txOne networks

Whitepaper April 2024

# Securing the Food Supply:
# Industrial Cybersecurity in the Food and Beverage Sector

Keep the Operation Running

# Contents

# Introduction

The food industry's shift toward smart manufacturing in line with Industry 4.0 trends has brought about significant advancements.

The integration of Information and Communication Technology (ICT) solutions into production lines enhances quality, efficiency, and compliance with the high food safety standards demanded by consumers. However, the digital transformation journey in the food and beverage sector has centered cybersecurity as a critical concern. As food and beverage companies increasingly automate and optimize operations across production, processing, distribution, and retail, new vulnerabilities emerge that cybercriminals can exploit. Attacks on these companies can disrupt food production and distribution, leading to shortages and price hikes. Moreover, they pose the risk of food contamination, exposing consumers to the threat of foodborne illnesses.

Recent events, such as the ransomware attack on meat packaging giant JBS that forced it offline, underscore the vulnerabilities within the industry. These incidents reveal a growing trend of cybercriminals targeting the food supply chain, elevating the importance of securing national agricultural sectors and food supply chains against both domestic and international threats. Cyberattacks transcend technical challenges, potentially disrupting daily life and threatening our food supply.

Despite a growing awareness of cybersecurity threats within the sector, awareness alone is not enough; the food and beverage manufacturing industry must continue to assiduously bolster its cyber defenses. The recent vulnerabilities exposed by cyberattacks call for an urgent and coordinated response to safeguard the sector from potential threats, ensuring the stability of food production and the safety of consumers. This necessitates not only the adoption of advanced cybersecurity measures but also a comprehensive strategy.

# 01 Cyber Threats to the Food and Beverage Industry

Since 2020, the food, beverage, and agriculture sectors have become targets for cyber threats at an increasing rate. 2021 stands out as the most severe year, having witnessed 65 cyber incidents in total. This uptick signifies a notable rise in cyber threats targeting this crucial sector that, despite the unprecedented severity, didn't significantly decrease in frequency in the following years of 2022 and 2023, maintaining a high level compared to pre-2020 figures.

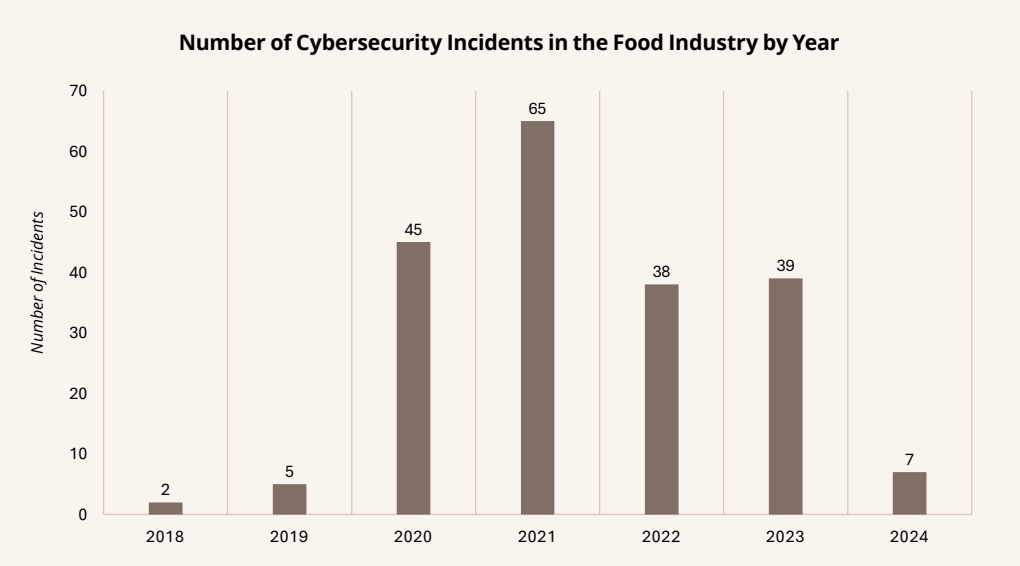



**FIGURE 1: Ransomware Attacks in the Global Food and Beverage Sector from September 2018 to February 2024** [1]

The adoption of Industry 4.0 and smart manufacturing within the food industry has brought about efficiencies and higher standards of food safety but has also introduced significant cyber vulnerabilities. The deep digital transformation across the sector has made it imperative to safeguard against the tampering of computer systems that control critical processes.

With the food, beverage and agriculture companies employing various technologies to automate and optimize operations, new vulnerabilities have emerged, making these companies attractive targets for cybercriminals. Attacks on these sectors can lead to disruptions in food production and distribution, potential food shortages, price increases, and risks of food contamination.

## Notable Ransomware Attacks in the Food and Beverage Industry

Ransomware attacks remain a significant and costly threat to the global economy, especially impacting the food and beverage industry. These criminal organizations have shifted their focus toward stealing vast amounts of data and encrypting systems, thereby doubling their chances of receiving ransom payments. Notably, in May 2021, REvil demanded an $11 million ransom from JBS, which the company paid to protect its customers.[2] Moreover, the targeted approach

by hackers, as demonstrated by the February 2023 attack on Dole PLC, aims to maximize damage by focusing on well-known companies. This incident forced the Dublin-based fruit and vegetable producer to temporarily shut down some of its North American production plants, leading to a shortage of prepackaged salad and a reported loss of about $10.5 million.[3]

| Year | Company Name | City | Country | Ransom Paid | Ransom Amount | Ransomware Strain |
|---|---|---|---|---|---|---|
| 2018 | Arran Brewery | Scotland | United Kingdom | No | $ 20,363 | Dharma |
| 2020 | Campari Group | Sesto San Giovanni | Italy | Unknown | $ 15,000,000 | Ragnar Locker |
| 2020 | Elior | Paris | France | Unknown | $ 650,000 | REvil |
| 2020 | Haldiram | Nagpur | India | Unknown | $ 750,000 | Unknown |
| 2020 | Lion Corporate | Sydney | Australia | Unknown | $ 800,000 | REvil |
| 2020 | Harvest Food Distributors (Sherwood Food Distributors) | California | United States | Unknown | $ 7,500,000 | REvil |
| 2021 | JBS USA Holdings, Inc. | Colorado | United States | Yes | $ 11,000,000 | REvil |
| 2021 | NEW Cooperative Inc. | Iowa | United States | Unknown | $ 5,900,000 | BlackMatter |
| 2021 | Schreiber Foods | Wisconsin | United States | Unknown | $ 2,500,000 | Unknown |
| 2021 | Yoshida Foods International, LLC | Oregon | United States | Yes | $ 100,000 | Unknown |
| 2022 | Rovagnati | Biassono | Italy | Unknown | $ 2,996,464 | LockBit |
| 2022 | Cici Enterprises, LP | Texas | United States | Yes | $ 400,000 | Unknown |
| 2023 | Telepizza | Madrid | Spain | Unknown | $ 543,615 | LockBit |
| 2023 | Vinovalie | Tarn | France | Unknown | $ 450,000 | NoEscape |
| 2023 | Portesa, Porcino de Teruel SA | Teruel | Spain | Unknown | $ 150,000 | Trigona |
| 2023 | Rosen's Diversified Inc | Minnesota | United States | Unknown | $ 100,000 | Medusa |
| 2024 | Kadac Australia | Braeside | Australia | Unknown | $ 100,000 | Medusa |

**TABLE 1: Notable Ransomware Attacks in the Food and Beverage Industry**

01

## Countries Most Affected by Ransomware Attacks

The top 10 affected countries illustrate the wide-reaching impact and severity of cyber threats within the food and beverage sector, with the United States experiencing the highest number of incidents at 91, followed by France with 21, and Canada with 14. This distribution showcases the extensive global reach and grave nature of cyber threats facing this crucial industry. Such a scenario urgently calls for enhanced cybersecurity defenses and heightened awareness among industry employees to secure the sector's stability and sustainable development.[4]

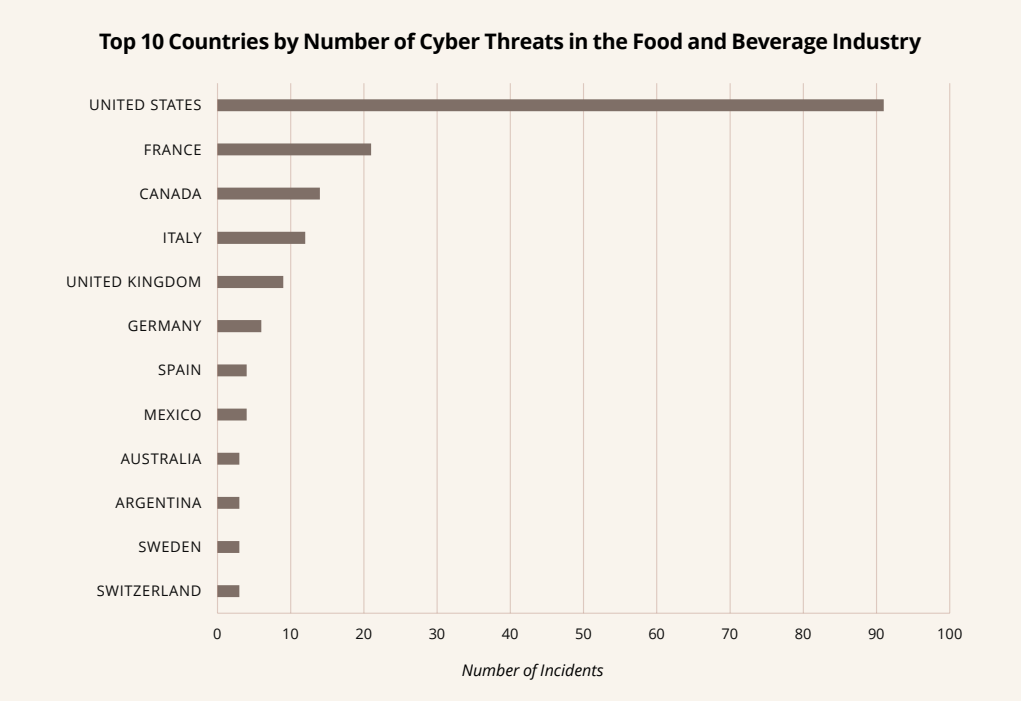



**FIGURE 2: Distribution of Ransomware Attacks in the Food, Beverage, and Agriculture Sectors by Country[1]**

## Case Study: The Ransomware Incident at JBS USA

The cyberattack on JBS USA Holdings, Inc., a subsidiary of the world's largest meat producer headquartered in Brazil, on May 30, 2021, spotlights the escalating cyber threats facing the food and beverage industry—an essential component of national and global supply chains. This incident exposes the sector's vulnerability to sophisticated cyber threats that can disrupt critical operations and impact the supply of essential goods.

In early June 2021, JBS disclosed that it had paid a ransom of approximately $11 million to shut down the cyberattack. This action, marking one of the largest ransom payments in the food industry's history, was the result of deliberations with internal and third-party cybersecurity experts brought in to assess the situation and formulate a response. JBS USA CEO Andre Nogueira described the decision as "very difficult", but necessary to prevent potential damages to customers.

The Federal Bureau of Investigation (FBI) identifies the cybercriminal group behind this attack as one of the world's most complex cybercrime organizations. The ransomware involved, REvil, has long been a pervasive threat to industrial networks, including those connected to Industrial Control Systems (ICS), accounting for a significant portion of attacks in recent years. REvil operates on a Ransomware-as-a-Service (RaaS) model, infiltrating systems through vulnerabilities, such as those in Citrix servers, or via phishing techniques, highlighting the cybercriminals' evolving strategies.[5]

By analyzing REvil's attack tactics in the ICS environment, one gains insight into the operations of this complex ransomware and its potential risks to critical infrastructure sectors. Here's an in-depth analysis based on the provided tactics and techniques:

| Tactic ID | Tactic Name | Description of REvil Strategy |
|---|---|---|
| T0828 | Productivity and Revenue Loss | Gains access to organizational networks and encrypts sensitive files used by OT devices, leading to operational disruptions and financial losses. |
| T0849 | Masquerading | Searches for the Ahnlab autoup.exe service running on the target system and injects its payload into this legitimate process to hide its malicious activities. |
| T0886 | Remote Services | Utilizes the SMB protocol to encrypt files on remotely connected file shares, demonstrating the ability to propagate across network shares. |
| T0853 | Scripting | Employs JavaScript, WScript, and PowerShell scripts for execution, using obfuscated PowerShell scripts within malicious JavaScript attachments to trigger the ransomware. |
| T0881 | Service Stop | Searches for and terminates processes listed in its configuration file to disrupt operational continuity and enable encryption routines to be completed without interference. |
| T0869 | Standard Application Layer Protocol | Sends HTTPS POST messages with randomly generated URLs for communication with remote servers, using encrypted channels to evade network detection. |
| T0882 | Operational Information Theft | Exfiltrates data to a C2 system via HTTPS POST messages before file encryption, compromising the confidentiality and integrity of sensitive operational data. |
| T0863 | User Execution | Established initially via user interaction with a malicious JavaScript file in a phishing email attachment. This drives home the importance of user awareness and training. |

**TABLE 2: REvil Strategies in OT/ICS [5]**

02

# Global Legislators Enact Cybersecurity in the Food and Beverage Industry

The U.S. Farm and Food Cybersecurity Act and the EU NIS2 Directive are landmark efforts to strengthen cyber defenses in the agriculture and food sectors. The U.S. act, proposed by Senators Gillibrand and Cotton, aims to reduce cybersecurity vulnerabilities, improve defenses, and conduct cross-sector simulations to test readiness in the event of food-related emergencies. The EU's NIS2 Directive extends cybersecurity requirements to food production, processing, and distribution, imposing risk management and reporting obligations on medium and large enterprises. Both initiatives reflect a growing recognition of the food supply chain's criticality to national and international security, mandating proactive measures against cyber threats.

# The United States Enhances Cybersecurity in Agriculture with the Farm and Food Cybersecurity Act

The U.S. Farm and Food Cybersecurity Act was initiated by Senators Gillibrand and Cotton on January 29, 2024.[6] This legislation underscores the critical importance of collaborative approaches to identifying and mitigating cyber threats, ensuring food safety and resilience, and fostering a culture of continuous improvement in cybersecurity practices across these essential sectors. Key points include:

1. Assessing the emergency response capabilities of government and private sectors.
2. Identifying and addressing vulnerabilities in the food supply chain.
3. Enhancing collaboration and information exchange among stakeholders in food production, processing, distribution, and consumption.
4. Evaluating and improving policies, plans, and resources related to food safety and cyber resilience.
5. Developing and disseminating best practices for safeguarding against cyber threats.
6. Ensuring the inclusion of all relevant parties in future exercises to enhance preparedness.

# EU's NIS2 Directive Sets Cybersecurity Standards for the Food Supply Chain

The EU NIS2 Directive represents a significant expansion from its predecessor by including the food industry within its regulatory scope, covering food production, processing, and distribution.[7] This extension addresses evolving cybersecurity threats, imposing risk management and reporting obligations on medium and large entities within the food supply chain across the EU. Small enterprises are exempt unless they are considered crucial for public security, safety, or health. This adjustment reflects an adaptive and comprehensive approach to cybersecurity, recognizing the critical importance of the food industry's resilience.

### Strengthening Responsibility and Obligations in the Food Supply Chain

The NIS2 Directive significantly updates cybersecurity responsibilities for the EU's food sector. It requires entities to register with national bodies, detailing comprehensive contact and operational information. To manage cybersecurity risks, entities must adopt measures including risk analysis, incident handling, and ensuring business continuity, all while considering cost and compliance with European and international standards. Additionally, the directive mandates prompt incident notification for significant cybersecurity events, ensuring essential services maintain their integrity and availability. This comprehensive approach aims to improve the food industry's cyber defenses by having organizations focus on these aspects of their cybersecurity posture:

02

1. Risk analysis and information system security policies
2. Incident handling
3. Business continuity
4. Supply chain security
5. Safety in acquisition, development, and maintenance
6. Policies and procedures to assess the effectiveness of cybersecurity risk management measures
7. Fundamental computer hygiene and training
8. Adequate strategies for password usage and encryption
9. Human resources security
10. Utilization of multi-factor authentication, secure voice/video/SMS communication, and secure emergency communication where applicable

## Incident Notification for Food Companies

The EU had already established incident notification obligations in Article 23 of NIS1 and declared in Article 24(1) that Operators of Essential Services (OES) should notify, without undue delay, all significant incidents affecting the availability, confidentiality, integrity, or authenticity of the network and information systems upon which their essential services rely. Thus, incorporating the stipulations from NIS1, food companies newly categorized as essential entities are now mandated to promptly report any incidents significantly impacting their provided services.[8]

| Report | What | Deadline |
|---|---|---|
| Early Warning | • Cross border impact<br>• Unlawful or malicious act | Within 24 hours upon becoming aware |
| Incident Notification | • Update to early warning data<br>• Initial assessment<br>• Severity and impact<br>• Indicators of compromise | Within 72 hours upon becoming aware |
| Intermediate Report | • Relevant status updates | Upon government request |
| Final Report | • Detailed description of the incident, including severity and impact<br>• Type of threat or root cause<br>• Applied and ongoing mitigation measures<br>• Cross border impact of the incident | No more than one month after submission of initial notification |

**TABLE 3: Incident Notification Protocols**

## Implementing Supervision and Enforcement in Food Industries

The NIS2 Directive sets forth a structured framework for supervising and enforcing cybersecurity practices within the food industry. This involves national agencies conducting inspections and, if necessary, taking corrective actions like issuing warnings or directives, and in more se-

vere cases, ordering a halt to non-compliant activities. Financial penalties are also outlined, with fines potentially reaching up to 1.4% of an entity's global revenue or 7 million euros. The directive allows for additional measures, such as suspension of certifications, to ensure compliance and thus enhance cybersecurity resilience among food sector entities.

| Feature | U.S. Farm and Food Cybersecurity Act | EU NIS2 Directive |
|---|---|---|
| Scope | Focuses on identifying and mitigating cybersecurity vulnerabilities within the U.S. food and agriculture sector. | Expands the scope to include food production, processing, and distribution as critical entities across EU member states. |
| Obligations | Mandates regular assessments of cybersecurity threats and vulnerabilities, improving private and governmental entities' defense capabilities in the food and agriculture industry. | Introduces risk management and reporting obligations for medium and large entities in the food supply chain, excluding small enterprises unless they are deemed critical. |
| Implementation | Involves collaboration between various federal departments to conduct annual cross-sector exercises simulating food-related emergencies or disruptions. | Requires entities to register with national regulatory bodies, implement comprehensive cybersecurity risk management measures, and adhere to incident notification protocols. |
| Focus on Collaboration | Encourages enhancement of security measures and resilience through inter-departmental cooperation and annual exercises. | Emphasizes the need for entities to manage cybersecurity risks and report incidents promptly, fostering a culture of cyber resilience. |
| Penalties/ Enforcement | Not explicitly mentioned; focuses more on collaborative efforts and development of best practices. | Specifies enforcement measures, including inspections, corrective actions, and administrative fines for non-compliance, with fines up to 1.4% of the previous year's global revenue or at least 7 million euros. |

**TABLE 4: Global Legislators Enact Regulations to Bolster Cybersecurity in the F&B Industry**

03

# Challenges Impacting Cyber Resilience in Food and Beverage Factories

In contrast to many industries, the food sector presents a unique complexity. It encompasses a diverse array of stages: from third-party suppliers, often farmers, through product delivery and food processing by manufacturers, to the intricate distribution networks that serve grocery stores and consumers directly. This sector's increasing automation and digitalization have made each link in the food supply chain more susceptible to threats. National and international criminal organizations frequently target the food supply chain, recognizing its critical role in society. Imagine the chaos if, during a national food shortage, hackers were to compromise the cooling systems of perishable food production and storage facilities. Just a few high-profile

attacks could incite panic among the public, leading to hoarding at grocery stores and threatening an already vulnerable food supply.

This looming danger highlights the real challenges faced by food enterprises of all sizes in their quest to fortify operational resilience. The necessity to secure the food supply chain against such threats has never been more pressing, demanding robust cybersecurity measures to protect against the manipulations of hackers aiming to disrupt the essential flow of food from farms to tables.

## Technology Dependence and Modernization of Cybersecurity

The rapid advancement of digitalization, especially in the fields of industrial automation and smart manufacturing, has enabled enterprises to process and analyze data at unprecedented speeds, thus improving production efficiency and market responsiveness. However, this development also demands that cybersecurity measures keep pace to protect the growing volume of data and connected devices from cyberattacks. Unfortunately, the update of security measures often lags behind technological advancements due to the breakneck pace of digitalization.[9] While digital technologies evolve swiftly, corresponding security measures do not receive synchronized strengthening, leading to vulnerabilities. Additionally, there's a lack of recognition of the different challenges and solutions needed for information technology versus IT/OT cybersecurity, not to mention the finer nuances of IT cybersecurity's differences from OT cybersecurity. Although they intersect technologically, information technology focuses more on the effective use and management of digital technologies, whereas cybersecurity concentrates on protecting IT/OT systems from threats and attacks.

To address these issues, we propose two strategies: first, strengthening cybersecurity investments to ensure they keep pace with technological development. This means not only investing in new technologies but also in corresponding security measures to protect these technologies from misuse. Second, it's crucial to clearly differentiate between IT/OT management and cybersecurity responsibilities, adopting professional measures for each. This requires establishing clear divisions of responsibility within the organization, ensuring that each department can adopt appropriate strategies and measures for issues within their professional domains, where network segmentation technology plays a crucial role.

## Supply Chain and Third-Party Risks

In today's increasingly interconnected business environment, supply chains and third-party service providers play a crucial role. However, as we've continuously reported in cybersecurity incidents, these links also provide new avenues for threat actors. Small and Medium Enterprises (SMEs), in particular, become targets of attacks due to their overreliance on external IT/OT services. This vulnerability arises not only because third-party services themselves can become potential security risks but also because many businesses lack internal security measures and assessments for these external risks.

The roots of this vulnerability lie in two aspects. First, enterprises often do not have sufficient resources or knowledge to establish and maintain robust internal cybersecurity systems. Second, the security measures of third-party providers may be insufficient, especially when these providers themselves fail to keep up with the latest security practices and technologies. Thus, when businesses outsource critical IT/OT services to these providers, they inadvertently expose

03

themselves to broader security threats.[10]

Given this situation, implementing the following strategies is particularly important. First, businesses need to strengthen their internal cybersecurity capabilities and awareness. This involves not only technological investments, such as deploying advanced security solutions and monitoring systems but also investing in personnel to ensure employees understand basic cybersecurity knowledge and best practices.

Second, conducting stringent security reviews and continuous monitoring of external suppliers is crucial. Enterprises should require all their IT/OT service providers to comply with specific security standards and conduct regular reviews to ensure these standards are upheld. Moreover, by implementing continuous risk assessment and monitoring programs, businesses can promptly identify and address any potential security threats.[10]

## The Challenge of Legacy Systems

On the journey toward Industry 4.0, the challenge posed by legacy systems has become increasingly obstructive. These systems are often retained for use in specific industries due to their long-term stable operation. However, over time, their security has become a matter of significant concern, especially when attempts are made to connect these systems with more modern technologies.[11]

The primary issue with these legacy systems is their vulnerability to attacks and the difficulty of updating them. Many systems run on outdated software and hardware, which, due to a lack of continuous support and updates, become ideal targets for attackers. Additionally, when businesses try to integrate these old systems with new technologies, the problem is exacerbated as this integration provides potential attackers more avenues to infiltrate the company's core network.

The difficulty in replacing or updating legacy systems is primarily due to financial considerations. For many businesses, completely replacing these systems means not only a substantial initial investment but also could lead to production disruptions and significant workflow adjustments. Therefore, despite the security risks, many companies choose to continue using these legacy systems.

Facing these challenges, there are two key strategies. First, businesses should gradually phase out these legacy systems in favor of more modern, secure technological solutions. While this may require significant investment and time, such a transition is vital for protecting the enterprise from increasingly complex cyber threats in the long run.

Second, implementing strict network segmentation and Cyber-Physical Systems Detection and Response (CPSDR) measures as an effective transitional strategy can reduce direct connections between systems. This way, even if legacy systems are attacked, it becomes difficult for attackers to penetrate the broader corporate network through these systems. CPSDR can leverage each OT environment’s unique context and behavior to produce specific situational intelligence decisions. It can not only detect potential unforeseen changes in equipment but also suppress them before they lead to instability.

## Security Awareness and Education

The importance of security awareness and education cannot be overlooked. These systems are the backbone of modern industry and infrastructure, supporting everything from food production to energy supply. However, with the increasing prevalence of "smart" devices, new security challenges have also emerged.

The problem has two main aspects. First, management and operational personnel often lack a comprehensive understanding of cybersecurity. This extends beyond traditional IT security, encompassing awareness of unique threats to OT/ICS. Second, as businesses increasingly rely on technology-driven solutions, the procurement of new technologies often overlooks security considerations. These newly introduced "smart" devices may open backdoors for cyber attackers, especially when these devices are connected to critical production and control systems.

Addressing these issues, formulating strategies becomes critically important. The first step is to strengthen cybersecurity training and education for all personnel. This means not only educating IT department staff but also those who deal directly with OT/ICS systems. Training should cover everything from basic cyber hygiene practices to advanced threat identification and response strategies, ensuring that every employee can act as a guardian of the frontline.

Second, security must be considered a core aspect when procuring new technologies and equipment. This involves more than just checking the security record of suppliers or requiring standard security features; a comprehensive security assessment process is needed to ensure that any new technology introduced does not increase the enterprise's security risks. Additionally, this assessment should consider how the equipment will integrate with existing OT/ICS environments and how these devices will be securely managed and maintained.

04

# Best Practices for Industrial Cybersecurity in the Food and Beverage Industry

In light of the evolving cybersecurity landscape, the food and beverage industry is increasingly recognizing the importance of enhancing its digital defenses. Given the sector's critical role in national and global supply chains, it's essential for companies within this domain to implement robust cybersecurity measures. Here are some key tenets for strengthening cybersecurity in the food and beverage industry:

| Security Practice | Recommended Action | TXOne Networks Assistance |
|---|---|---|
| Third-Party Validation of Cybersecurity Control Effectiveness | Cyber risk assessment for OT/ICS assets must be conducted periodically. Integral components of this assessment are evaluating risks tied to contracting with third party OT/ICS organizations and adjusting for changes in regulatory requirements. | • **Portable Inspector** can be used for risk assessment and is a valuable tool for OT customers. It performs vulnerability assessments on various operating systems, identifying and reporting the criticality of each vulnerability found. It also provides effective malware scanning and removal for standalone computers and air-gapped systems during malware scanning. **Portable Inspector (PI)** automatically collects detailed snapshots of asset data, including computer information, Windows Update status, and application lists without any additional effort required from operators.<br>• **Safe Port** assists in sanitizing external storage media within a protected and secure setting. It is suitable for use in OT environments because it is capable of inspecting external media as well as identifying and removing malware. |

| Security Practice | Recommended Action | TXOne Networks Assistance |
|---|---|---|
| Asset Inventory | Organizations need to regularly update their inventory of all IP-addressable assets, including IPv6 and OT systems for both IT and OT systems on a monthly basis at minimum. | • **Portable Inspector**: Collects details of asset data, including device information, Windows Update status, and application lists.<br>• **EdgeFire**: Enables high asset visibility through passive asset identification and IT/OT traffic communication within OT networks.<br>• **Stellar**: Provides an ICS application inventory that is informed by OT vendors. **Stellar** supports both legacy systems and modern systems. |
| Mitigating Known Vulnerabilities | In line with CISA's Known Exploited Vulnerabilities Catalog,[13] vulnerabilities in internet-facing systems should be patched or mitigated promptly, with the most critical assets taking priority.<br>For OT assets where traditional patching isn't viable or jeopardizes operational safety, alternatives like network segmentation and monitoring are employed and documented. These controls aim to prevent public internet access and reduce the risk of exploitation. | • **EdgeIPS** offers cutting-edge protection against unidentified threats by leveraging its comprehensive and up-to-date threat intelligence. Utilizing the Zero Day Initiative (ZDI) vulnerability reward program, **EdgeIPS** provides exclusive protection for your systems against undisclosed and zero-day threats. By implementing virtual patching, your network gains a robust and up-to-date initial defense against known threats (including CISA's Known Exploited Vulnerabilities Catalog). This gives users greater control over the patching process, creating a proactive defense strategy during incidents and offering additional protection for legacy systems.<br>• **Stellar** is equipped with unique application trust lists and locking technology to ensure system integrity, including Operational Lock, USB Device Lock, Data Lock, and Configuration Lock. It can be used as an alternative to help asset owners buy more time until their assets can be upgraded to the final patch provided by the Original Equipment Manufacturer (OEM). |

| Security Practice | Recommended Action | TXOne Networks Assistance |
|---|---|---|
| Network Segmentation | OT network access is tightly controlled, allowing only necessary connections such as specified IP addresses and ports. Inter-network communications between IT and OT must use intermediaries like firewalls, bastion hosts, 'jump boxes', or Demilitarized Zones (DMZs), which should be rigorously monitored and logged, allowing only approved assets. | • **EdgeFire** is an industrial next-generation firewall designed for segmenting OT networks. It can be used to monitor/secure network communications, services, and connection points between different zones, limiting them to the minimum necessary to meet operational, maintenance, and safety requirements.<br>• **EdgeIPS Pro** is a purpose-built appliance, set up for friendly, rackmounted deployment and equipped with in-depth OT protocol filtering to enable administrators to easily manage microsegmentation for a complex environment. |
| Detection of Unsuccessful (Automated) Login Attempts | Organizations should track all failed login attempts, alerting their security teams if multiple unsuccessful attempts occur quickly, such as five within two minutes. These alerts should be logged for future analysis. | • **EdgeIPS & EdgeFire** series are able to restrict access achieved through dial-up connections or connections from other sites' networks and prevent unauthorized connections. Network access can only be established when necessary and after authentication, thereby enabling businesses to reduce attacks on their OT networks.<br>• **Stellar** has the ability to detect behavioral anomalies and swiftly determine the trustworthiness of operations using an expanded ICS application and certificate library, achieving an optimal balance between performance and detection rates. Furthermore, **Stellar** employs trust list technology for the validation of software applications, preventing malicious programs from sending and receiving commands. |
| Disable Unnecessary Features by Default | The default system policy deactivates unnecessary features, like Microsoft Office macros or similar embedded code, across all devices. If there's a need to enable certain services under specific conditions, a distinct policy is put in place. This allows authorized users to request the activation of these services on specified assets. | • **Stellar** is an effective Cyber-Physical Systems Detection and Response (CPSDR) solution designed to prevent the unauthorized execution of applications that are not included in the approved list. By implementing strict controls, **Stellar** ensures that only authorized applications are allowed to run within the system. This proactive approach significantly reduces the risk of unauthorized software compromising the security and stability of the environment. |

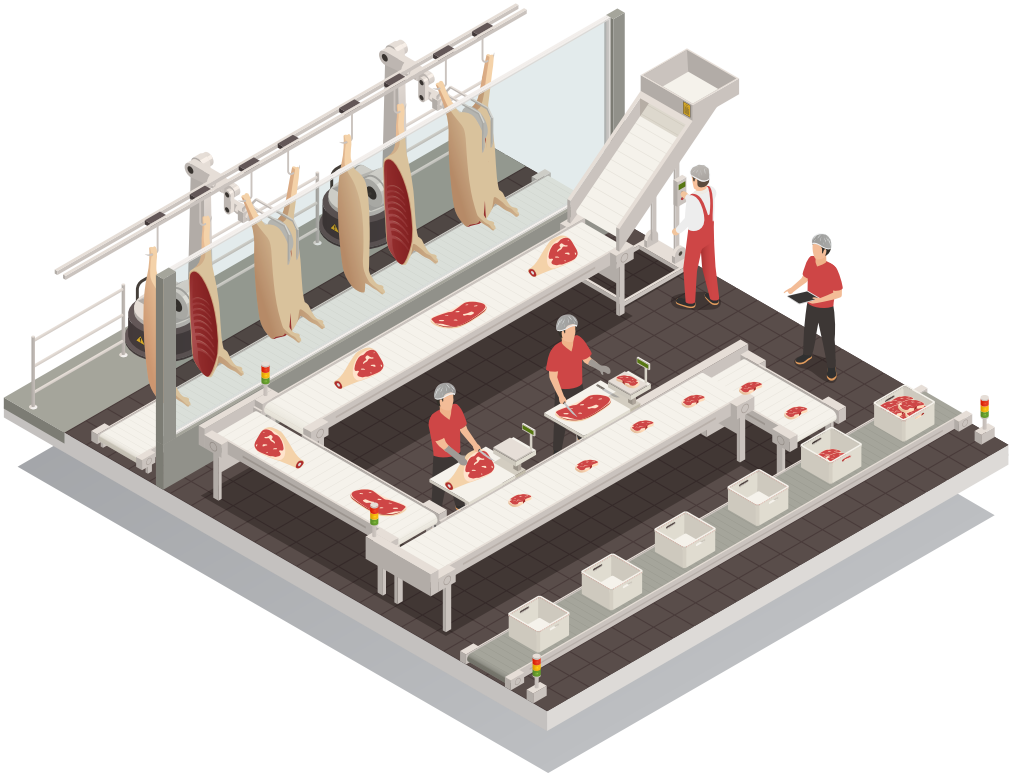
| Security Practice | Recommended Action | TXOne Networks Assistance |
|---|---|---|
| Document Device Configurations | Organizations should maintain current and comprehensive records of all critical IT and OT assets' configurations, aiding in effective vulnerability management, response, and recovery. These documents shall be regularly reviewed, updated, and monitored. | • **Stellar** implements a write protection feature to ensure the security of critical data, configurations, and files by preventing unauthorized overwriting. With **Stellar's** write protection functionality, organizations can effectively safeguard their valuable information from accidental or intentional modifications that could compromise the integrity or confidentiality of the data. This proactive measure adds an extra layer of protection, ensuring that only authorized individuals or processes have the necessary permissions to make changes, thereby reducing the risk of unauthorized overwriting and maintaining the integrity of critical data assets. |
| Document Network Topology | Organizations should keep precise documentation of their updated network topology and related information for both IT and OT networks. This documentation shall be regularly reviewed, updated, and tracked to ensure accuracy and relevancy. | • **EdgeOne** supports OT network visibility and looks into assets from specific vendors and all network elements, assets, software, and devices as well as application traffic. |
| Hardware and Software Approval Process | Establish an administrative policy or an automated procedure mandating approval prior to the installation or deployment of any new hardware, firmware, or software/versions. Organizations should maintain a risk-assessed allowlist of sanctioned hardware, firmware, and software, specifying approved versions where possible. For OT assets, it's crucial that these processes align with established change control and testing activities. | • **Stellar** can lock down sensitive assets, limit access, and preserve system resources with its simple and reliable trust list technology. Once deployed, this solution allows only the execution of approved applications necessary to daily operations, preventing the spread and execution of malware without reliance on pattern files or other resources. |

| Security Practice | Recommended Action | TXOne Networks Assistance |
|---|---|---|
| Incident Response (IR) Plans | Organizations should develop and regularly update IT and OT cybersecurity incident response plans, tailored to both common and specific threats and tactics. Drills, conducted at least annually and as true to life as possible, shall inform updates to these plans based on lessons learned. | • **SageOne** offers a multi-dimensional view of an organization's cybersecurity posture through visual representations. It provides a holistic security perspective with granularity, including the proportion of protected/unprotected assets, asset health status and anomaly detection, asset exposure level assessment, and an overview of the asset lifecycle. Asset managers can efficiently evaluate system vulnerabilities through the **SageOne** dashboard, setting priorities and response plans. This enables a macroscopic ordering of risk management priorities to effectively and accurately reduce the level of risk. |
| Log Collection | Logs focusing on access and security, such as those from intrusion detection/prevention systems, firewalls, data loss prevention systems, and VPNs, should be gathered and preserved for detection and incident response purposes, including forensics. If a critical log source like Windows Event Logging is disabled, security teams shall immediately be alerted.<br><br>In the case of OT assets with non-standard or unavailable logs, network traffic and communications between these assets and others shall be monitored and recorded. | • **Stellar** diligently records all event incidents generated by its agents, offering an invaluable additional layer of security to your systems. By logging these incidents, **Stellar** enhances your ability to monitor and analyze potential security threats, enabling proactive measures for protection.<br>• **ElementOne** seamlessly logs all events generated from **PI** and **PI Pro**. This comprehensive logging functionality ensures complete visibility of security incidents throughout your network.<br>• **EdgeOne** performs a similar function by logging all event incidents generated within your network. This powerful solution adds another layer of security by meticulously recording these events, allowing for comprehensive monitoring and analysis. |
| Secure Log Storage | Logs should be stored in a central system, such as a security information and event management tool or central database and ought to be accessible or modifiable only by authorized and authenticated users. Logs shall be stored for the duration of time determined by risk or pertinent regulatory guidelines. | • **Stellar** implements a write protection feature to ensure the security of critical data, configurations, and files by preventing unauthorized overwriting. With **Stellar's** write protection functionality, organizations can effectively safeguard their valuable information from accidental or intentional modifications that could compromise the integrity or confidentiality of the data. This proactive measure adds an extra layer of protection, ensuring that only authorized individuals or processes have the necessary permissions to make changes, thereby reducing the risk of unauthorized overwriting and maintaining the integrity of critical data assets. |

| Security Practice | Recommended Action | TXOne Networks Assistance |
|---|---|---|
| Prohibit Connection of Unauthorized Devices | Organizations should implement policies and procedures to prevent the connection of unauthorized media and hardware to their IT and OT assets. This includes restricting the use of USB devices and removable media, as well as disabling features like AutoRun.<br><br>For OT assets, when possible, steps should be taken to either remove, disable, or secure physical ports to block unauthorized device connections.<br><br>Alternatively, procedures should be established to allow access through sanctioned exceptions. | • **Stellar's** USB Vector Control feature can block the use of external storage media. It can also be used to allow a few selected external storage devices based on device identification like Vendor ID, Product ID or Serial Number.<br><br>• **Safe Port** assists in sanitizing external storage media within a protected and secure setting. It is suitable for use in OT environments because it is capable of inspecting external media as well as identifying and removing malware. |
| No Exploitable Services on the Internet | Assets accessible via the public internet should not offer any services vulnerable to exploitation, like the remote desktop protocol. If such services need to be accessible, suitable countermeasures ought to be put in place to deter abuse and exploitation. All non-essential operating system applications and network protocols should be deactivated on internet-facing assets. | • **EdgeFire/EdgeIPS** are a comprehensive solution that specializes in OT-aware segmentation, offering enhanced support for secure access control to OT/ICS asset information systems. With **EdgeFire/EdgeIPS**, organizations can enforce strict measures to restrict access to authorized entities such as EWS (Engineering Workstations) and HMI (Human-Machine Interface) devices. By implementing this level of segmentation, **EdgeIPS** ensures that only trusted and designated sources can interact with the OT/ICS asset information systems. limiting the risk of unauthorized access or potential vulnerabilities. |
| Limit OT Connections to Public Internet | OT assets shouldn't be connected to the public internet, except when it's absolutely necessary for operational purposes. Any exceptions to this rule must be properly justified and documented, and these assets should have extra security measures in place to prevent and identify efforts at exploitation Such measures include logging, Multi-Factor Authentication (MFA), and mandatory access through a proxy or another intermediary. | • **EdgeFire** is an advanced next-generation firewall solution specifically crafted for OT environments. This solution facilitates network segmentation and effectively isolates connectivity between facilities and production zones. By implementing **EdgeFire**, organizations can enhance the security and control of their OT networks. This enables a more secure and efficient operational environment, ensuring that critical systems and assets remain protected from potential threats. |

| Security Practice | Recommended Action | TXOne Networks Assistance |
|---|---|---|
| Detecting Relevant Threats and TTPs | Organizations should create and maintain a documented list of threats and cyber actor Tactics, Techniques, and Procedures (TTPs) pertinent to their specific context, such as their industry or sector. They should also ensure they have the capability to identify occurrences of these primary threats through methods like rule setting, alert systems, or commercial prevention and detection systems. | • **Stellar** uses Operations Behavior Anomaly Detection, which enables the identification of any abnormal behavior within system operations. By leveraging advanced algorithms and analytics, **Stellar** effectively detects deviations from expected patterns or behaviors in real-time. **Stellar's** Operations Behavior Anomaly Detection enhances the overall security posture by providing early detection and timely alerts, allowing for prompt investigation and mitigation of any suspicious activities within the system operations. |
| Incident Reporting | Organizations should establish policies for reporting confirmed cybersecurity incidents, clearly specifying the entities that need to be notified, such as Information Sharing and Analysis Centers/Organizations (ISAC/ISAOs). Incidents must be reported within the timeframes specified by regulations or as quickly as possible. | • TXOne Networks' Threat Research continuously monitors and detects IoT/ICS threat terrain via our large-scale, fully automated, threat hunting system. Threat data is continuously gathered through a worldwide network of hunting engines, submissions, feedback loops, customers & partners, and our own Threat Research Labs researchers. These threat intelligence systems promptly protect our customers' critical assets and operations. |
| Vulnerability Disclosure/ Reporting | Organizations should maintain a public and easily discoverable method for security researchers to report vulnerabilities to the organization's security team, such as through an email address or a web form, regarding assets that are vulnerable, misconfigured, or otherwise exploitable. Considering the integrity and complexity of vulnerabilities, effective submissions should receive prompt acknowledgment and response. Verified and exploitable vulnerabilities ought to be mitigated according to their severity. | • **ElementOne** offers a comprehensive overview of an organization's assets and associated risks. It displays asset type, OS, top 10 missing patches, total asset number, and critical vulnerabilities.<br>• **SageOne** streamlines vulnerability management across multiple product lines across multiple sites. By prioritizing vulnerabilities with an adaptive severity-emergency approach, **SageOne** enhances the organization's overall security posture and eases the burden of effort on management. |

| Security Practice | Recommended Action | TXOne Networks Assistance |
|---|---|---|
| Incident Planning and Preparedness | Develop, maintain, and execute plans to recover and restore to service business- or mission-critical assets or systems that might be impacted by a cyber incident. | • **SageOne** offers a multi-dimensional view of an organization's cybersecurity posture through visual representations. It provides a holistic security perspective with granularity, including the proportion of protected/unprotected assets, asset health status and anomaly detection, asset exposure level assessment, and an overview of the asset lifecycle. Asset managers can efficiently evaluate system vulnerabilities through the **SageOne** dashboard, setting priorities and response plans. This enables a macroscopic ordering of risk management priorities to effectively and accurately reduce the level of risk. |



# Conclusion

As the food and beverage industry increasingly relies on digital systems for smooth operations, it bears a great deal of responsibility in safeguarding itself from significant cyber threats, given its critical role in the economy. The NIS2 Directive was designed to ensure that critical infrastructure industries employ modern cybersecurity defenses to protect the global food supply chain. Furthermore, placing cybersecurity at the forefront is essential when designing new automated systems. These fresh mandates will take effect in the second half of 2024, and TXOne Networks stands ready to assist the food industry in tackling cyber threats and simplifying compliance.

## Why TXOne

At TXOne, we understand the unique cybersecurity challenges facing the food industry, especially with the increasing automation of operations and networking of the food supply chain. Recognizing the need for specialized security solutions, we have dedicated ourselves to providing comprehensive cybersecurity measures that not only meet but exceed the requirements of the regulations. Our approach is to equip businesses within the food supply chain with the tools and knowledge necessary to safeguard their operations against the evolving landscape of cyber threats.

Our solutions are built on the foundation of OT zero trust, creating custom, OT-native, safety-by-design security policies aimed at maintaining operational integrity, protecting the supply chain from attacks, and ensuring operational continuity. By leveraging advanced technologies and expert insights, we offer a holistic approach to cybersecurity, encompassing:

- Security Inspection
- Cyber-Physical Systems Detection and Response (CPSDR)
- Network Defense
- Cyber-Physical Systems (CPS) Protection Platform

# Reference

[1] Rebecca Moody, “Map of worldwide ransomware attacks (updated daily)”, Comparitech, January 06, 2023.

[2] Aishwarya Nair, Chris Reese, “Meatpacker JBS says it paid equivalent of $11 mln in ransomware attack”, Reuters, June 11, 2021.

[3] Anna Ribeiro, "Dole ransomware incident affected half of its legacy servers with direct costs reaching $10.5 million", Industrial Cyber, May 22, 2023.

[4] Rebecca Moody, “Ransomware attacks on food, beverage, and agriculture organizations have cost the world economy $1.36bn in downtime alone”, Comparitech, June 05, 2023.

[5] MITRE ATT&CK, “REvil, Software S0496”, MITRE, Date Accessed April 07, 2024.

[6] Anna Ribeiro, “US lawmakers propose Farm and Food Cybersecurity Act to boost cyber protections for agriculture, food supply chain”, Industrial Cyber, January 31, 2024.

[7] Uniqkey, "The NIS2 Directive", Uniqkey, March 03, 2023.

[8] Sandra Schmitz-Berndt, “Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive”, Journal of Cybersecurity, April 05, 2023.

[9] Mark Marron, “IT Modernization Efforts Need to Prioritize Cybersecurity”, Cyber Defense Magazine, December 01, 2023.

[10] Kevin Townsend, “Cybersecurity Threats to the Food Supply Chain”, SecurityWeek, May 12, 2020.

[11] Brian Van Vleet, “Top Food & Beverage Cybersecurity Challenges”, Rockwell Automation, September 19, 2022.

[12] Cybersecurity and Infrastructure Security Agency CISA , “Cross-Sector Cybersecurity Performance Goals: CISA” CISA, Date Accessed April 07, 2024.

[13] Cybersecurity and Infrastructure Security Agency CISA, “Known Exploited Vulnerabilities Catalog: CISA”, CISA, Date Accessed April 07, 2024.

txOne networks