White Paper: Cybersecurity and Food Safety in the Digital Era: Bridging the Gap for Data-Driven Platforms such as EFRA

Authors: Müberra Yerinde1, Bengü Öztürk2, Ali Hürriyetoğlu1

Wageningen

December 2025

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 digital transformation of the agri-food sector is fundamentally reshaping how food safety is monitored, managed, and governed. In this context, cybersecurity is no longer a peripheral technical concern, but a foundational condition for ensuring food safety in digitally mediated food systems. Advanced technologies such as Internet of Things (IoT) sensors, cloud-based data platforms, artificial intelligence (AI), and machine-learning-driven prediction systems now underpin critical food safety functions, including real-time monitoring, traceability, risk forecasting, and early warning systems. While these innovations significantly improve efficiency and transparency, they also introduce new cybersecurity risks that directly affect food integrity, supply continuity, and public trust.

Data-driven food safety platforms have emerged as central components of this transformation by aggregating datasets, documentation, and analytical tools to support risk monitoring and decision-making across the food system. The EFRA project represents one such platform, bringing together heterogeneous food safety data and machine-learning-based prediction systems, with pilot applications focusing on areas such as poultry production and pest alarm systems. While platforms of this kind address major challenges related to data sharing and predictive food safety, they also introduce distinct cybersecurity challenges associated with shared digital infrastructures, multi-stakeholder access, and the concentration of safety-critical information.

This white paper builds on the EFRA example to examine cybersecurity as a foundational component of food safety in data-driven digital environments. It outlines the current relevance of cybersecurity for modern food systems, explores how cyber incidents can affect food safety outcomes, and explains why cybersecurity should be integrated into the design, governance, and operation of digital food safety platforms in order to ensure reliability, trust, and long-term resilience.

Introduction: Food Safety in a Digital Context

Food safety has traditionally focused on preventing biological, chemical, and physical hazards that could harm consumers. Regulatory frameworks, inspection regimes, and quality management systems were designed for environments in which risks were largely physical and observable (Fung et al., 2018). However, the integration of digital technologies across the food chain has increasingly linked food safety with the protection of digital systems that generate, process, and store safety-critical information. (Alqudhaibi et al., 2024; Mubarik and Khan, 2025).

Modern food systems increasingly rely on interconnected cyber-physical infrastructures. Sensors are used to monitor temperature, hygiene, and environmental conditions; software platforms manage traceability, documentation, and regulatory compliance; and artificial intelligence (AI) models support early warning, risk assessment, and decision-making processes (Alqudhaibi et al., 2024; Mubarik and Khan, 2025). Within this digitalized environment, failures or compromises in digital systems can create undesired scenarios. Manipulated sensor data, unavailable monitoring systems, or compromised predictive models may allow unsafe conditions to go undetected, delay corrective actions, or enable contaminated products to enter the food chain, leading to broader operational disruptions (Chundhoo et al., 2021). The EFRA platform operates within this digital paradigm as a data-driven infrastructure that aggregates datasets, documentation, and machine-learning tools to support food safety monitoring and decision-making, thereby functioning as a critical information hub. As such, its reliability and trustworthiness depend not only on data quality and scientific validity but also on robust cybersecurity.

2. Status of Cybersecurity in the Food Sector

2.1 Current Maturity and Challenges

- Despite increasing digitalization, the food sector continues to exhibit relatively low cybersecurity maturity, particularly when compared to more established critical infrastructure domains (Goldenits and Neubauer, 2025; Anton et al., 2024). Cybersecurity responsibilities are often fragmented across IT departments, operational units, and external service providers, with limited integration into food safety management systems (Goldenits and Neubauer, 2025).Key challenges identified across the food sector include: Limited awareness of cyber risks among food safety professionals
- Weak separation between enterprise IT systems and operational technology (OT)
- Insufficient security controls for IoT devices and sensors
- Heavy dependence on third-party software, cloud services, and data providers
- Resource constraints, particularly among small and medium-sized enterprises

As a result, cybersecurity is frequently reactive rather than preventive, with measures introduced only after incidents occur (Food and Ag-ISAC, 2024; Food and Ag-ISAC, 2025).

2.2 Cybersecurity as an Emerging Food Safety Requirement

As food safety systems increasingly rely on digital infrastructures, cybersecurity has become an implicit prerequisite for ensuring safe and reliable food systems(Yisa et al., 2023). Digital systems supporting hazard analysis, monitoring, traceability, and predictive analytics depend on the confidentiality, integrity, and availability of data, and disruptions affecting any of these dimensions can undermine food safety outcomes by distorting risk assessments, delaying detection, or weakening regulatory oversight (Nankya et al., 2023). In highly interconnected digital food safety environments, cybersecurity risks may propagate rapidly across systems and organizational boundaries, meaning that a single vulnerability can affect multiple processes, datasets, or decision-support functions simultaneously (Yisa et al., 2023). In this context, cybersecurity must be understood as an integral component of food safety governance, closely linked to operational practices, regulatory compliance, and risk management objectives.

3. Conceptual Pathways Linking Cybersecurity and Food Safety

1. Cybersecurity influences food safety through multiple interrelated pathways that link failures in digital systems to physical food safety outcomes. **Protection of Food Integrity** Digital systems control and verify safety-critical parameters such as temperature, processing time, and contamination thresholds. Cyber manipulation of these systems can directly alter safety-critical parameters, thereby translating digital compromise into physical food safety risks.

2. **Reliability of Monitoring and Early Warning Systems**
   Machine-learning models and alarm systems used in digital food safety applications depend on trustworthy data. Cyber-attacks that distort data inputs or models can lead to false negatives or false positives, weakening early detection and delaying safety interventions.

3. **Continuity of Food Supply**
   Cyber incidents can halt production, processing, or logistics. Such disruptions may compromise cold-chain integrity, delay recalls, and increase the likelihood of unsafe products reaching consumers.

4. **Regulatory Compliance and Traceability**
   Food safety regulations rely on accurate records. Data loss or manipulation undermines traceability, weakens auditability, and limits the effectiveness of recalls and regulatory oversight.

5. **Consumer Trust and Public Confidence**
   Public trust in food systems depends on transparency and reliability Cyber incidents involving data manipulation, service disruption, or delayed responses can erode public confidence and reduce trust in food safety institutions.

4. Categories of Cyber Risks in Digital Food Safety Environments

4.1 Key Threat Categories

The cybersecurity study underpinning this white paper identifies a diverse threat landscape affecting digital food systems:

- **Ransomware Attacks:** Disrupt access to monitoring, traceability, and production systems.
- **IoT and Sensor Exploitation:** Enables attackers to falsify environmental or quality data.
- **Supply-Chain Attacks:** Exploit trusted vendors or software updates.
- **Data Integrity Attacks:** Target databases and documentation used for food safety compliance.
- **Insider Threats and Human Error:** Phishing and misconfigurations remain common entry points.
- **Cyber-Physical Attacks:** Target industrial control systems to manipulate physical processes.

4.2 Examples of Cybersecurity Events in the Food Sector

Several real-world incidents illustrate the potential impact of cyber-attacks on food safety and operations:

- **JBS Foods (2021):** A ransomware attack forced the shutdown of meat processing plants across multiple continents, disrupting supply chains and highlighting the vulnerability of OT systems. (Wikipedia, 2021)
- **Dole Food Company (2023):** Cyber incidents disrupted production and distribution, affecting food availability and logistics. (CNN, 2023)
- **Lactalis Group (2021):** France-based dairy producer experienced a cyberattack that impacted some IT systems and highlighted vulnerabilities in digital infrastructures. (BleepingComputer, 2021)

Taken together, these incidents demonstrate that cyber-attacks on food systems rarely remain confined to digital disruption, but instead translate rapidly into operational, economic, and food safety consequences across interconnected systems.

5. Impact of Cybersecurity Incidents on Food Safety

Cybersecurity incidents affect food safety on multiple levels:

- **Operational Impact:** Production shutdowns, loss of monitoring capabilities, and delayed responses.
- **Safety Impact:** Increased risk of unsafe products entering the market due to compromised controls.
- **Economic Impact:** Financial losses from downtime, recalls, and reputational damage.
- **Regulatory Impact:** Non-compliance with food safety and reporting obligations.
- **Societal Impact:** Reduced public trust and increased concern during food safety events.

In highly digitalized food safety environments, these impacts are often interconnected, meaning that a single cyber incident can simultaneously trigger operational disruption, increase food safety risks, undermine regulatory compliance, and erode public trust.

○ 6. Food Safety and Cybersecurity: Governance Considerations

Cybersecurity in food safety intersects with multiple standards and regulatory frameworks, including:

- **ISO 22000** for food safety management systems
- **ISO/IEC 27001** for information security management
- **IEC 62443** for industrial automation and control systems
- **NIST Cybersecurity Framework** for risk-based security management
- **EU NIS2 Directive** for critical infrastructure cybersecurity

While these standards and frameworks provide important guidance, the relationship between cybersecurity and different policy and disciplinary domains is commonly discussed as an ongoing governance and coordination challenge. These discussions highlight the need for more holistic and integrated approaches to cybersecurity (Fan, 2024). 7. Implications for the EFRA Platform

For EFRA, cybersecurity should be integrated as a core design and governance principle. The need for this integration is particularly pronounced given EFRA's role as a large-scale, data-driven ecosystem. The platform brings together heterogeneous and multilingual data sources, advanced analytics pipelines, federated learning approaches, and an open marketplace for data and AI services. This high degree of interoperability, automation, and user participation expands the potential attack surface and amplifies the impact of security weaknesses. Consequently, cybersecurity considerations for EFRA must extend beyond basic infrastructure protection to address data provenance, model integrity, controlled access, and trust across organizational boundaries.

Key considerations for the EFRA platform include:

- Secure storage and controlled access to datasets and documentation
- Integrity protection for machine-learning models and training data
- Secure APIs and data-sharing mechanisms
- Monitoring and logging to detect anomalies and misuse
- Clear governance for user roles, responsibilities, and incident response

By embedding cybersecurity into its architecture and governance model, EFRA can strengthen trust among stakeholders, ensure the reliability of data-driven food safety services, and support the platform's long-term sustainability within an increasingly interconnected digital food safety ecosystem.

○ 8. Toward Cyber-Resilient Digital Food Safety Systems

Building cyber-resilient food systems requires a holistic approach that combines technology, organization, and governance. Technical safeguards must be complemented by training, awareness, and cross-sector collaboration. Governance frameworks should explicitly recognize cybersecurity as a food safety issue and integrate it into regulatory and operational practices.

The findings of the underlying cybersecurity study provide a foundation for this transition, emphasizing resilience rather than purely defensive security, particularly for data-driven food safety platforms operating across organizational and regulatory boundaries.

○ 9. Conclusion

Digitalization has transformed food safety into an information-centric discipline. In this context, cybersecurity is no longer optional; it is essential for protecting food integrity, ensuring supply continuity, and maintaining public trust. The EFRA project, as a data-driven food safety platform, illustrates both the opportunities and the risks of this transformation.

By addressing the cybersecurity gap identified at the outset of the project and integrating the insights presented in this white paper, EFRA and similar initiatives can ensure that innovation in food safety is accompanied by robust digital resilience. Ultimately, embedding cybersecurity into food safety frameworks is a prerequisite for safe, transparent, and trustworthy food systems in the digital age.

References

Fung, F., Wang, H.-S. and Menon, S., 2018. Food safety in the 21st century. *Biomedical Journal*, 41(2), pp.88–95. https://doi.org/10.1016/j.bj.2018.03.003

Alqudhaibi, A., Krishna, A., Jagtap, S., Williams, N., Afy-Shararah, M. and Salonitis, K., 2024. Cybersecurity 4.0: safeguarding trust and production in the digital food industry era. *Discover Food*, 4(2). https://doi.org/10.1007/s44187-023-00071-7

Mubarik, M.S. and Khan, S.A. (eds.), 2025.
Smart Supply Chain Management: Design, Methods and Impacts. Singapore: Springer Nature. https://doi.org/10.1007/978-981-96-1333-5

Chundhoo, V., Chattopadhyay, G., Karmakar, G. and Appuhamillage, G.K., 2021.
Cybersecurity risks in meat processing plant and impacts on total productive maintenance. *Proceedings of the International Conference on Maintenance and Intelligent Asset Management (ICMIAM)*. IEEE. https://doi.org/10.1109/ICMIAM54662.2021.9715193

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

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

Food and Ag-ISAC, 2024. Annual Cyber Threat Report 2024. Food and Agriculture Information Sharing and Analysis Center.

Food and Ag-ISAC, 2025. Q1 Ransomware Analysis Report. Food and Agriculture Information Sharing and Analysis Center.

Yisa, A.G., Yisa, M.G., Osamor, J. and Yisa, M.N., 2023.
The impact of cyber threats on the global food supply chain: A focus on grain storage security. *Authorea Preprint*. https://doi.org/10.22541/au.169511622.28532721/v1

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

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

Wikipedia, 2021. JBS S.A. ransomware attack.

Available at: https://en.wikipedia.org/wiki/JBS_S.A._ransomware_attack

CNN, 2023. Dole food company cyberattack disrupts production and distribution.

Available at: https://edition.cnn.com/2023/02/22/business/dole-cyberattack

BleepingComputer, 2021. World's leading dairy group Lactalis hit by cyberattack.

Available at: https://www.bleepingcomputer.com/news/security/worlds-leading-dairy-group-lactalis-hit-by-cyberattack/

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.