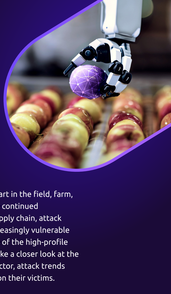


Serving up Sector Insights

Cybersecurity trends for the food and beverage industry

Disruption in the food and beverage sector can start in the field, farm, factory or at distribution and retail level. With the continued digitisation of operations at every stage of the supply chain, attack surfaces are expanding, leaving organisations increasingly vulnerable and exposed to malicious activity. In light of some of the high-profile attacks that have recently hit the headlines, we take a closer look at the motivations behind threat actors targeting the sector, attack trends and the financial impact of cybercriminal activity on their victims.

Frequency of Attack

The food and beverage manufacturing industry is the seventh most attacked globally, **bearing the brunt of 5.5%[1] of all ransomware attacks in 2023.**

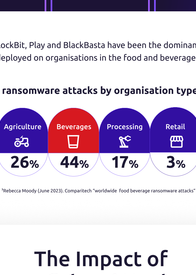
[1]Global AG Tech Initiative (April 2024). The Reality of Ransomware Attacks in Agriculture

Number of Cybersecurity Incidents in the Food Industry by Year

Year	Number of Incidents
2018	2
2019	5
2020	45
2021	65
2022	38
2023	39

As of February 2024, 7 ransomware attacks had been reported in the sector, indicating a potential increase in the total number of ransomware attacks for the year vs 2023.

Top 10 countries by number of ransomware attacks on food and beverage organisations[2]



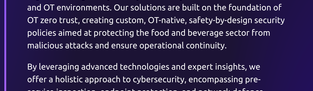
[2]Rebecca Moody (June 2023). Comparitech "worldwide food beverage ransomware attacks"

Threat Actor Motivations, Tactics & Targets

Top 3 reasons cyber criminals target the food & beverage supply chain:

Alphv, Revil, LockBit, Play and BlackBasta have been the dominant ransomware strains deployed on organisations in the food and beverage industry

Share of ransomware attacks by organisation type in 2022[3]



[3]Rebecca Moody (June 2023). Comparitech "worldwide food beverage ransomware attacks"

The Impact of a Cyber Attack

2018-2023

Global economic cost of downtime*

$1.36bn[4]

*as a result of ransomware attacks on food, beverage and agricultural organizations

[4]Rebecca Moody (June 2023). Comparitech "worldwide food beverage ransomware attacks"

A tried and tested recipe for security

TXOne Networks secures the operations of more than 3,600 organisations globally with cybersecurity solutions tailored for ICS and OT environments. Our solutions are built on the foundation of OT zero trust, creating custom, OT-native, safety-by-design security policies aimed at protecting the food and beverage sector from malicious attacks and ensure operational continuity.

By leveraging advanced technologies and expert insights, we offer a holistic approach to cybersecurity, encompassing pre-service inspection, endpoint protection, and network defence during onboarding, staging, production, and maintenance.

Discover how TXOne can secure your organisation with OT-native solutions that protect your assets throughout their entire life cycle.

Contact us