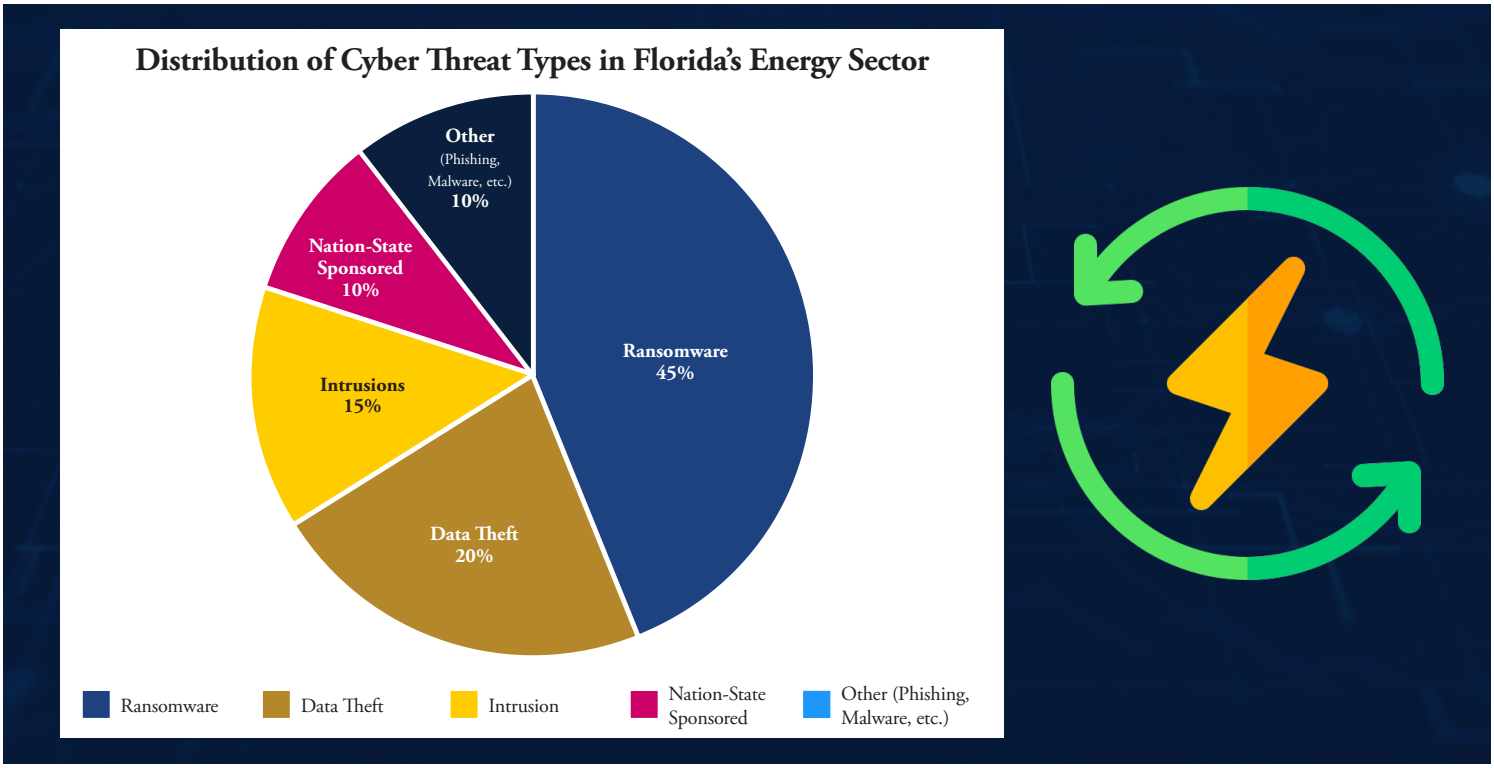
ENERGY SECTOR CYBERSECURITY

Sector Overview

This resource is for stakeholders in Florida's Energy sector, including electricity providers, oil and gas operators, renewable energy companies, and other critical energy infrastructure organizations. The sector is essential for maintaining statewide operations and public safety. A disruption can cause cascading impacts across other critical infrastructure sectors. These risks make strong cybersecurity measures essential to protect energy systems from ransomware threats.

Ransomware Threat Profile

Despite its critical nature, approximately 31% of Florida's energy providers currently meet the Department of Homeland Security's (DHS's) basic ransomware readiness standards, positioning it moderately among the 16 CI sectors. The sector faces unique cybersecurity challenges due to its reliance on interconnected operational technology (OT) systems and industrial control systems (ICS), which, if compromised, can cause widespread operational disruption.



Top Vulnerabilities

- **Legacy Turbine & Substation Control Systems**
  - Many Florida energy providers operate generation and distribution equipment with ICS firmware that is no longer supported, leaving exploitable vulnerabilities in grid and plant operations.
- **Insufficient OT-Focused Incident Response Testing**
  - Few providers run ransomware tabletop drills simulating OT and SCADA disruptions, meaning recovery procedures for black-start or islanding scenarios remain untested.
- **Understaffed OT Cybersecurity Roles**
  - Smaller municipal and co-op utilities often lack engineers trained in both operational technology and cybersecurity, delaying threat detection in critical systems.
- **Flat Network Architectures Linking IT & OT**
  - Some providers still connect billing, HR, and email systems directly to grid monitoring and plant control networks, giving ransomware a direct path to critical operations.

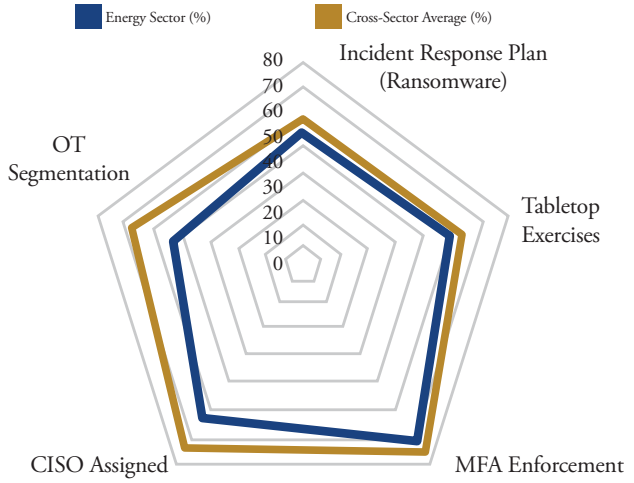
FIU Jack D. Gordon Institute for Public Policy
JGI@fiu.edu
CYBER FLORIDA AT THE UNIVERSITY OF SOUTH FLORIDA

ENERGY SECTOR CYBERSECURITY

Action Checklist

- Develop and test ransomware-specific Incident Response Plans for power generation plants, substations, and pipeline operations, including OT restoration procedures.
- Segment control networks (SCADA, DCS, PLC) from corporate IT systems to prevent ransomware spread between business and operational environments.
- Conduct quarterly vulnerability scans and patch cycles for turbine controllers, relay systems, and other high-value ICS assets.
- Assign a dedicated OT cybersecurity lead or engineer with authority over ICS/OT protections.
- Enforce Multi-Factor Authentication (MFA) for remote vendor access to substations, generation facilities, and pipeline control systems.
- Maintain offline and immutable backups of critical operational data including SCADA configurations, protective relay settings, and generation schedules.

Ransomware Readiness Practices: Energy Sector vs. Cross-Sector Average



Note: In 2024, Florida's Energy sector scored 55% for Incident Response Plans and Tabletop Exercises (vs. 60% averages), 70% for MFA (vs. 75%), and 60% for CISO assignment (vs. 72%). OT segmentation was lowest at 50%, compared to 65% across sectors.

Notable Incidents

- **TECO Energy (2023):** Attempted ransomware attack targeted internal systems; quickly contained but prompted network segmentation upgrades.
- **Gulf Power Substation Vendor Breach (2022):** Third-party vendor compromise allowed unauthorized access to grid monitoring tools; no outage occurred, but data ex-filtration confirmed.
- **Colonial Pipeline Attack (2021):** Disrupted fuel delivery along the East Coast, underscoring pipeline vulnerability to ransomware.
- **Delta-Montrose Electric Association (2021):** Ransomware disrupted billing systems and exposed customer data, forcing a rebuild of affected systems.

State-Funded Resources & Education

Technical Tools

- **CISA Ransomware Readiness Assessment (CSET)**
- **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)
- **Electric Sector Coordinating Council (ESCC) Cybersecurity Playbook**
- **DOE Cyber-Informed Engineering (CIE) Strategy**

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