# Sector Report: Cybersecurity in the Food Sector

Authors: Müberra Yerinde1, Bengü Öztürk2, Ali Hürriyetoğlu1

*Wageningen*

Funded by the European Union

*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 European Commission-EU. Neither the European Union nor the granting authority can be held responsible for them*

## Executive Summary

The food sector is undergoing rapid digital transformation driven by Industry 4.0 technologies, including Internet of Things (IoT) sensors, cloud platforms, artificial intelligence (AI), blockchain-based traceability, and cyber-physical production systems. These technologies significantly enhance food safety by enabling real-time monitoring, predictive risk assessment, and end-to-end traceability. At the same time, the increased reliance on these technologies introduces new and often underappreciated cybersecurity risks that directly affect food integrity, supply continuity, regulatory compliance, and public trust.

This report synthesizes our findings and contextualizes them for policymakers, regulators, platform developers (such as EFRA), and food system stakeholders. It presents the current status and importance of cybersecurity in the food sector, the evolving threat landscape, relevant standards and regulatory frameworks, the potential impacts of cyber incidents on food safety, and strategic directions for building cyber-resilient food systems.

## 1. Introduction: Digital Food Systems and Cyber Risk

Over the past decade, digital technologies have become integral to food safety management across the agri-food sector. Systems supporting monitoring, traceability, documentation, and regulatory compliance increasingly rely on interconnected digital infrastructures. As a result, food safety is no longer dependent solely on physical controls, but also on the confidentiality, integrity, and availability of food safety–critical information systems. (Nankya et al., 2023)

Across the food sector, digital sensors, software platforms, and data-driven decision-support tools are routinely deployed to monitor production conditions, manage traceability, and enable risk-based food safety interventions. While these technologies enhance efficiency, transparency, and responsiveness, they also increase the sector's exposure to cyber risks by creating new dependencies on complex and interconnected information systems.

In digitally enabled operational environments, cyber incidents may result in tangible operational, regulatory, and economic consequences. Inaccurate or unavailable data, disrupted monitoring systems, or compromised digital workflows can undermine compliance efforts, delay corrective actions, and affect the continuity of food safety controls. These dynamics reflect a sector-wide convergence between cybersecurity and food safety and highlight the need to address cyber risks as an integral component of contemporary food safety governance (Goldenits and Neubauer, 2025; Fan, 2024).

## 2. Status and Importance of Cybersecurity in the Food Sector

### 2.1 Current State of Cybersecurity Maturity

Cybersecurity practices within the food sector vary across organizations. Factors such as organizational size, operational complexity, and access to technical resources influence how cybersecurity is approached and implemented in practice. Large food producers tend to adopt more formal cybersecurity policies and structured management practices, whereas small and medium-sized enterprises (SMEs) often rely on more limited and informal arrangements. (Hetzenauer, Sone and Yusoff, 2023)

Across the sector, cybersecurity responsibilities are commonly assigned to information technology (IT) functions and are not always explicitly linked to food safety operations or broader risk management processes. In many organizations, operational technology (OT), including industrial control systems, remains closely connected to enterprise IT environments, and approaches to third-party and supply-chain cybersecurity assessment differ between firms (Goldenits and Neubauer, 2025; Anton et al., 2024).

Survey-based evidence helps to contextualize these patterns. Selected results from a survey of Austrian food companies indicate that, although cybersecurity is widely recognized as an important issue, systematic cybersecurity assessments of digital business partners remain limited (see Figure 1) (Hetzenauer, Sone and Yusoff, 2023). These findings suggest that cybersecurity maturity within the food sector does not follow a uniform trajectory and is strongly shaped by organizational context.

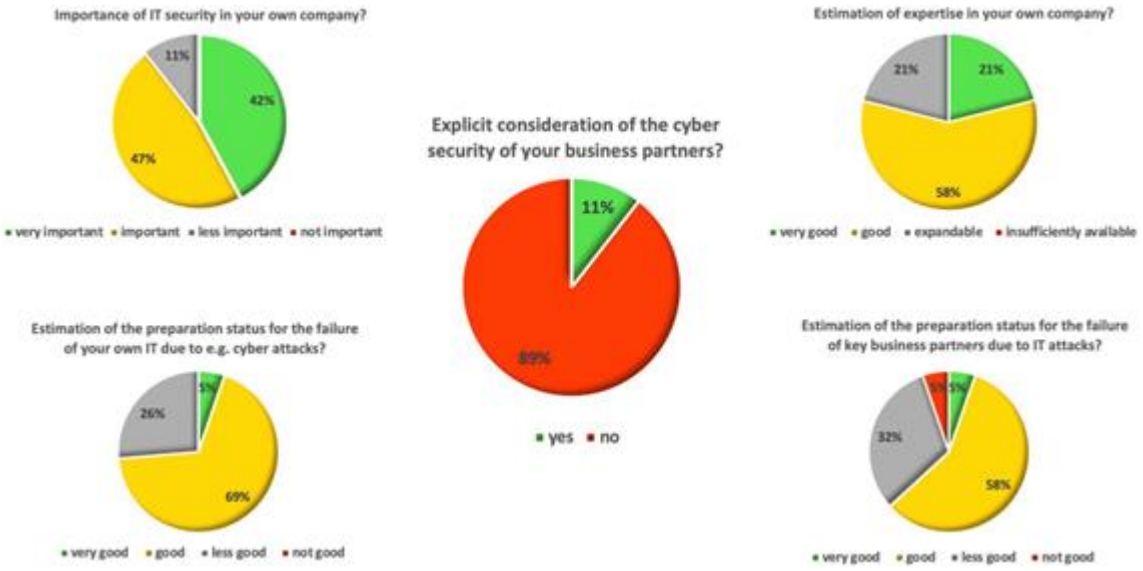


Figure 1 Overview of survey results on cybersecurity preparedness among Austrian food companies (Hetzenauer et al., 2023).

### ■ 2.2 Relevance of Cybersecurity for Food Safety Operations

The increasing reliance of food safety operations on digital technologies has elevated the operational relevance of cybersecurity throughout the food sector. Core food safety functions, including temperature monitoring, hygiene control, contamination detection, and traceability, are now largely supported by digital sensors, software platforms, and data management systems.

At the same time, automated processes and data-driven decision-support tools are routinely used to support safety-related actions such as process adjustments, alerts, and recall coordination. Given the high degree of interconnection across modern food supply chains, cyber incidents affecting a single organization or system may propagate across producers, processors, logistics providers, and retailers (Hassija et al., 2021).

From an operational perspective, incidents involving data manipulation, system unavailability, or unauthorized access can disrupt monitoring activities, delay corrective actions, and complicate regulatory compliance (Aghware and Jacob, 2025). These observations highlight the practical importance of cybersecurity for maintaining the continuity, reliability, and effectiveness of food safety operations in increasingly digitalized food systems.

## ○ 3. Digital Technologies Shaping Food Safety

### ■ 3.1 IoT and Smart Farming

IoT devices enable continuous monitoring of environmental and production conditions. While they improve early detection of hazards, they also expand the attack surface. Poorly secured sensors, gateways, or wireless networks can be exploited to manipulate data or disrupt operations.

### 3.2 Blockchain and Traceability Systems

Blockchain-based traceability systems strengthen data integrity and transparency across the food supply chain. However, vulnerabilities remain at integration points (e.g., IoT–blockchain interfaces), governance layers, and privacy management, particularly under regulations such as GDPR.

### 3.3 AI and Cloud-Based Platforms

AI models support predictive food safety analytics and decision-making. Cloud infrastructures provide scalability but introduce risks related to data breaches, misconfiguration, model poisoning, and dependency on third-party providers.

### 3.4 Integrated Supply Chain Platforms

ERP systems, national databases, and cross-border platforms create efficiency but also systemic vulnerability. A cyber incident in one node can rapidly propagate through shared digital interfaces.

## 4. Cyber Threat Landscape in the Food Safety Domain

### 4.1 Dominant Threat Types

The food sector faces a diverse and evolving set of cyber threats:

- **Ransomware:** Disrupts production, logistics, and traceability systems, often forcing shutdowns.
- **Supply-Chain Attacks:** Exploit trusted software or service providers.
- **IoT and Sensor Manipulation:** Alters environmental or quality data, potentially masking contamination.
- **Data Integrity Attacks:** Modify or falsify traceability and compliance records.
- **Insider Threats and Human Error:** Phishing, weak credentials, and misconfigurations remain major entry points.
- **Cyber-Physical Attacks:** Target ICS/SCADA systems to manipulate physical processes.

### 4.2 Emerging Risks

Emerging cyber risks in the food safety domain are increasingly shaped by the widespread adoption of advanced digital technologies, the growing convergence of biological and digital systems, and the expanding geopolitical and informational dimensions of food security. These risks are often less visible than conventional cyber threats, evolve rapidly, and are not always fully addressed by existing technical, organizational, or regulatory safeguards. Examples of such emerging risks include adversarial attacks targeting artificial intelligence models used in food safety analytics, cyber-biosecurity threats affecting laboratory and testing infrastructures, geopolitical spillover effects that expose food systems to state-sponsored or hybrid cyber activities, and coordinated misinformation or disinformation campaigns during food safety incidents.

## 5. Impact of Cybersecurity Incidents on Food Safety

Cyber incidents in the food sector have multidimensional impacts:

- **Food Integrity:** Altered process parameters or falsified data can result in unsafe products reaching consumers.
- **Operational Continuity:** Production halts and logistics disruptions can cause shortages and waste.
- **Regulatory Compliance:** Loss or corruption of records undermines audits and certifications.
- **Economic Losses:** Ransom payments, downtime, recalls, and reputational damage can be severe.
- **Public Health and Trust:** Delayed detection or response increases health risks and erodes confidence.

These impacts demonstrate that cybersecurity incidents are not merely technical events but systemic food safety crises.

## 6. Standards, Regulations, and Frameworks

### 6.1 Relevant Standards

Several international standards are relevant to food safety cybersecurity:

- **ISO 22000:** Food safety management systems.
- **ISO/IEC 27001:** Information security management systems.
- **IEC 62443:** Security for industrial automation and control systems.
- **NIST Cybersecurity Framework:** Risk-based cybersecurity management.

However, these standards are often implemented in isolation rather than as integrated frameworks.

### 6.2 Regulatory Landscape

In the European context, regulatory frameworks such as the NIS2 Directive significantly expand cybersecurity obligations for critical sectors, including parts of the food sector. While food safety regulations have traditionally focused on product integrity, hygiene, and consumer protection, cybersecurity legislation primarily addresses the security and resilience of digital systems and services, creating parallel compliance requirements that are not always fully aligned in scope, terminology, or enforcement. As digital technologies become increasingly embedded across food production, processing, and distribution, ensuring coherence between food safety regulations and cybersecurity legislation emerges as a key governance challenge, particularly for organizations operating across national borders and complex supply chains.

## 7. Toward Cyber-Resilient Food Systems

### 7.1 Technical Measures

- Secure-by-design IoT and OT architectures
- Network segmentation and zero-trust principles
- Encryption and integrity verification for food safety data
- AI-based anomaly detection and monitoring
- Secure backup, recovery, and business continuity mechanisms

### ■ 7.2 Organizational and Human Factors

- Cybersecurity awareness for food safety professionals
- Clear incident response and crisis communication plans
- Regular audits and penetration testing
- Third-party and supply-chain cybersecurity risk management

### ■ 7.3 Governance and Ecosystem Coordination

- Integration of cybersecurity into food safety management systems
- Cross-sector information sharing and threat intelligence
- Harmonization of standards and regulatory frameworks
- Data governance and access control across shared digital platforms

## ○ 8. Implications for Digital Food Safety Platforms (e.g., EFRA)

For digital food safety platforms, cybersecurity should be treated as a core design and governance requirement rather than a peripheral technical feature. Such platforms increasingly function as shared infrastructures that aggregate heterogeneous datasets, analytical tools, and machine-learning models to support food safety monitoring and decision-making. This aggregation increases both their operational value and their exposure to cyber risks. Protecting data assets, ensuring the integrity of analytical and predictive models, securing application programming interfaces (APIs), and establishing clear governance mechanisms for data sharing and access control are therefore essential. Given their role in coordinating multiple stakeholders and supporting safety-critical processes, embedding cybersecurity from the outset is fundamental to maintaining system reliability, trust, and long-term sustainability.

## ○ 9. Conclusion

Cybersecurity has become inseparable from food safety in the digital era. As food systems rely increasingly on interconnected digital infrastructures, cyber risks translate directly into safety, economic, and societal risks. This sector report demonstrates the need to reposition cybersecurity as a foundational component of food safety policy, practice, and innovation.

Building cyber-resilient food systems requires coordinated action across technology, organization, and governance. By integrating cybersecurity into food safety frameworks, data-driven food safety platforms such as EFRA, which aggregate food safety data, analytical tools, and predictive models to support risk monitoring and decision-making, can help ensure that digital transformation enhances, rather than undermines, the safety, integrity, and trustworthiness of food systems.

# References

Nankya, M., Chataut, R. and Akl, R., 2023.

Securing industrial control systems: Components, cyber threats, and machine learning-driven defense strategies. Electronics, 12(14), 3029. https://doi.org/10.3390/electronics12143029

Goldenits, G. and Neubauer, T., 2025. Taxonomy of cybersecurity considerations in agriculture. *Computers and Electronics in Agriculture*, 237, 110724. https://doi.org/10.1016/j.compag.2025.110724

Fan, X., 2024. *Between fragmentation and integration: the United Nations and global cybersecurity regulation*. Doctoral Thesis, Maastricht University. https://doi.org/10.26481/dis.20240927xf

Hetzenauer, C., Sone, T. and Yusoff, N., 2023.

Information security challenges in the digitalisation of the Austrian food industry: Assessment of food suppliers and implications. Research Report/Assessment, [unpublished preprint / ResearchGate]. https://www.researchgate.net/publication/376221797_Information_Security_Challenges_in_the_Digitalisation_of_the_Austrian_Food_Industry_Assessment_of_Food_Suppliers_and_Implications

Anton, E., Aptyka, H. and Teuteberg, F., 2024. Got milk? Got cybersecurity risks! Unraveling ransomware threats in the German dairy industry. *Organizational Cybersecurity Journal: Practice, Process and People*, 4(2), pp.105–130. https://doi.org/10.1108/OCJ-02-2024-0006

Hassija, V., Chamola, V., Gupta, V., Jain, S. and Guizani, N., 2021. A survey on supply chain security: Application areas, security threats, and solution architectures. *IEEE Internet of Things Journal*.

Aghware, F. and Jacob, L.A., 2025. Farm-level cyber security vulnerabilities: Implications for sustainable agriculture and food security in Nigeria. *Journal of African Advancement and Sustainability Studies*.

ISO, 2018. ISO 22000:2018 — Food safety management systems — Requirements for any organization in the food chain. International Organization for Standardization.

ISO/IEC, 2022. ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements. International Organization for Standardization / International Electrotechnical Commission.

IEC, 2018. IEC 62443 — Industrial communication networks — Network and system security. International Electrotechnical Commission.

NIST, 2018. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. National Institute of Standards and Technology, U.S. Department of Commerce.

European Union, 2022. Directive (EU) 2022/2555 (NIS2) on measures for a high common level of cybersecurity across the Union. Official Journal of the European Union.