GOVERNMENT FACILITIES SECTOR CYBERSECURITY

Sector Overview

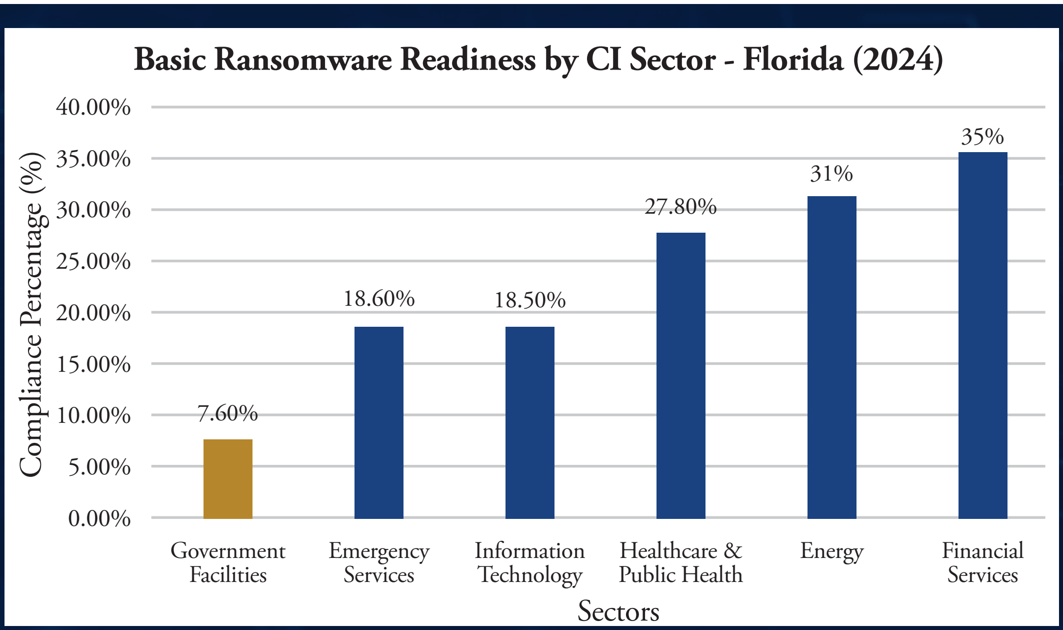
This resource is for stakeholders in Florida's Government Facilities sector, including:

- State agencies
- Municipalities
- Local governments

These entities deliver vital public services such as emergency response and public utilities. Many lack dedicated cybersecurity infrastructure or funding, especially at the county or municipal level. These gaps make them highly susceptible to ransomware attacks that can disrupt government operations and public safety.

Ransomware Threat Profile

Only 8% of Florida's government facilities meet the Department of Homeland Security's (DHS) basic ransomware readiness standards, ranking last among all 16 critical infrastructure (CI) sectors. Low compliance is driven by organizational, technical, and funding challenges.



Note: Government Facilities have the lowest ransomware readiness of any critical infrastructure sector in Florida at 7.6%. This is less than half the readiness level of sectors such as Healthcare & Public Health (27.8%) and significantly below Financial Services (35%), which leads all measured sectors.

Top Vulnerabilities

▶ **Incident Response Gaps in Public Services**

- Few agencies conduct ransomware-specific tabletop exercises. Many lack updated response plans that address service continuity for essential public functions.

▶ **Reliance on Legacy Administrative Systems**

- Outdated tax, court, and permit software remains common, creating exploitable entry points for attackers.

▶ **Limited Cybersecurity Staffing in Local Governments**

- Many counties and cities have no cybersecurity lead (CISO) or specialized team to oversee defenses.

▶ **Vendor and Contractor System Access Risks**

- Outsourced services for payment processing, public record hosting, and IT support often have inadequate cybersecurity oversight, increasing supply chain exposure.

FIU Jack D. Gordon Institute for Public Policy

JGI@fiu.edu

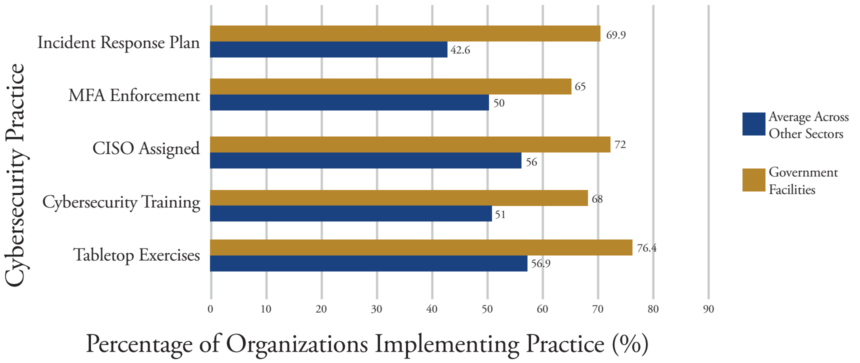
CYBER FLORIDA AT THE UNIVERSITY OF SOUTH FLORIDA

GOVERNMENT FACILITIES SECTOR CYBERSECURITY

Action Checklist

- Develop and test a ransomware Incident Response Plan with COOP for tax, courts, permitting, and public records systems.
- Enforce MFA on remote access and privileged accounts; use phishing-resistant methods for treasury and payment portals.
- Segment networks and isolate legacy administrative apps; restrict direct internet and RDP exposure.
- Maintain offline & immutable backups for ERP, email, and case management; verify restores monthly.
- Deploy EDR and centralized logging; patch critical vulnerabilities in 15 days & high in 30 days.
- Require vendor controls in contracts: MFA, least privilege, audit logs, 24-hr incident notice; review access quarterly.
- Run annual ransomware tabletops with leadership, legal, finance, IT, & public affairs; update plans from lessons learned.

Ransomware Readiness Gaps - Government Facilities (2024)



Note: Government Facilities lag behind other sectors in every core ransomware readiness practice. The largest gap is in Incident Response Plan adoption (42.6% vs. 69.9%), followed by Multi-Factor Authentication (50.0% vs. 65.0%) and CISO assignment (56.0% vs. 72.0%). These gaps point to critical weaknesses in preparation and leadership structure.

Notable Incidents

- **Washington County Sheriff's Office (2023):** Ransomware disabled jail and financial systems, leaving staff unable to access critical records and law enforcement databases for weeks.
- **City of Fort Lauderdale (2023):** A fraudulent invoice scam diverted $1.16 million in funds, which was intercepted and recovered, showing the financial risks tied to phishing and ransomware campaigns.
- **First Judicial Circuit Courts (2023):** Ransomware disrupted court audio systems and exposed sensitive employee data, including Social Security numbers, impacting court operations in multiple counties.
- **St. Lucie County Tax Collector (2023):** BlackCat ransomware forced systems offline, with confirmed data compromise affecting taxpayer records.

State-Funded Resources & Education

Technical Tools

- **CISA Ransomware Readiness Assessment (CSET)**
- **StopRansomware.gov Portal**
- **Multi-State Information Sharing and Analysis Center (MS-ISAC)**

Templates & Planning

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

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)

COOP: Continuity of Operations Plan
MFA: Multi-Factor Authentication
RDP: Remote Desktop Protocol
ERP: Enterprise Resource Planning
EDR: Endpoint Detection and Response
CISO: Chief Information Security Officer

FIU Jack D. Gordon Institute for Public Policy

JGI@fiu.edu

CYBER FLORIDA AT THE UNIVERSITY OF SOUTH FLORIDA