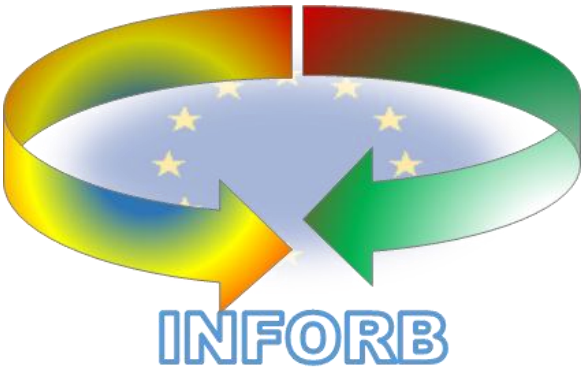

PRACTICAL GUIDE TO INCREASING CYBER SECURITY IN ORGANIZATIONS AND ENTITIES IN THE FOOD SECTOR

DELIVERABLE D2.3

Version 1.0

SUMMARY

This "Practical guide to increasing cyber security in organizations and entities in the food sector" provides a practical and structured framework for organizations in the food sector that wish to improve their cybersecurity in accordance with the requirements of the NIS 2 Directive and the specific needs of the industry. The main purpose is to increase cybersecurity, protect systems, networks, and data of organizations in the food sector, ensure compliance, align security practices with the requirements of NIS2, GDPR, and other relevant regulations, support operational resilience, develop the organizations' capacity to prevent, detect, and respond to cyber incidents, protect reputation and customer trust, and avoid security breaches that could affect the trust of customers and partners. This guide is an essential tool for organizations in the food sector that wish to improve their cybersecurity and comply with European regulations. By addressing cyber risks in a proactive and structured manner, organizations can protect critical assets, ensure food safety, and maintain the trust of customers and business partners.

PROJECT:

101128047 – INFORB – DIGITAL-ECCC-2022-CYBER-03-NIS-DIRECTIVE

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

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.

Information on document control

Settings	Value
Title of the document:	Practical guide to increasing cyber security in organizations and entities in 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) Document:	Gabriel Hîmpă, Silviu-Nicolae Dorobanțu, Gergana Rakova, Eli Kuyamova, Panayotka Panayotova
Deliverable identifier:	D2.3
Delivery due date:	30.06.2025
Delivery date:	24.06.2025
Project Manager:	Constantin CĂLIN
Document version:	V1.0
Sensibility:	PU-Public
Date:	23.06.2025

Document appraisers and appraisers

Name	Role	Action	Date
Gabriel Hîmpă	Leader of WP 2	Draft document created	11.12.2024
Gabriel Hîmpă	Leader of WP 2	Original version (DNSC)	10.04.2025
Gergana Rakova	Project Coordinator	Update version (BGMEG)	17.06.2025
Eli Kuyamova	Project and Cybersecurity Expert		
Panayotka Panayotova	BG Project Leader	Agreed BG contribution	18.06.2025
Advisory Board of Experts	Evaluation	Agreed version	20.06.2025
Constantin Călin	Project Manager	Final document agreed and delivered	24.06.2025

History of documents

Revision	Date	Created by	Brief description of the changes
V0	10.04.2025	Leader of WP 2	Document created
V0.1	10.05.2025	Leader of WP 2	Rectification of the updated document with information
V0.1.1	15.05.2025	Leader of WP 2 & Cybersecurity Expert	Update the document
V0.1.2	15.05.2025	Cybersecurity Expert	Updated English language
V0.1.3	18.06.2025	Coordinator/Project Leader	Updated English language by Bulgarian Experts
V1.0	23.06.2025	Leader of WP 2	Final document version 1

Table of Contents

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.

INTRODUCTION

This "Practical Guide for Enhancing Cybersecurity in Food Sector Organizations" (hereinafter "the Guide") has been developed under the INFORB project – "Implementation of the NIS Directive in the Food Production, Processing, and Distribution Sector in Romania and Bulgaria" – co-funded by the European Commission.

The Guide aims to support entities in addressing cybersecurity risks relevant to the food sector by aligning their practices with Directive (EU) 2022/2555 (NIS2), GDPR, and relevant standards (ISO/IEC 27001, HACCP, ISO 22000, IEC 62443). It promotes the identification of critical entities and digital infrastructures, particularly considering increasing threats to industrial control systems (ICS/SCADA), operational technology (OT), and digital supply chains.

This is the first structured resource focused on the food sector as a critical domain newly recognized under NIS2. The Guide emphasizes risk-based security, regulatory compliance, business continuity, and food safety as interconnected pillars of cyber resilience.

The main objective of the project is to identify economic entities and classify them as essential and important entities within a critically important sector, to assess and ensure cybersecurity, including the supply chain, specifically for the sector "Food Production, Processing, and Distribution" (hereinafter referred to as the "food" sector).

The guide is an important tool for economic enterprises in the food sector, helping them to timely identify their specific vulnerabilities considering the threats in the digital environment in which they operate, to continuously improve and strengthen their cybersecurity capabilities, so that they can effectively manage cybersecurity risks.

Purpose

The main purpose of this Guide is to support food sector organizations in enhancing their cybersecurity posture by:

- *Protecting digital and physical assets related to food production, processing, and distribution.*
- *Ensuring the confidentiality, integrity, and availability (CIA) of sensitive data and operational systems.*
- *Preventing, detecting, and responding to cyber threats that may compromise food safety, operational continuity, or consumer trust.*
- *Promoting the integration of cybersecurity within existing food safety frameworks such as HACCP and ISO 22000.*
- *Supporting compliance with NIS2, GDPR, and national cybersecurity legislation (e.g., OUG 155/2024).*

The Guide also aims to raise awareness, build organizational resilience, and foster a proactive cybersecurity culture among technical and non-technical personnel.

Objectives

Raising awareness of cyber risks

This objective aims to raise awareness among economic organizations in the food sector about the cyber risks specific to this field by highlighting cyber threats (e.g. ransomware attacks, data breaches, or compromise of industrial control systems) and their impact on food safety, population health, operations, as well as the reputation of the economic entity.

Critical Infrastructure Protection

A second important objective is **to identify and protect critical infrastructures** that have a significant impact on cybersecurity and the proper functioning of essential services. These may include data processing systems, distribution networks, production management systems, etc.

Providing a practical framework for action

In this context, provide clear and enforceable steps for vulnerability assessment, threat estimation, identification of likely risks, and implementation of cybersecurity risk assessment and management measures through Recommendations for the protection of information systems, networks and data, including the use of firewalls, encryption of communications, access management and regular updates.

Ensuring compliance with industry-specific regulations

This objective aims to help organizations align their cybersecurity practices with the requirements of the NIS 2 directive and other relevant regulations, as well as explain legal requirements and provide tools for incident reporting and compliance management.

Protecting the digital supply chain

Support organizations in assessing and securing the cybersecurity posture of their supply chain partners. Recommend due diligence, contractual security clauses, continuous monitoring, and alignment with ISO 28000, ISO 27036, and supplier risk scoring practices.

Increasing operational resilience

Objective: To improve the ability of organizations to prevent, detect and respond to cyber incidents.

Details: Developing incident response and business continuity plans, as well as implementing continuous monitoring practices.

Promoting education and training

Objective: Improving employees' cybersecurity awareness and skills through continuous training, phishing simulations, and role-specific education. Ensuring the inclusion of both IT and non-IT staff, especially those working with OT/ICS environments. Promoting a security culture through behavior..

Details: Providing resources and recommendations for employee training and awareness programs.

Protecting sensitive data and privacy

- **Objective**: To ensure the confidentiality, integrity and availability of sensitive data.
- **Details**: Implementing data protection measures such as encryption, regular backups, and access management.

Preventing cyberattacks and minimizing the impact

- **Objective**: To reduce the risk of cyberattacks and limit their impact on operations.

- **Details**: Recommendations for preventing attacks (e.g. using antivirus solutions, intrusion detection) and planning rapid responses.

Supporting innovation and adaptability

- **Objective**: To encourage organizations to adopt innovative cybersecurity technologies and practices.
- **Details**: Promoting the use of advanced solutions, such as artificial intelligence for early detection of threats, and adapting to new cyber risks.

Protecting customer reputation and trust

- **Objective**: To maintain and strengthen the trust of customers and business partners by ensuring a secure digital environment.
- **Details**: Avoiding security breaches that could affect reputation and transparency in incident management.

Facilitating collaboration and information sharing

- **Objective**: Foster sector-wide collaboration through threat intelligence sharing platforms, participation in ISACs (Information Sharing and Analysis Centres), and DNSC coordination. Promoting trusted channels for reporting and mutual support.
- **Details**: Promoting the sharing of threat and vulnerability information between entities.

Providing practical tools and resources

- **Objective**: To provide tools, checklists and examples of good practices to facilitate the implementation of security measures.
- **Details**: The guide includes resources that can be applied immediately in organizations, such as security policy templates or incident response plans.

Adapting to new trends and threats

- **Objective**: To help organizations stay abreast of evolving cyber threats and adapt their security strategies.
- **Details**: Providing guidance for monitoring cybersecurity trends and innovations.

The objectives of this guide are **practical, relevant and tailored to the needs of the food sector**. They aim to provide organizations with a clear and enforceable framework for improving cybersecurity while ensuring regulatory compliance and protecting critical assets. Therefore, this guide is an essential tool for building a cybersecurity culture and ensuring the resilience of organizations in an increasingly complex digital environment.

Legislative and regulatory framework

- **OUG no. 155/2024** in Romania – establishes the legal obligations for entities in critical sectors, including:
  - Articles 5 to 8: definitions of the entities concerned.
  - Articles 14 to 15: cybersecurity requirements.
  - Articles 16–18: notification of incidents to the DNSC.
- **Law no. 58/2023** in Romania – strengthens the national institutional structure for cyber defence and introduces audit and risk-sharing obligations.

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.

- **Bulgaria Cybersecurity Law that transposed the original NIS1 directive**, establishing a framework for identifying operators of essential services and regulating security measures.
- **Bulgaria Ordinance for Minimal Requirements for Network and Information Security established via the Law on Cybersecurity**. As a legal document it specifically stipulates the different domains of network and information security (cybersecurity) that each and every subject that falls under its jurisdiction, including public administration (excluding the ones listed in article 5), must adhere to. All entities, falling under its jurisdiction are required to implement and uphold the principles and technical requirements laid out in the Ordinance, including but not limited to: network and information security management; information documentation; classification of information; supply chain management; risk management; information assets management; human resources security; change management; third party relations; traffic filtering; cryptography; administration; access control; remote access; protection of software and hardware; protection against malicious software; protection of web application and servers; DNS protection; physical protection; and others. The document obliges the subjects that fall under its jurisdiction to undertake specific measures for network and information security risk management that includes adopting a documented process of regular risk assessments based on a risk assessment methodology, endorsed by the subject.
- **Regulation (EU) 2022/2554 (DORA)** – applicable to relevant collaborating financial and ICT entities.
- **DNSC orders issued in 2024**:
  - Order on **disturbance criteria and thresholds**.
  - Order on **the notification process and the PlatformaNIS2@RO (**called *NIS2@RO platform*).
  - Order on **the assessment of the risk score and the applicable CyFUN level**.

Official tools

- **NIS2@RO platform** – DNSC enrolment, information and notification.
- **Standard forms for self-assessment** – published by DNSC.
- **Standard forms for self-assessment** in Bulgaria under Bulgaria Ordinance for Minimal Requirements for Network and Information Security.

Transposition in Romania and Bulgaria

- **Transposition in Romania**
  - With the publication **of Emergency Ordinance no. 155/2024**, Romania transposed **Directive (EU) 2022/2555 (NIS2),** establishing clear requirements for the protection of networks and information systems in national civil cyberspace. Law **no. 58/2023** strengthens the cyber defence and coordination component.
- **Transposition in Bulgaria**
  - Bulgarian Ministry of E-Governance have prepared a draft amendment to the Cybersecurity Act. This document was submitted to Parliament in July 2024 for adoption, 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. The legislative process continuing towards the end of 2024 and is at the final stage of that adoption.

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.

- ➲ Until the entry into force of the NIS2 amendments, Bulgaria continues to apply the provisions of the existing law (NIS1).

General aspects about the guide

This guide is developed to support economic entities in the food sector in:

- Understanding the legal status (essential/important entity).
- The assessment of cyber risk and the application of proportionate levels of measures to minimise them.
- Alignment with international best practices (Cyber Fundamentals, ISO/IEC 27001, NIST CSF).
- The fulfilment of notification, audit and operational resilience obligations.

The following shall also be added:

- Geopolitical and economic context that increases the risk of attacks on food infrastructure.
- The need for interoperability between IT and OT systems.
- The urgent need to form an organizational culture of security among non-IT workers.

SECTION 1. BASICS OF CYBERSECURITY IN THE FOOD SECTOR

Cybersecurity in the food sector refers to the protection of information systems, networks, data and digital infrastructures used in the production, processing, distribution and marketing of food products. This involves implementing measures and practices that prevent, detect, and respond to cyber threats that could affect the organization's operations, food safety, data privacy, and reputation.

1.1. What is Cybersecurity?

1.1.1. Definition:

- Cybersecurity, also referred to as digital or IT security, encompasses policies, processes, technologies, and human factors aimed at protecting information systems, networks, devices, and data from cyber threats such as unauthorized access, data breaches, malware, or service disruption. It ensures the confidentiality, integrity, and availability (CIA) of digital assets and supports business continuity. Cybersecurity is the practice of protecting information systems, networks, devices, and data from cyberattacks, unauthorized access, and other threats.

1.1.2. Purpose:

- To preserve the confidentiality, integrity, and availability (CIA) of information and systems, ensuring uninterrupted operations, data protection, and resilience against cyber threats that could compromise food safety, supply chains, or compliance with legal obligations.
- **Official documents:** Verification of the entity's official registrations in the commercial register and other government databases to confirm the NACE codes under which the entity is registered.

1.2. Specifics of the food sector

1.2.1 Critical Assets in the food sector include:

- **Industrial Control Systems (ICS)/SCADA:** Manage automated production lines and temperature control in food processing.
- **Operational Technology (OT):** Machines and sensors used in food sorting, packaging, or storage.
- **Sensitive data:** Customer information, proprietary recipes, supplier contracts, and quality control documentation.
- **IoT devices:** Smart thermometers, flow meters, and humidity sensors connected to cloud services.
- **Supply chain management platforms:** Digital systems that coordinate procurement, logistics, and delivery.

1.2.2 Key cyber threats in the food sector include:

- **Ransomware attacks** that halt operations and encrypt critical data.
- **Supply chain attacks,** where third-party software or hardware introduces vulnerabilities.
- **Manipulation of ICS/OT systems,** which can alter temperature, hygiene, or ingredient levels, endangering food safety.
- **Data breaches** exposing customer data, intellectual property, or traceability information.
- **Fake orders and invoice fraud** targeting procurement systems.
- **Denial-of-Service (DoS/DDoS)** attacks affecting logistics platforms or inventory control.

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.

1.3. Cybersecurity principles (key components)

- **Confidentiality:** Preventing unauthorized access to sensitive data such as recipes, contracts, and health records.
- **Integrity:** Guaranteeing that production parameters, temperature logs, and batch data are accurate and unaltered.
- **Availability:** Ensuring that digital services (e.g., ICS interfaces, ERP systems, customer portals) are accessible when needed for operational continuity.

1.4. Cyber risks in the food sector

- **Ransomware:** Can disrupt production, storage, or delivery.
- **Phishing and social engineering:** May lead to unauthorized access or invoice fraud.
- **ICS/SCADA attacks:** May compromise production quality, food traceability, or hygiene controls.
- **Insider threats:** Intentional or accidental data leakage by employees.
- **Third-party vulnerabilities:** Exploits introduced via partners or suppliers.
- **Unpatched legacy systems:** Common in long-standing food factories.

1.5. Cybersecurity measures

- **Firewalls and IDS/IPS:** Filter malicious traffic and detect intrusion attempts.
- **Encryption:** Apply to sensitive data, both in storage and during transmission.
- **Access control:** Implement Role-Based Access Control (RBAC) and Multi-Factor Authentication (MFA).
- **Patch management:** Apply security updates promptly, especially for ICS and OT components.
- **Physical security:** Protect ICS devices from unauthorized physical access.
- **Network segmentation:** Isolate production networks from business or external networks.

1.6. Regulatory compliance

- **EMERGENCY ORDINANCE no. 155 of 30 December 2024 (Romania)** on the establishment of a framework for the cybersecurity of networks and information systems in the national civil cyberspace.
- **Amendment of the Cybersecurity Act (Bulgaria), No. 51-402-01-17**, submitted by the Council of Ministers to the National Assembly on December 12, 2024, adopted on first vote on February 20, 2025.
- **NIS 2**: EU Directive on the security of network and information systems, which imposes strict requirements for cybersecurity, enforces risk management and incident reporting for essential and important food entities.
- **GDPR:** General Data Protection Regulation, which sets rules for the protection of personal data.
- **ISO/IEC 27001:2022**: An international standard for information security management, framework for establishing an Information Security Management System (ISMS).
- **HACCP & ISO 22000**: Although focused on food safety, cybersecurity must integrate with these systems where digital processes (temperature monitoring, traceability) are involved.

1.7. The importance of education and awareness

- **Employee trainings**: Educating employees about cyber risks and safe practices.
- **Attack simulations**: Testing employee response to threats.

1.8. Incident response plans

- **Incident detection and analysis**: Rapid identification of suspicious activities.
- **Containment and remediation**: Limiting the impact of incidents and restoring systems.
- **Recovery and learning**: Incident analysis to improve security measures.

Conclusion

Cybersecurity is a foundational component of food sector resilience. By understanding risks, implementing layered security controls, and integrating cybersecurity with food safety systems (e.g., HACCP), organizations can ensure compliance, protect operations, and uphold consumer trust in an increasingly digital and regulated landscape.

SECTION 2. IDENTIFYING AND ASSESSING CYBER RISKS IN THE FOOD SECTOR

2.1. Risk assessment

2.1.1. Definition

- **Risk assessment** is the process of identifying, analysing and assessing the cyber risks to which an organization is exposed. This involves understanding threats and vulnerabilities, as well as the potential impact on critical assets.

2.1.2. The importance of risk assessment in the food sector

- Risk assessment in the food sector must consider the convergence of IT and OT systems, especially in automated production lines, refrigeration systems, and logistics. Beyond protecting data, assessments should evaluate how cyber risks impact food safety, regulatory compliance (e.g., ISO 22000), and business continuity. Mapping vulnerabilities in ICS/SCADA systems, IoT devices, and digital supply chains is critical to ensuring both cybersecurity and food traceability.

2.2. Steps in risk identification

2.2.1. Identification of critical assets

- The first step is to identify the organization's critical assets, such as industrial control systems (ICS), customer data, production systems, and the supply chain.

2.2.2. Identification of threats and vulnerabilities

- The next step is to identify potential threats (e.g., ransomware attacks, data breaches) and vulnerabilities (e.g., outdated software, lack of multi-factor authentication) that could affect critical assets. Risk is the probability that a threat will exploit a vulnerability, multiplied by the possible impact.

2.3. Risk assessment methods

2.3.1. Risk matrix

- A risk matrix is a tool used to assess risks, classifying them according to their likelihood of occurrence and potential impact. This allows for the prioritization of risks and the efficient allocation of resources for their management.

2.3.2. Assessment tools and techniques

- There are various risk assessment tools and techniques, including security audits, penetration tests, vulnerability scans, and assessments of compliance with security standards. Strategic assessment workshops can help identify critical business needs and vulnerabilities in networks and information systems.

2.4. Examples of risks specific to the food sector

2.4.1. Supply chain attacks

- Attacks on the digital supply chain can compromise the software or hardware used by suppliers, thus affecting the cybersecurity of entities in the food sector. Ensuring the security of the digital supply chain is a key component of the provisions of the NIS 2 Directive.

2.4.2. Compromise of industrial control systems

- Industrial control systems (ICS) are used to manage production processes in the food sector. Compromising these systems can lead to production disruptions, product quality, or even food safety issues.

2.5. Food-specific cyber threats

2.5.1. Ransomware

- Attackers encrypt an organization's data and demand a ransom to restore access. Prior to encryption, attackers exfiltrate sensitive data and threaten to leak it. HIVE ransomware has been used in cyberattacks on multiple software platforms, including Windows, Linux, and ESXI Hypervisor.

2.5.2. Data threats

- These include unauthorized access and data leaks, where cybercriminals target data sources for unauthorized access. Money remains the most common motivation for such attacks.

2.5.3. Social engineering

- Tricking victims into opening malicious documents, files, or emails, giving attackers unauthorized access to systems or services. Phishing (via email) or smishing (via text messages) are the most common. Almost 60% of security system penetrations include a social engineering component

2.5.4. Threats to availability

- Attacks that block access to data and services (DoS), increasingly affecting mobile networks and connected devices.

2.5.5. Supply chain attacks

- Supply chain attacks can compromise the software or hardware used by suppliers, thus affecting organizations in the food sector.

2.5.6. Compromise of industrial control systems (ICS)

- Attackers take control of the systems that manage production processes, which can affect food safety.

2.5.7. Code injection

- Attackers try to extract data, steal credentials, take control of the targeted web server, or promote their malicious activities through the exploitation of web application vulnerabilities.

2.5.8. Exploit-uri de tip drive-by

- The distribution of malware through drive-by exploits is almost entirely focused on compromising legitimate websites.

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.

SECTION 3. CYBERSECURITY MEASURES

To protect food business organisations from cyber threats, it is essential to implement a combination of technical, organisational and procedural measures. Here is a breakdown of the main cybersecurity measures.

3.1. Assessment of the economic dimension

3.1.1. Firewalls, Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)

- **Firewalls**:
  - **Function**: Blocks unsolicited and potentially malicious traffic between networks.
  - **Benefits**: Protects internal networks from unauthorized access and external attacks.
  - **Example**: Configuring a firewall to allow only legitimate traffic to and from the organization's network.
- **Intrusion Detection Systems (IDS):**
  - **Feature**: Monitors the network for suspicious activity and generates alerts.
  - **Benefits**: Detects attack attempts or abnormal behaviours.
- **Intrusion Prevention Systems (IPS):**
  - **Feature**: Automatically blocks detected malicious activities.

3.1.2. Regular Updates and Patch Management

- **Software Updates**:
  - **Feature**: Fixes known vulnerabilities in operating systems, applications, and firmware.
- **Patch management**:
  - **Function**: Systematic management and application of security patches.

3.2. Access management

3.2.1. Multi-factor authentication (MFA)

- **Feature**: Requires multiple forms of verification to access systems (e.g., password + code sent to your phone).
- **Benefits**: Reduces the risk of unauthorized access even if the password is compromised.
- **Example**: Implementing MFA for access to critical systems and sensitive data.

3.2.2. Role-Based Access Control (RBAC)

- **Feature**: Limits access to resources based on the user's role in the organization.
- **Benefits**: Ensures that each user has access only to the resources necessary to perform their tasks.

- **Example**: A manufacturing employee only has access to industrial control systems, not financial data.

3.3. Data protection

3.3.1. Encryption of data both at rest and in transit

- **Encryption at rest**:
  - **Function**: Protects data stored on servers, storage devices, or in the cloud.
- **Encryption in transit**:
  - **Function**: Protects data transmitted between systems or over the internet.
  - **Benefits**: Prevents data from being intercepted and read by attackers.
- **Example**: Using HTTPS to communicate with websites and APIs.

3.3.2. Regular backups and data recovery plans

- **Regular backups**:
  - **Function**: Creating backups of critical data at regular intervals.
  - **Benefits**: Ensures data recovery in case of accidental loss or deletion.
- **Data Recovery Plans**:
  - **Feature**: Defines steps to restore data and systems after an incident.
  - **Benefits**: Minimizes downtime and data loss.
- **Example**: Performing daily backups and periodically testing the recovery process.

3.4. Security of Industrial Control Systems (ICS)

3.4.1. Isolation of industrial networks (air-gapping)

- **Function**: Ensuring segmentation between OT and IT environments using firewalls, DMZs, and unidirectional gateways where appropriate. Avoid relying solely on physical air-gapping, as many food processing environments require data exchange (e.g., between ERP and ICS systems). Enforce strict access controls and monitoring between zones.
- **Benefits**: Reduces the risk of cyberattacks on industrial control systems.
- **Example**: Using dedicated networks for production equipment without an internet connection.

3.4.2. Continuous monitoring of ICS systems

- **Function**: Real-time monitoring of the activity of industrial control systems to detect anomalies.
- **Benefits**: Allows for quick identification of suspicious activity or attack attempts.
- **Example**: Implementation of specialized monitoring solutions for ICS, which detect unauthorized changes in production parameters.

3.5. Recommended additional measures

3.5.1. Employee training and awareness

- **Function**: Develop customized training programs for production line workers, warehouse staff, QA/QC personnel, and IT teams. For ICS/OT operators, integrate digital hygiene into food safety briefings (e.g., the impact of unauthorized USB devices or insecure PLC

configurations). Include simulations of real-world threats, such as fake maintenance alerts or social engineering targeting plant supervisors.

- **Benefits**: Reduces the risk of human error that can lead to security breaches
- **Example**: Regular trainings on phishing, password management, and mobile device security.

3.5.2. Incident response plans

- **Function**: Defining the steps to follow in the event of a cyber incident.
- **Benefits**: Ensures a quick and effective response to minimize impact.
- **Example**: Create a plan that includes identifying, containing, remediating, and recovering from an incident.

3.5.3. Working with partners and suppliers

- **Function**: Ensuring that partners and suppliers comply with high security standards.
- **Benefits**: Reduces supply chain risks.
- **Example**: Assessing the cybersecurity of suppliers and including security requirements in contracts.

Conclusion

Implementing these cybersecurity measures is essential to protect food business organizations from cyber threats. By combining technical solutions, clear policies, and employee education, organizations can reduce risk, ensure regulatory compliance, and maintain the trust of customers and partners.

SECTION 4. COMPLIANCE WITH NIS 2 AND OTHER REGULATIONS

For organizations in the food business, compliance with cybersecurity regulations is essential to minimize risks, protect sensitive data, and avoid penalties.

4.1. Requirements of the NIS 2 Directive

4.1.1. Obligations for Food Sector Organisations

➲ **What is NIS 2?**

- **NIS 2** (EU Directive on the security of network and information systems) is an update of the NIS Directive, which expands the scope and introduces more stringent requirements for cybersecurity.

➲ **Who is affected?**

- Essential entities include large companies in areas such as energy, transport, health or companies considered large, based on turnover, which provide essential services.
- Important entities include medium-sized organisations in areas such as manufacturing, courier or food distribution, which are essential at the country level but do not have the same degree of vulnerability.
- The Directive targets those food businesses operating exclusively in the field of logistics, wholesale distribution and large-scale industrial production and processing with a significant market share at national level

➲ **Key obligations:**

- **Implementation of appropriate security measures**:
  - Organisations must adopt technical and organisational measures to manage cyber risks.
- **Risk management**:
  - Periodic risk assessment and implementation of risk mitigation measures.
- **Notification of incidents**:
  - Companies must apply effective risk management and report serious or significant cyber incidents to the competent national authorities.
- **Cooperation with authorities**:
  - Working with national and European authorities to improve cybersecurity.
  - Entities shall take appropriate technical, operational and organisational measures to manage risks threatening the security of the information systems used for their operations.

4.1.2. Incident reporting and risk management

➲ **Incident reporting:**

- Organizations must report quickly and without undue delay any cybersecurity incident with significant impact.

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.

- Organizations classified as Essential or Important under NIS2 (based on size and relevance) must report major incidents as follows:
  - Initial notification: within 24 hours via the DNSC NIS2@RO platform.
  - Detailed technical report: within 72 hours.
  - Final remediation report: within 30 calendar days.
- Incidents include compromise of ICS/SCADA systems, food traceability disruption, data exfiltration, or DoS impacting production.
- **Examples of reportable incidents**: Ransomware attacks, data breaches, major disruptions to production systems.

➲ **Risk management:**

- Implement a risk management framework that includes:
  - Identification and assessment of risks.
  - Implementation of prevention and protection measures.
  - Continuous monitoring and improvement of the security posture.

The NIS 2 Directive addresses the security of supply chains and supplier relationships, requiring companies to address cybersecurity risks in supply chains.

4.2. GDPR and data protection

The NIS2 Directive establishes a unified legal framework to support cybersecurity in 18 critical sectors across the EU.

In addition to NIS 2 requirements, food business organizations must also comply with the General Data Protection Regulation (GDPR) to protect the personal data of customers and employees.

4.2.1. What is GDPR

➲ **GDPR** (General Data Protection Regulation) is a European regulation that sets strict rules for the protection of personal data.

➲ **Applicability**: Applies to all organisations that process personal data of EU citizens.

4.2.2. How to protect the personal data of customers and employees

➲ **Data minimization:**

- Collection and processing of only necessary personal data.

➲ **Consent:**

- Obtaining the explicit consent of individuals before processing their data.

➲ **Data Encryption**:

- Protect personal data with encryption both at rest and in transit.

➲ **Access Management**:

- Limiting access to personal data to authorized persons only.

➲ **Notification of security breaches**:

- Reporting any personal data breach to data protection authorities within 72 hours.

➲ **Privacy Policies**:

- Ensuring that both customers and employees are informed about how their data is processed.

4.3. International cybersecurity standards

4.3.1. ISO/IEC 27001

➲ **What is ISO/IEC 27001:**

- An international standard that provides a framework for implementing an information security management system (ISMS).

➲ **Benefits**:

- **Systematic approach**: Helps organizations identify, assess, and manage information security risks.
- **Compliance**: Demonstrates compliance with regulations such as GDPR and NIS 2.
- **Improved trust**: Increases the trust of customers and business partners.

➲ **Key elements**:

- **Risk assessment**: Identification of risks to information assets.
- **Policies and procedures**: Development of information security policies.
- **Monitoring and auditing**: Periodic review of the system to ensure efficiency.

4.3.2. Old standards relevant:

Organizations can use international cybersecurity standards, such as ISO/IEC 27001, to establish, implement, maintain, and continuously improve an information security management system (ISMS).

These standards provide a framework of best practices for managing information security and can help organizations demonstrate compliance with legal and regulatory requirements.

The Directive requires each Member State to adopt a national cybersecurity strategy, including policies on supply chain security, vulnerability management and cybersecurity education and awareness.

➲ **ISO/IEC 27002:** Provides guidelines and best practices for implementing information security controls

➲ **NIST Cybersecurity Framework**: A framework developed by the U.S. National Institute of Standards and Technology (NIST) that provides recommendations for managing cyber risks.

➲ **PCI DSS (Payment Card Industry Data Security Standard)**: Mandatory for organizations that process card payments, to protect credit card data.

➲ **IEC 62443:** Standard for the safety of industrial control systems (ICS), relevant to the food sector.

4.4. Ensuring compliance

4.4.1. Condition assessment

- Conducting an audit to assess the level of compliance with NIS 2, GDPR and other relevant standards.
- Identify gaps and develop an action plan to remedy them.

4.4.2. Implementation of security measures

- Adopting technical (e.g. encryption, firewalls) and organisational (policies, procedures) measures.
- Ensuring that all systems and software are updated and patched.

4.4.3. Employee training

- Organizing regular trainings to raise awareness about cybersecurity and data protection.

4.4.4. Continuous monitoring and review

- Monitoring the activity of networks and systems to quickly detect and respond to threats.
- Periodic review of policies and procedures to ensure that it remains effective and compliant.

4.5. Ongoing documentation and monitoring

4.5.1. Final qualification report

- **Detailed documentation:** Preparation of a final report documenting the entire evaluation and qualification process, including all relevant steps and conclusions.
- **Archiving of documents:** Archiving of the report and all supporting documents for future reference and for possible inspections or audits.

4.5.2. Continuous monitoring

- **Periodic Reviews:** Establishing a schedule of periodic reviews to update assessments and ensure continued compliance with the NIS2 Directive.
- **Updating information:** Keeping information up to date on the entity's economic size, organizational structure, and compliance.

This final stage of classification ensures that all relevant entities in the food business are correctly identified and in accordance with the requirements of the NIS2 Directive. The detailed assessment and qualification process contributes to the security and resilience of critical infrastructures, thus protecting food security and public health.

Romania OUG 155/2024 requirement/ Law Amending the Bulgaria Cybersecurity Law requirements	CyberFundamentals	ISO/IEC 27001:2022	NIST CSF Function	Comment
Proportionate security measures	All CyFUN Levels	A.5, A.6, A.8	Protect (PR)	Adaptation to the DNSC/BGMEG risk score
Reporting an incident (Art. 16–18, according OUG 155/2024)	RS.CO, RS. IM	A.16, A.17	Respond (RS)	24h/72h/30d

Risk assessment and self-analysis	ID.RA, ID.RM	A.6, A.15	Identify (ID)	DNSC/BGMEG Form, Annual Assessment
Audit periodic	PR. PT-1, ID.RA-3	A.9, A.10	Protect (PR)	Minimum for Important Entity
Entity Classification (DNSC/ BGMEG Score)	–	–	–	Annex 2 DNSC Order 2024/ Subsidiary regulatory framework after adoption of the Bulgaria Law on Amendments and Supplements to the Cybersecurity Law

Conclusion

Compliance with the NIS 2 Directive, GDPR, and other cybersecurity standards is essential for food business organizations. By implementing appropriate security measures, risk management, and regulatory compliance, organizations can protect critical assets, ensure data privacy, and maintain customer and partner trust.

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.

SECTION 5. SUPPLY CHAIN SECURITY

5.1. Cyber risks in the digital supply chain

5.1.1. Partner and supplier vulnerabilities.

- Conduct periodic cybersecurity risk assessments for suppliers using a standardized checklist based on ISO 27036 and ISO 28000.

  Assessment of:

  - The supplier's patch management policy.
  - Their access to your systems (VPN, APIs).
  - Their incident reporting capabilities.
  - Compliance with NCSA obligations (if located in Romania).

Include security clauses in contracts, define shared responsibilities, and require cyber insurance for critical partners.

5.2. Supply chain security measures

To minimize supply chain disruptions, companies need to dynamically adapt modes of transportation, using real-time information. Automated shipment management and shipping processes, cloud collaboration, and standardized shipping documentation can help offset these risks.

5.2.1. Assessment of partner security.

- Cyber threats pose a major risk to supply chain security, as IT networks and connected devices can create portals for cybercriminals. Over 80% of a company's cyber incidents come from supplier compromise. Thus, it is important to choose software solutions with secure cybersecurity features.
- An organizational and programmatic strategy that involves cybersecurity risk assessment and management activities, including supply chain specific risks, is essential.
- ISO 28000 is a safety management system standard, applicable in all organizations that are part of a supply chain, providing the possibility to carry out risk assessments and apply appropriate methods to keep these risks under control.

5.2.2. Contracts and security requirements for suppliers

- The implementation of a security management system contributes to increasing the level of security awareness at all levels of the organization [3]. Already implemented security standards can be integrated into one complete system, in accordance with ISO 28000.

5.3. Collaboration and information sharing

Collaborating on network security, devices, and programs can help identify and mitigate threats. Also, investments in employee training in the field of security are essential.

<u>To assess the security of partners in the supply chain, the following methods can be used:</u>

5.3.1. Monitoring supplier performance.

- Manufacturers can identify problems when and where they occur, assess their severity, provide suppliers with informed feedback, work together to find solutions, and decide whether performance issues are a reason for partnering.

5.3.2. Performance measurement

- Manufacturers measure supplier performance in several ways, including contract compliance, operational performance (quality of work, delivery times, on-time delivery, full delivery), business processes (defect prevention, inspections, regulatory compliance), and financial condition (bankruptcy risk, liquidity, profitability).

5.3.3. Use of a KPI scorecard

- Standard measures allow companies to make comparisons between suppliers. Performance monitoring works best when it is continuous, with regular reviews and checks of suppliers.

5.3.4. Supply chain risk assessment

- Identifying potential risks to the supply chain, whether they come in the form of changes in demand (due to inflation), supplier reliability (as a consequence of COVID), transport disruptions (Suez Canal), regulatory changes (Brexit) or natural disasters (climate change).

5.3.5. Collection of information

- Manufacturers collect information on the performance of their suppliers in order to control costs, reduce risks and hold them accountable for delivering quality products on time]. This information also includes data on suppliers' compliance with workers' safety, human rights and environmental legislation, mentioning any current or past violations. Some SCM applications automate this data capture and issue non-compliance alerts.

5.3.5. Review of the objectives set

- Companies measure the progress of their supply chain transparency by reviewing set goals, identifying improvements, and discussing goals they have not met (and why). Close collaboration with suppliers is essential.

5.3.5. ISO 28000 certification

- ISO 28000 certification provides a framework for organizations that operate, or rely on, any element of the supply chain to assess and implement controls to reduce security risks.

SECTION 6. CYBER INCIDENT RESPONSE

6.1. Cyber incident response plan

An incident response plan is an action manual for managing security incidents. It ensures a quick and efficient response, minimizing the impact of a security breach. A well-defined plan allows you to identify the problem, minimize the damage and reduce the cost of an attack.

6.2. Steps for incident management

Understanding the phases of incident management is essential for an effective cybersecurity response.

6.2.1. Incident detection and analysis:

- After detecting the incident and its source, you need to limit the damage.

6.2.2. Containment and remediation:

- This may involve disabling network access for infected computers and installing additional security solutions. You may also need to reset passwords or block the accounts of people who may have caused the incident.

6.2.3. Recovery and learning from incidents:

- Next is the restoration of services, validation, and testing of the system. Any compromised components should be verified, and the accounts that allowed the intrusion should be removed or blocked.

6.3. Examples of cyber incidents in the food sector

While there are no specific case studies on cyber incidents in the food sector, we can learn valuable lessons from cybersecurity incidents in general:

- **The importance of cybersecurity:** The adoption of remote work has accelerated digitalization, highlighting the need for cybersecurity.
- **Costs of Security Incidents:** Security incidents can result in significant financial losses, including substantial fines, remediation costs, and loss of business opportunities. The average cost of a data breach was $3.35 million in 2020, up 9.8% from the previous year.
- **Causes of security incidents:** Security incidents can be caused by factors such as insecure passwords, improper processes, system vulnerabilities, lack of updates, attacks on partners, malware, and human error.
- **Impact of security incidents:** Security incidents can affect any type of user, from individuals to multinational companies, leading to identity and reputation compromise, as well as money theft.
- **Prevention measures:** The implementation of automation technologies within cybersecurity services can significantly reduce the costs of a data breach and response time; Preparing for incident response through exercises and simulations can contribute to significant savings.

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 need for a proactive security system:** Opting for a proactive security system, such as a Security Operations Centre (SOC), can improve monitoring and incident response capabilities.
- **Mapping the level of cybersecurity:** The DNSC team aims to map the level of cybersecurity for entities in the food sector.
- **Fines for non-compliance with security requirements**.

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.

SECTION 7. EMPLOYEE EDUCATION AND AWARENESS

7.1. The role of employees in cybersecurity

Employees play a critical role in maintaining an organization's cybersecurity. They must be aware of potential cyber threats and take the necessary precautions to protect sensitive data. This includes being vigilant when accessing emails or using mobile devices and avoiding clicking on suspicious links or attachments. Educating and training employees on cybersecurity issues can significantly reduce the likelihood that they will fall into the trap of phishing attacks. Therefore, employees can become a first line of defence against cyberattacks, improving the overall security of the organization.

7.2. Training and awareness programs

7.2.1. Developing an effective programme:

- Designing awareness programs aligned with the roles:
  - **IT & InfoSec**: incident response, threat intelligence, SIEM monitoring.
  - **OT/ICS operators**: secure device use, remote access hygiene.
  - **Management**: risk ownership, decision-making under cyber pressure.
  - **QA & HACCP**: impact of cyber threats on food safety and recall processes.
- It must cover a wide range of topics and techniques to give employees the power to make the right decisions.
- Such a program must be a formalized process, designed to increase employees' skills and reduce the risk of a possible security breach.
- Use periodic simulations and adaptive learning platforms for maximum retention.

7.2.2. Essential topics: phishing, password management, mobile device security:

- Phishing: Training should include essential recommendations to recognize and avoid phishing attacks. Simulations and periodic testing can increase employees' understanding of the types and impact of cyberattacks.
- Password management: Employees must be trained on the importance of using strong passwords and managing them securely.
- Mobile Device Security: Training should cover the necessary precautions to protect sensitive data when using mobile devices.

7.3. Cyberattack simulations

- Cyber-attack simulations carried out periodically are an effective way to test employees' response to threats and to identify areas that need improvement in a timely manner.
- These simulations help to complement theoretical knowledge about phishing and other types of cyberattacks.
- By regularly testing employee knowledge, organizations can improve understanding and strengthen their defence against cyber threats.

SECTION 8. CONTINUOUS MONITORING AND IMPROVEMENT

8.1. The importance of continuous monitoring

Continuous monitoring is an essential element of cybersecurity strategies, especially in the food sector, where production systems, supply chain and sensitive data are exposed to significant cyber risks. It involves constantly observing and analysing networks, systems, and activities to quickly detect and respond to potential threats. Here is why it is so important.

8.1.1. Early detection of threats: Continuous monitoring allows the rapid identification of suspicious activities or attack attempts before they cause significant damage (detection of a phishing attack in the initial phase, before employees click on malicious links; identification of abnormal network behaviours that could indicate a **ransomware** or **DDoS attack**).

8.1.2. Rapid incident response: Continuous monitoring provides real-time information, allowing the security team to act immediately to limit the impact of an incident (automatically closing a network port that is scanned by an attacker; isolating an infected device to prevent the spread of malware).

8.1.3. Minimisation of downtime: In the food sector, interruptions in production or distribution can have serious financial consequences. Continuous monitoring helps prevent or limit these disruptions (Quickly detect and remediate a fault in an industrial control system (ICS) that could lead to a production stoppage).

8.1.4. Protection of sensitive data: Implement Data Loss Prevention (DLP) systems, encrypted storage, and access logging for sensitive assets such as supplier contracts, customer databases, and recipe formulas. Use anomaly detection tools to identify exfiltration attempts or unauthorized downloads.

8.1.5. Regulatory compliance: Many regulations, such as **NIS 2** and **GDPR,** require organizations to monitor system activity and report incidents on short notice. (Reporting a cyber incident to the competent authorities within 24 hours, as required by NIS 2; monitoring access to personal data to ensure compliance with the GDPR).

8.1.6. Vulnerability identification: Continuous monitoring helps identify vulnerabilities in systems and networks before they are exploited by attackers (detecting outdated software that could be exploited by an attacker; identifying a weak firewall configuration that allows unauthorized access).

8.1.7. Process of strengthening and optimizing security measures and practices: Through continuous analysis of security data, organizations can identify trends and patterns that allow them to improve their security strategies. (Identifying a type of attack that occurs frequently and implementing specific measures to prevent it; optimizing security policies based on the data collected).

8.2. Security monitoring tools

- **Attack Detection and Prevention Systems (IDS/IPS):** aimed at monitoring network traffic to detect and block suspicious activity or cyberattacks.

- **Network security monitoring solutions:** using artificial intelligence and machine learning to identify anomalous network behaviours.
- **Vulnerability management tools:** scanning systems and networks to identify vulnerabilities and recommend fixes.
- **Security Information and Event Management (SIEM) systems:** centralizing and analysing data from multiple sources to detect and respond to threats in real time.
- **IT device security tools**: protecting IT devices (such as those used in food production and distribution) from cyberattacks.
- **Data security solutions:** monitoring and protecting sensitive data against unauthorized access or loss.
- **Penetration testing tools:** simulating cyberattacks to identify weaknesses in the system.
- **Cloud security solutions**: monitoring and protecting data and applications hosted in the cloud.
- **Compliance and audit tools:** ensuring compliance with security standards (such as GDPR, ISO 27001) and facilitating security audits**.**
- **Incident response systems:** rapid identification and remediation of security incidents.
- **Supply chain security tools:** monitoring and protecting the supply chain against cyber risks.
- Security solutions for SCADA/ICS: protection of industrial control systems (SCADA) and technological operating systems (OT) used in the food industry.
- **Web application security solutions**: identifying vulnerabilities in web applications used for order management, logistics or customer service.
- **Employee training and awareness tools:** educating employees about cyber risks and security best practices.

8.3. Regular audits and evaluations

8.3.1. Employee education and awareness:

- Employees play a crucial role in maintaining an organization's cybersecurity. They must be aware of potential cyber threats and take the necessary precautions to protect sensitive data.
- This includes being vigilant when accessing emails or using mobile devices and avoiding clicking on suspicious links or attachments. Educating and training employees on cybersecurity issues can significantly reduce the likelihood that they will fall into the trap of phishing attacks. Therefore, employees can become a first line of defence against cyberattacks, improving the overall security of the organization.

8.3.2. Developing an effective programme:

- An effective cybersecurity training program is essential to change employee behaviours and educate them about cyber risks and best practices. It should cover a wide range of topics and techniques to empower employees to make the right decisions. Such a program should be a formalized process, designed to enhance employees' skills and reduce the risk of a potential security breach.

8.3.3. Key topics to be discussed:

- Phishing what: Training should include essential tips for recognizing and avoiding phishing attacks. Simulations and periodic testing can increase employees' understanding of the types and impact of cyberattacks.
- Password management: Employees must be trained on the importance of using strong passwords and managing them securely.
- Mobile Device Security: Training should cover the necessary precautions to protect sensitive data when using mobile devices.
- Cyberattack simulations are an effective way to test employees' response to threats and identify areas that need improvement.
- These simulations help to complement theoretical knowledge about phishing and other types of cyberattacks.
- By regularly testing employee knowledge, organizations can improve understanding and strengthen their defence against cyber threats.

SECTION 9: CASE STUDIES AND PRACTICAL EXAMPLES

9.1. Cyber incidents in the food sector

- The DNSC team in Romania aims to map the level of cybersecurity for entities in the food sector. Romania's energy sector accounted for 31% of all cyberattacks in 2023, followed by the transport sector with 22% and government services with 19%.
- In Romania, the daily incidence of cyberattacks is 20,000-30,000. The main industries targeted are pharmaceuticals, public administration, energy, retail and transport; In Bulgaria, in 2024, the National Computer Security Incident Response Team noted a continuous complication of the cyber situation in the country, with 8,951 signals registered. Of these, 3,775 were registered as incidents, according to the taxonomy of the European Cybersecurity Agency – ENISA. The most common causes of incidents remain the spread of malicious code (66%) and fraud (phishing) (31%). The National Computer Security Incident Response Team has sent 6,206 recommendations and instructions for resolving cyber incidents.
- Understanding the anatomy of past cyberattacks is crucial for strengthening defences and encouraging resilience in the face of future threats.

9.2. Examples of good practice

- The implementation of NIS 2 marks a new era in cybersecurity regulation within the EU, one that requires a high level of vigilance and responsibility from companies.
- A cyber incident response strategy is vital for any organization, given that three-quarters of cyberattacks that have managed to penetrate organizations' security systems have resulted in significant financial losses for companies.
- Developing strong resilience and continuously working to increase maturity in the face of cyber risk are essential for organizations. Cyber insurance should complement, not replace, a robust cybersecurity posture.
- Organizations should:
  - Undergo cybersecurity maturity assessments before applying.
  - Cover supply chain-related cyber risks (vendor-caused disruptions).
  - Include business interruption and regulatory fine clauses.
  - Align policies with NIS2 incident thresholds.

9.3. Common threats

- **Ransomware:** Attackers encrypt an organization's data and demand a ransom to restore access. In 2021, ransomware globally caused €18 billion in damage, 57 times more than in 2015.
- **Malware:** Malware, such as viruses, worms, and Trojans, can affect a system.
- **Social engineering:** Deceiving victims into providing unauthorized access to systems or services, most often through phishing. Almost 60% of security system penetrations include a social engineering component.

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.

- **Data threats:** Unauthorized access and data leaks, where the most common motivation is to obtain money.
- **Availability threats:** Attacks that block access to data and services, such as denial of service (DDoS) attacks.
- **Disinformation:** Distributing misleading information to cause fear and uncertainty.
- **Supply chain threats:** Attacks on suppliers and customers, which can be difficult to supervise due to complex systems and the multitude of suppliers.
- **Weak passwords:** Passwords that are easy to guess or crack are a major vulnerability.
- **Malicious or untrained users:** User errors and disgruntled employees can compromise security.

The sectors most frequently affected by cyber threats are public administration, digital service providers, the general public, the service sector, the financial/banking sector and the healthcare sector.

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.

SECTION 10: USEFUL RESOURCES AND TOOLS

10.1. Useful tools and resources for cybersecurity

- **Cybersecurity checklists:** Using checklists for implementing security measures.
- **Guides and reference standards:** Recommended resources for deepening knowledge.
- **Recommended software tools:** Cybersecurity solutions.

10.2. Other recommendations

- Installation of security software specially designed for mobile devices, capable of detecting and removing viruses and blocking spam messages.
- Implementing a security policy and bringing it to the attention of all employees.
- Using a VPN client to access the company network remotely and implementing 2FA/MFA authentication.
- Implementing email security measures such as SPF, DKIM and DMARC, enabling message encryption and using a Data Loss Prevention solution.
- Keeping operating systems up to date, installing an antivirus/antimalware solution and periodically scanning the system.
- Limiting the amount of publicly exposed information about the system or organization and implementing security controls, such as firewalls, encryption, and authentication.
- Backing up critical data and systems and segmenting networks to limit the movement of attackers.
- Conducting regular security audits to identify vulnerabilities.

10.2.1. Example

Playbook ransomware (synthetic)

- ***Detection:*** *Antivirus/EDR/SIEM alert.*
- ***Isolation:*** *immediate disconnection of the infected system.*
- ***Notification:*** *manager incident, CSIRT, top management.*
- ***Assessment:*** *which systems are affected? are backups intact?*
- ***DNSC notification:*** *if there is a major incident.*
- ***Fix:*** *restore from backup, updates, change passwords.*
- ***Final report:*** *lessons learned, policy review.*

🔐 *All stages must be documented and approved by management.*

Minimum security policy (example BASIC entity)

Recommended content:

- *purpose and objectives.*
- *scope.*
- *responsibilities (IT, management, users).*
- *basic controls (MFA, backup, patching).*
- *politicians de access, words, encrypt.*
- *incident response plan and annual review.*

🔄 *It is reviewed annually or after major incidents. Approval is mandatory by the executive management.*

CONCLUSION

With cyber threats on the rise and regulations tightening, food organizations need to treat cybersecurity as a strategic priority, not just a legal obligation.

This guide provides not only an interpretation of the legal requirements of the NIS2 Directive and national legislation (GEO 155/2024, Law 58/2023, Amendment of the Cybersecurity Act, No. 51-402-01-17, submitted by the Council of Ministers to the National Assembly on December 12, 2024, adopted on first vote on February 20, 2025), but also a set of practical and applicable measures that can be implemented gradually, depending on the specifics of each organization.

By raising awareness, assessing risk, implementing technical and organizational measures, and building a culture of cybersecurity, food companies can:

- Protect food safety.
- Prevent bottlenecks in the supply chain.
- Follow compliance requirements.
- Maintain the trust of customers and partners.

We invite all organizations to use this guide as **a starting point for a sustainable transformation**, strengthening their digital capacities in a responsible, resilient and adapted to current challenges.

«Cybersecurity is not just an IT goal – it is an organizational responsibility».

* * *

The official version of the Guide is in English, while at the national level, in Romania and Bulgaria, it will be published in the official languages of these countries, namely Romanian and Bulgarian.

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.