txOne networks

EXECUTIVE SUMMARY

A Recipe for Resilience

Strengthening cybersecurity in the food and beverage sector

While the integration of internet-connected technologies in the food and beverage sector is revolutionising operations, it is also introducing significant cybersecurity challenges. The industry has become the seventh most attacked globally, suffering substantial economic losses from ransomware and other cyber threats. This ebook delves into these pressing issues, offering strategic insights and practical solutions tailored to fortify OT cybersecurity defences within the food and beverage supply chain. By understanding and implementing these measures, organisations can safeguard against emerging threats and preserve their golden batch in production environments.

Wider attack surfaces created by the fast introduction of interconnected agricultural machinery, data collection tools, and processing facilities is rendering organisations increasingly vulnerable to malicious activity. The prevalence of outdated legacy systems alongside newer technologies creates further vulnerabilities, as older systems may lack updated security measures. The situation is compounded by a growing reliance on third-party suppliers for software and technology, where a cyber breach at any point in the network can compromise every connected vendor.

Attracted to lower hanging fruit, cybercriminals are turning their attention to the food and beverage industry, driven by motives ranging from financial gain to environmental activism. Attack vectors include social engineering, exploitation of software vulnerabilities, and direct tampering of critical systems by insiders. These threats pose serious risks, including operational disruption or health and safety issues which could have severe consequences for both businesses and consumers.

Recent legislative changes, such as the EU NIS2 Directive and the Cyber Resilience Act, are adding to the pressure, imposing new cybersecurity requirements on food production and distribution entities. Medium and large organisations now face a series of strict compliance obligations, while smaller enterprises may also be impacted depending on their significance.

To fortify their industrial cybersecurity defences, comply with new regulations and protect the entire supply chain from disruption, organisations should introduce and invest in the following 7 core practices;

Threat Detection

Maintain a documented list of sector-specific threats and implement systems to detect and alert on deviations from normal operations.

Third-Party Validation

Regularly assess cyber risks associated with OT/ICS assets and third-party vendors.

Vulnerability Management

Apply patches promptly or use virtual patches for immediate protection.

Network Segmentation

Segment networks to limit access and contain threats.

Unauthorised Device Control

Implement policies to block unauthorised devices and media.

Internet-facing Services

Avoid exposing vulnerable services on the internet.

Incident Response

Develop and update incident response plans, conducting regular drills.

Download the eBook to gain actionable insights from our experts and support your OT cybersecurity strategy.

Get your free copy