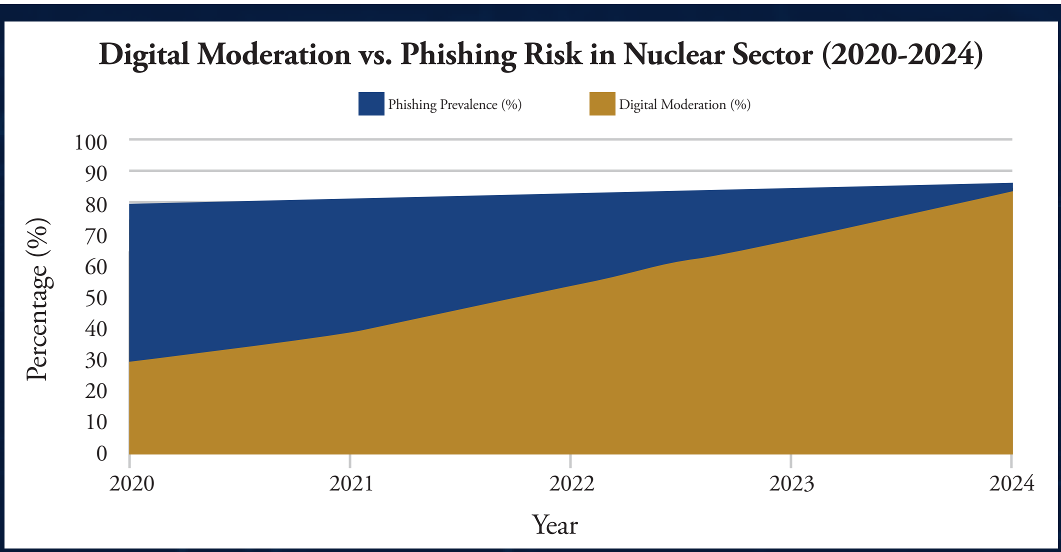
NUCLEAR REACTORS, MATERIALS, AND WASTE CYBERSECURITY

Sector Overview

This resource is for stakeholders in Florida's Nuclear Reactors, Materials, and Waste sector. This includes operators of nuclear power plants, research reactors, nuclear medicine production facilities, radioactive materials handlers, and waste storage/disposal sites. This sector supports energy generation, medical treatment, research and national security. Nuclear materials are hazardous and reactor systems are complex so even small disruptions can create safety risks and lead to environmental or economic damage. Ransomware incidents affecting this sector could compromise critical safety systems, delay waste management operations, or disrupt regulatory compliance activities.

Ransomware Threat Profile

Nuclear facilities follow some of the most strict cybersecurity requirements due to federal oversight. Despite this, ransomware is still a credible threat, especially to business networks, engineering systems and contractor access points. Only 33% of organizations in the sector meet DHS basic ransomware readiness standards. This is slightly higher than the cross sector average but still leaves significant gaps. Key risks come from outdated digital control systems, vendor network connections, and valuable intellectual property tied to nuclear technology.



Note: From 2020–2024, digital modernization in U.S. nuclear facilities rose from 30% to 85%. Over the same period, phishing remained the leading ransomware entry point, increasing from 80% to 88% of reported attacks. This overlap shows modernization expands the digital attack surface, while phishing persists as the main entry point.

Top Vulnerabilities

▸ **Digital Reactor Control Interfaces**

- Modernized control rooms mix legacy analog systems with digital monitoring. A ransomware hit could disrupt data visibility or delay safety decisions.

▸ **Fuel Cycle Vendor Access Points**

- Enrichment, fabrication, and transport contractors often keep remote access for logistics and reporting. Weak vendor security can allow network entry.

▸ **Specialized Safety & Radiation Monitoring Systems**

- Radiation sensors and safety interlocks often run on proprietary software with rare updates, leaving longterm weaknesses.

▸ **High-Value Nuclear Research Data**

- Universities and labs store sensitive reactor, isotope, and fuel design data that can be stolen for extortion or foreign intelligence.

▸ **Waste Handling & Storage Facility IT Gaps**

- Waste tracking and scheduling systems are often less protected than plant controls, creating indirect attack paths.

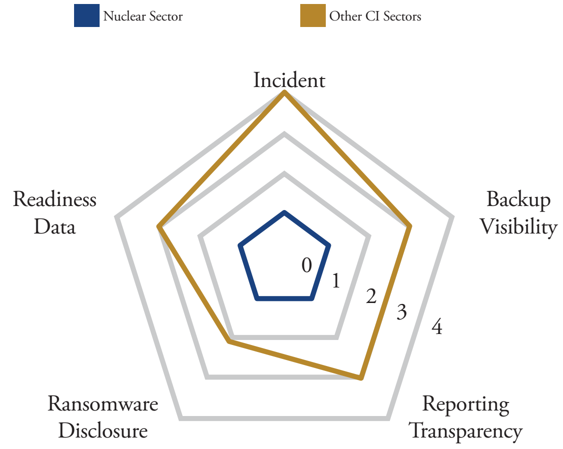
NUCLEAR REACTORS, MATERIALS, AND WASTE CYBERSECURITY

Action Checklist

- Develop and test ransomware-specific Incident Response Plans for reactor control, radiation monitoring, and waste management systems.
- Enforce Multi-Factor Authentication (MFA) for all administrative, engineering, and vendor accounts, with phishing resistant authentication for critical systems.
- Conduct annual ransomware tabletop exercises simulating vendor compromise, business IT outage, and engineering workstation lockouts.
- Segment digital instrumentation & control systems from business networks; disable unnecessary remote access.
- Maintain offline, immutable backups of reactor safety parameter displays, regulatory compliance records, and waste tracking databases.
- Require all contractors handling nuclear materials or IT systems to meet federal cybersecurity standards (e.g., NRC, DOE, NIST).
- Implement continuous monitoring with anomaly detection tuned to nuclear operations.

Ransomware & Cyber Visibility

Nuclear Sector vs. Other Critical Infrastructure



Note: The nuclear sector reports far fewer ransomware incidents than most CI sectors. While 14 of 16 sectors reported activity in 2022, nuclear-related public cases remain rare, leaving visibility gaps in cyber metrics.

Notable Incidents

- **Nuclear Research Facility Vendor Breach (2023):** A ransomware attack on a third-party IT contractor disrupted scheduling at a U.S. university research reactor and exposed sensitive technical data. Operations were unaffected, but the case highlighted vendor access risk.
- **Ukrainian Nuclear Plant Cyber Disruption (2022):** During geopolitical conflict, cyberattacks targeted nuclear plant business systems and engineering workstations. The incident showed the potential for state-backed ransomware-like activity to threaten civilian nuclear operations.
- **Westinghouse Electric Company (2021):** Ransomware disrupted corporate IT systems and delayed project deliverables to U.S. nuclear plants. While reactor operations were isolated, the breach revealed supply chain vulnerabilities.

State-Funded Resources & Education

Technical Tools

- **CISA Ransomware Readiness Assessment (CSET)**
- **NRC Cybersecurity Regulatory Guides**
- **DOE Cybersecurity Capability Maturity Model**

Templates & Planning

- **Cyber Florida Incident Response Plan Templates**
  Available Upon Request
- **NIST Cybersecurity Framework**
  (https://www.nist.gov/cyberframework)
- **IAEA Nuclear Security Series: Computer Security at Nuclear Facilities**

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)