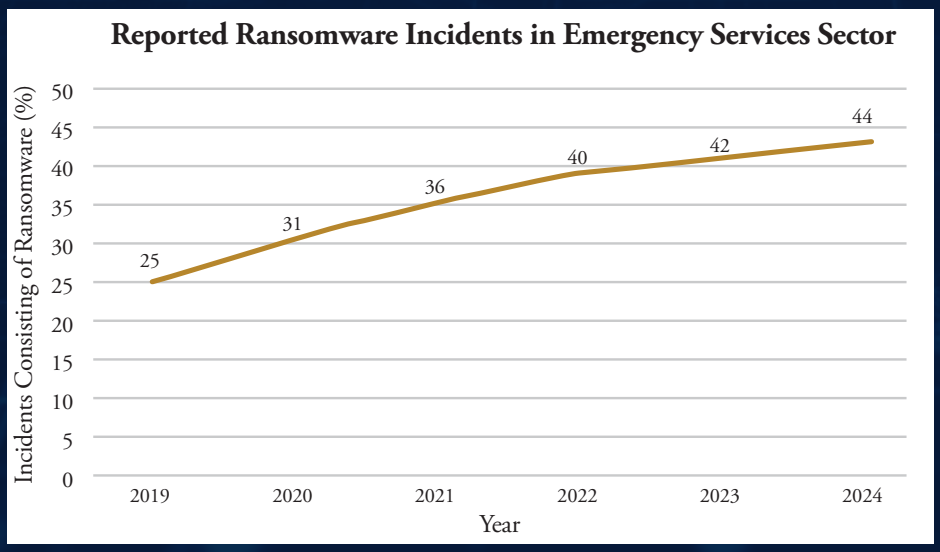
EMERGENCY SERVICES SECTOR CYBERSECURITY

Sector Overview

This resource is for stakeholders in Florida's Emergency Services sector, including law enforcement, fire and rescue, emergency medical services (EMS), 911 call centers, and emergency management agencies. These organizations are critical to protecting lives, property, and public safety during crises. Ransomware can disrupt emergency dispatches and delay life-saving response. It can also undermine public trust in essential services. The sector operates around the clock and depends on real-time communications, making it highly vulnerable to even brief downtime.

Ransomware Threat Profile

Only about 19% of Florida's emergency services providers meet the Department of Homeland Security's (DHS) basic ransomware readiness standards. This places the sector slightly above Government Facilities but behind several other critical infrastructure sectors. While agencies are well-practiced in physical disaster response, many struggle to keep pace with the fast-moving and evolving nature of ransomware threats.



Note: Ransomware incidents in Florida's Emergency Services sector rose from 25% in 2019 to 44% in 2024. The sharpest increase was between 2019 and 2021, with slower but steady growth in recent years, indicating sustained targeting of the sector.

Top Vulnerabilities

- **911 and Dispatch System Disruption**
  - Computer-aided dispatch (CAD) and NextGen 911 systems are increasingly digital and interconnected. Ransomware targeting these systems can prevent calls from being logged or routed to first responders.
- **Legacy Public Safety Networks**
  - Many agencies rely on outdated radio, records management, and emergency notification systems that lack modern security controls, creating exploitable entry points.
- **Interagency Dependency Risks**
  - Emergency response relies on coordination between multiple agencies and jurisdictions. A ransomware attack on one partner can delay response or disrupt regional command-and-control operations.
- **Cybersecurity Staffing and Training Gaps**
  - Many agencies lack a dedicated cybersecurity lead. Training often emphasizes physical safety over cyber incident readiness.
- **Vendor and Third-Party Access Risks**
  - Contracted IT, medical, and communications providers may have remote access without strict controls, creating potential ransomware entry points.

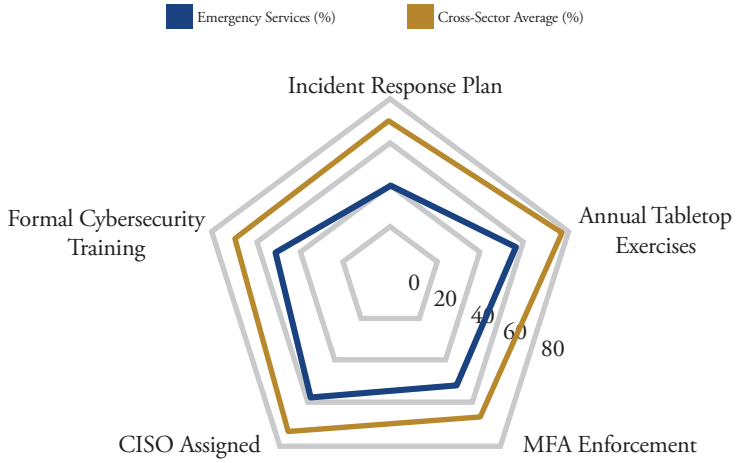
FIU Jack D. Gordon Institute for Public Policy
JGI@fiu.edu
CYBER FLORIDA AT THE UNIVERSITY OF SOUTH FLORIDA

EMERGENCY SERVICES SECTOR CYBERSECURITY

Action Checklist

- Develop and update ransomware-specific Incident Response Plans for CAD, 911, and public safety systems.
- Enforce Multi-Factor Authentication (MFA) across all administrative and operational accounts.
- Conduct annual ransomware-specific tabletop exercises involving all emergency service disciplines and mutual aid partners.
- Modernize or segment legacy dispatch, radio, and records systems to reduce attack surfaces.
- Implement and test secure backups for CAD, 911, dispatch, and operational systems, stored offline or in isolated cloud environments for rapid recovery.
- Assign a dedicated cybersecurity lead (CISO or equivalent) or designate trained personnel responsible for cyber defense.

Ransomware Readiness: Emergency Services vs. Cross-Sector Average



Note: Emergency Services lags behind the cross-sector average in all five core ransomware readiness practices. Incident Response Plan adoption is 42.6% vs. 69.9% average; Annual Tabletop Exercises 56.9% vs. 76.4%; MFA Enforcement 50.0% vs. 65.0%; CISO assignment 56.0% vs. 72.0%; and Formal Cybersecurity Training 51.0% vs. 68.0%. The widest gap is in Incident Response Plan implementation, highlighting a critical area for improvement.

Notable Incidents

- **Washington County Sheriff's Office (2023):** Ransomware disabled jail and financial systems for weeks, disrupting critical operations and restricting access to essential records.
- **Dawson County, Georgia 911 Outage (2023):** A cyberattack disrupted 911 services for multiple counties, delaying emergency response and revealing weaknesses in shared dispatch networks.
- **City of New Orleans Cyberattack (2020):** Ransomware forced police and fire departments offline for weeks, showing the operational impact on public safety agencies.

State-Funded Resources & Education

Technical Tools

- **CISA Ransomware Readiness Assessment (CSET)**
- **SAFECOM Guidance for Public Safety Communications**
- **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)
- **APCO/NENA Public Safety**
- **Cybersecurity Resources**

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