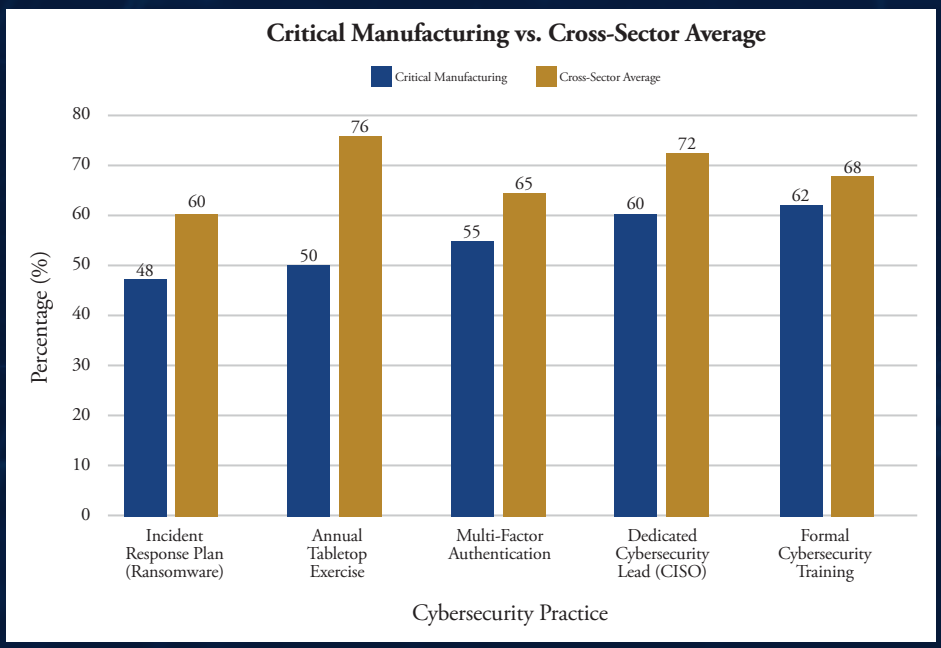
CRITICAL MANUFACTURING SECTOR CYBERSECURITY

Sector Overview

This resource is for stakeholders within Florida's Critical Manufacturing sector, including producers of metals, machinery, electrical equipment, transportation equipment, and other manufacturing enterprises essential to the state's economy and security. This sector also includes Department of Defense contractors and industrial base suppliers, which are frequent targets of nation-state Cyberattacks. Disruptions from ransomware can severely impact supply chains and production, threatening economic stability across the state and reinforcing the need for strong cybersecurity protections.

Ransomware Threat Profile

Florida's critical manufacturing sector shows moderate ransomware readiness, with about 31% of organizations meeting the Department of Homeland Security's (DHS) basic cybersecurity standards. However, the sector's reliance on complex supply chains and connected production systems, along with its use of operational technology (OT) and industrial control systems (ICS), leaves it exposed to advanced ransomware threats.



Note: Critical Manufacturing falls 10–26% behind the cross-sector average in several core ransomware readiness practices, with the biggest gap seen in tabletop exercises and CISO assignment.

Top Vulnerabilities

- **Just-In-Time Production Disruption**
  - Ransomware attacks on scheduling, inventory, or robotics systems can bring lean manufacturing operations to a halt, causing major production losses.
- **Proprietary Process Exposure**
  - Many facilities store sensitive production formulas or designs. Ransomware groups may exfiltrate this IP to extort manufacturers or auction it to competitors.
- **Remote Monitoring Exploits**
  - Modern plants rely on remote SCADA or IoT systems for oversight. Poorly secured interfaces offer attackers a route into both business and operational networks.
- **Integration with Defense Industrial Base**
  - Less than half of critical manufacturing entities regularly conduct ransomware-specific incident response exercises or have updated and tested recovery plans.

FIU Jack D. Gordon Institute for Public Policy
JGI@fiu.edu
CYBER FLORIDA AT THE UNIVERSITY OF SOUTH FLORIDA

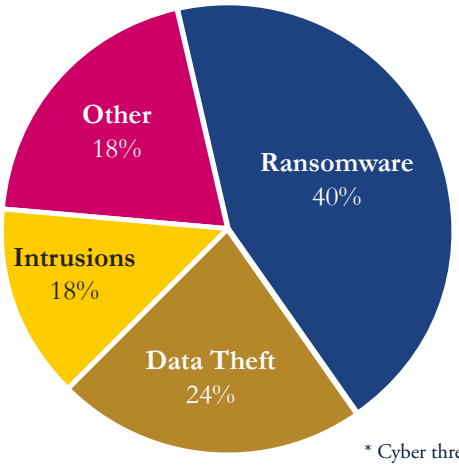
CRITICAL MANUFACTURING SECTOR CYBERSECURITY

Action Checklist

- Develop and regularly update ransomware-specific Incident Response Plans.
- Enforce Multi-Factor Authentication (MFA) across critical operational and administrative systems.
- Conduct annual ransomware specific tabletop exercises.
- Evaluate and securely segment legacy ICS/OT systems.
- Establish secure and regularly tested backups of critical production and business data.
- Assign dedicated cybersecurity personnel (CISO or equivalent).

Note: Ransomware accounts for 40% of cyber threats reported in Florida's manufacturing sector, surpassing data theft and intrusion as the most common and disruptive attack type.

Cyber Threats Faced by Critical Manufacturing



* Cyber threat data 2024

Notable Incidents

- **Fidelity National Financial (2023):** Fidelity National Financial in Jacksonville was hit by a ransomware attack from the BlackCat group. The attack disrupted services tied to title insurance and mortgage processing, delaying critical transactions across Florida's manufacturing and real estate sectors.
- **Norsk Hydro Attack (2019):** A ransomware attack on Norsk Hydro caused major production shutdowns and widespread system outages. The company faced recovery costs of over $70 million, showing how vulnerable manufacturing operations and supply chains are to cyber disruption.

State-Funded Resources & Education

Technical Tools

- **CISA Ransomware Readiness Assessment (CSET)**
- **Manufacturing Extension Partnership (MEP) Cybersecurity Toolkit**
- **DOE Cybersecurity Capability Maturity Model (C2M2)**

Templates & Planning

- **Cyber Florida Incident Response Plan Templates**
  Available Upon Request
- **NIST Cybersecurity Framework**
  (https://www.nist.gov/cyberframework)
- **DHS Cybersecurity Guidelines for Critical Manufacturing**

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)

FIU Jack D. Gordon Institute for Public Policy

JGI@fiu.edu

CYBER FLORIDA AT THE UNIVERSITY OF SOUTH FLORIDA