survival in the market (the threat of substantial fines of up to 2% of turnover cannot be ignored).

However, compliance for the sake of the law is not enough. As we have pointed out, **cyber risks are constantly evolving**. Attackers refine their tactics, new vulnerabilities emerge, and the geopolitical context can turn food infrastructure into targets (think of attacks orchestrated by hostile states aimed at causing shortages or panic). Therefore, organizations must adopt a proactive and anticipatory attitude, exceeding the minimum imposed by NIS2. The implementation of international standards, the close partnership with security experts, periodic resilience testing (through audits, pentest, red team exercises) and continuous improvement are the elements of a **virtuous circle** of maturity in security.

This handbook provided both theoretical and practical insight into the essentials: from the **legal framework** (what compels us to act), to **risk management** (how we identify and prioritize hazards), to **food chain-specific cybersecurity** (what are the concrete vulnerabilities and how do we address them), to **operational continuity** (how to prepare for the inevitable incident) and **incident response** (what we do when it happens), to **international cooperation** (because we are not alone in this fight) and **good practices** (the tools we have at our disposal, already tested by others). We have integrated real examples – fortunately, not very numerous so far in the food industry – which, however, serve as early warnings. The attacks on food distributors and beverage manufacturers in recent years show us that **the threat is present and current**.

Romania and Bulgaria, through their particularities, share both challenges and opportunities. Both have gone through accelerated digitalization, but they also face inherited IT infrastructures and sometimes limited resources in companies, especially in the SME area. The transposition of NIS2 comes to level the playing field – all significant players must achieve a certain level of security. Collaboration between companies, sectors and authorities will be key to raising the entire ecosystem to the required level. The DNSC in Romania and the future NIS2 authority in Bulgaria must continue to provide guidance (sectoral guides, trainings, exercises) and act as trusted partners of the industry, not just as control bodies.

At the macro level, we can say that **the security of the food supply chain is a common European problem**, and solutions are built through collective effort. Standardizing best practices, rapidly exchanging threat intelligence (through a robust pan-European network) and creating a culture of resilience will make the difference in the face of tomorrow's attacks. We don't have to wait for a catastrophic incident to act; On the contrary, our goal is to prevent it or, if it cannot be prevented, to **drastically limit its impact**.

Finally, we remember some **key messages**:

- *Awareness:* The food supply chain is exposed to significant cyber risks. The management of organizations in the field must recognize this fact and treat it as a major business risk, not as a strictly technical matter.
- *Preparation:* Implementing risk and security management structures (policies, teams, processes) is essential. We cannot improvise in the middle of a crisis; Well-put plans in place save time and resources and protect reputation.
- *Prevention through collaboration:* No entity can achieve absolute security alone. Partnerships with suppliers to improve their security, participation in information exchange communities, alignment with common standards – all this raises the level of security for the entire chain.
- *Effective response:* When incidents occur, how we react makes all the difference. Transparent communication, rapid intervention and correct reporting to the authorities reduce the damage and speed up the return to normal.
- *Continuous learning:* Cybersecurity is an ongoing process. After each exercise or incident, we draw conclusions and improve ourselves. Technology evolves, threats evolve – and we must evolve.

By applying the knowledge and tools outlined in this manual, IT managers, security officers, and all professionals involved in the food supply chain can develop a **robust cyber risk management system**. It will protect not only the economic interests of companies, but also the well-being of the citizens who depend on their services. At stake is the public's trust that, regardless of the challenges – be they pandemics or cyberattacks – **food will continue to reach everyone's table** safely.

In conclusion, food supply chain cybersecurity is not just a legal compliance requirement, but a responsibility to society. Romania and Bulgaria, together with their European partners, are taking important steps in this direction, and success will depend on the joint commitment of the authorities, the private sector and academia. This handbook hopes to have helped to consolidate knowledge and provide a useful guide for all those involved in protecting such a vital sector. Let's address these challenges with seriousness, cooperation and perseverance, for a future where cyber resilience becomes second nature to the food supply chain.

Bibliography

- Directive (EU) 2022/2555 (NIS2) (https://eur-lex.europa.eu/eli/dir/2022/2555/oj?locale=ro).
- GEO 155/2024 (Romania) – Emergency Ordinance for Cybersecurity (https://legislatie.just.ro/Public/DetaliiDocumentAfis/293121).
- ENISA – *Good Practices for Supply Chain Cybersecurity*, 2023 (https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity)
- Burcu Yasar – *Securing European Cyberspace: Is the Food and Agriculture Sector Critical?* CiTiP Blog KU Leuven (https://www.law.kuleuven.be/citip/blog/securing-european-cyberspace-is-the-food-and-agriculture-sector-critical/)
- Roaliment.ro – *The food industry, in the crosshairs of hackers: an ignored emergency*, (https://www.roaliment.ro/procesare/industria-alimentara-in-vizorul-hackerilor-securitatea-cibernetica-devine-o-urgenta-ignorata/).
- Digital Watch – *Bulgaria's Cybersecurity Law – updates and NIS2 transposition*, (https://cyberupgrade.net/blog/compliance-regulations/nis2-directive-regulations-and-implementation-in-bulgaria/)
- Ogletree Deakins – *The EU's NIS2 Directive: ... Risk Management, Incident Reporting, and Penalties*, (https://ogletree.com/insights-resources/blog-posts/the-eus-nis2-directive-covered-entities-compliance-monitoring-risk-management-incident-reporting-and-penalties/).
- ENISA – *Threat Landscape 2022* (https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022).
- NIS Cooperation Group – *Cyprus: Good practices in supply chain security*, Bowcut, S. *"Shielding the supply: Cybersecurity in food and agriculture,"*, Food and Ag-ISAC, *"Food and Agriculture Sector 2024 Cyber Threat Trends,"* report summary. (CybersecurityGuide.org)
- TXOne Networks, *"Cybersecurity in the Food Sector: How Cyberattacks Can Disrupt the Supply Chain,"* (https://www.txone.com/blog/how-cyberattacks-disrupt-food-supply-chain)
- ISA Global Cybersecurity Alliance (ISAGCA), *"Industrial Control System (ICS) Security and Segmentation,"* (https://gca.isa.org/blog/industrial-control-system-ics-security-and-segmentation)
- MEGA International, *"Risk Management Process Steps (ISO 31000),"* (https://www.mega.com/blog/what-is-risk-management-process)
- C-Risk, *"ISO 27005 – Information security risk management (overview of steps),"* (https://www.c-risk.com/blog/iso-27005)
- CISA, *"Cyber Storm VIII Exercise (Food and Agriculture Sector),"* (https://www.cisa.gov/resources-tools/programs/cyber-storm).