FOOD & AGRICULTURE SECTOR CYBERSECURITY

Sector Overview

This resource is for stakeholders in Florida's Food & Agriculture sector. It includes farms, food processors, packaging facilities, distributors, retailers and agricultural cooperatives. The sector safeguards the state's food supply and supports public health while adding billions to Florida's economy. Operations depend on interconnected supply chains and specialized industrial equipment. Many businesses also rely on third-party service providers. These factors make the sector a prime target for ransomware attacks that can disrupt public health services, cause food shortages and create major economic losses.

Ransomware Threat Profile

Only 17% of Florida's Food & Agriculture organizations meet the Department of Homeland Security's basic ransomware readiness standards, falling well below the statewide average. Agricultural operations are often decentralized and many use aging operational technology. The sector also depends on global logistics networks. These conditions create an environment with a high-risk susceptibility to ransomware. Cyber criminals know the sector cannot tolerate long outages and often use this urgency to pressure victims into paying ransoms quickly.

Key Ransomware Risk Factors in Food & Agriculture

Risk Level	Why it Matters for the Sector	Estimated % of Orgs Affected
Cold Chain Dependency	Refrigeration & climate-controlled storage vulnerable to OT/ICS outages; spoilage risk	62%
Legacy ICS/SCADA Systems	Outdated operational systems with poor patching and security	54%
Seasonal Workforce Turnover	High staff turnover creates training & access control gaps	47%
Third-Party Vendor Reliance	Shared logistics, shipping & payment systems expand attack surface	39%
Limited Cybersecurity Staffing	Many organizations lack dedicated CISO or security team	44%

Note: Cold chain dependency (62%) and legacy ICS/SCADA systems (54%) are the most widespread ransomware risk factors in this sector. High seasonal workforce turnover (47%) and limited cybersecurity staffing (44%) further weaken defenses, leaving critical operations exposed.

Top Vulnerabilities

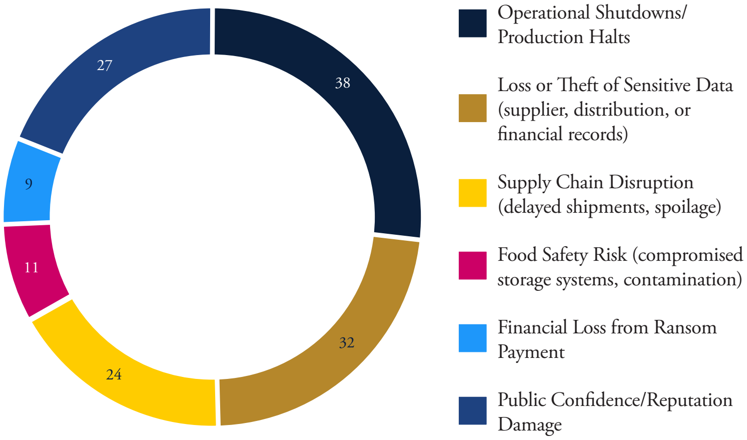
- **Cold Chain & Logistics Dependency**
  - Refrigeration and delivery systems for perishable goods depend on real-time coordination. A ransomware attack can cause mass spoilage & halt distribution. This can trigger cascading shortages.
- **Aging ICS and Farm Equipment**
  - GPS-guided tractors, irrigation systems & processing equipment often run outdated firmware. Many lack modern authentication, making them easy ransomware entry points.
- **Sparse Cybersecurity Staffing**
  - Small and rural operations often lack full-time IT or cybersecurity staff. This limits their ability to detect & respond to attacks.
- **Data Privacy Gaps**
  - Customer, supplier, and crop yield data is often stored without strong encryption or segmentation. Theft of this data can be used for extortion or disrupt competitive operations.

FOOD & AGRICULTURE SECTOR CYBERSECURITY

Action Checklist

- Develop & regularly update ransomware-specific Incident Response Plans tailored to cold chain systems and ICS/SCADA operations.
- Enforce Multi-Factor Authentication (MFA) across all critical systems & vendor platforms.
- Conduct annual ransomware-specific tabletop exercises that include cold chain failure & vendor system compromise scenarios.
- Secure & segment legacy ICS and GPS-enabled agricultural systems.
- Implement & regularly test secure backups of operational & business data, prioritizing cold storage monitoring systems & production line controls.
- Assign a dedicated cybersecurity lead (CISO or equivalent).

Common Consequences of Ransomware in Food & Agriculture



Note: Operational shutdowns and production halts were the most common consequence of ransomware in this sector in 2024, impacting an estimated 38% of incidents. Data loss (32%) and supply chain disruption (24%) also ranked among the top outcomes.

Notable Incidents

- **FreshPoint Florida Outage (2024):** A ransomware-linked incident disrupted produce deliveries from the Orlando branch to schools, hospitals and restaurants statewide.
- **Florida Citrus Cooperative Breach (2023):** Ransomware encrypted accounting and shipping systems at a major citrus processor in Central Florida. Deliveries were delayed and sensitive contract data was exposed.
- **JBS Foods Attack (2021):** The global meat processor was forced to halt operations after a ransomware attack. Florida facilities experienced production delays and distribution impacts.

State-Funded Resources & Education

Technical Tools

- **CISA Ransomware Readiness Assessment (CSET)**
- **FDA Food defense Plan Builder**

Templates & Planning

- **Cyber Florida Incident Response Plan Templates**
  Available Upon Request
- **NIST Cybersecurity Framework**
  (https://www.nist.gov/cyberframework)
- **Food Protection and Defense Institute Guidance**

State-Funded Resources

- **FIU Cyber Leadership Courses**
  (https://gordoninstitute.fiu.edu/cybersecurity-policy/training/cybersecureflorida/index.html)
- **CISA Cyber Hygiene Services**
  Free Assessments & Scans
  (https://www.cisa.gov/resourcestools/ programs/cyberhygiene-services)