CHEMICAL SECTOR CYBERSECURITY

Sector Overview

This resource is for stakeholders in Florida's Chemical sector, including:

- Chemical manufacturing plants
- Hazardous material producers
- Agricultural chemical suppliers
- Pharmaceutical companies
- Chemical storage and transportation providers

This sector supports public safety, environmental protection, healthcare, and economic stability. A ransomware incident could threaten human health, disrupt supply chains, and cause environmental damage due to the hazardous nature of the materials handled.

Ransomware Threat Profile

Florida's Chemical sector has become a high-value ransomware target due to its reliance on industrial control systems, operational technology (OT), and specialized management software. Ransomware-related incidents grew from 10% of reported cyber threats in 2018 to over 40% in 2024. The combination of hazardous materials and interconnected supply chains increases the stakes of any successful attack.

Top Vulnerabilities

- Aging Distributed Control Systems & PLCs
- Third-Party Logistics & Supply Chain Weaknesses
- Limited OT-Focused Ransomware Testing
- Unsegmented Network Architecture Between IT & OT

Notable Incidents

- **Occidental Chemical Plant (2022):** Ransomware halted production at a major chemical plant, forcing temporary shutdowns of key process lines. The attack highlighted the potential for OT-targeted ransomware to disrupt production schedules and create safety concerns in regulated facilities.
- **Brenntag Chemical Distributor (2021):** A ransomware attack disabled billing and customer service systems for municipal water and chemical divisions, forcing manual operations. Restoration took weeks, delaying work orders and public service responses.

State-Funded Resources & Education

Technical Tools

- **Assessment (FCRA) + NIST 2.0 CSF**
  (https://cyberflorida.org/cip/)
- **State of Florida Cyber Risk**
- **Chemical Facility Anti-Terrorism**
- **Standards (CFATS) Program**
  (https://www.cisa.gov/cfats)
- **DOE Cybersecurity Capability Maturity Model (C2M2)**
  (https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2)

Templates & Planning

- **Cyber Florida Incident Response Plan Templates**
  Available Upon Request
- **NIST Cybersecurity Framework**
  (https://www.nist.gov/cyberframework)
- **ACC Responsible Care Cybersecurity Guidance**

State-Funded Resources

- **FIU Cyber Leadership Courses**
  (https://gordoninstitute.fiu.edu/cybersecurity-policy/training/cybersecureflorida/index.html)
- **Cyber Florida Frontline Training Program**
  (https://cyberflorida.org/firstline/)
- **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