



# COMMUNICATIONS SECTOR CYBERSECURITY

## Sector Overview

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

- Telecommunications providers
- Wireless and satellite companies
- Internet service providers (ISPs)
- Broadcasting organizations

## Ransomware Threat Profile

Only 22% of Florida communications organizations meet Department of Homeland Security (DHS) ransomware readiness standards. This sector depends on complex network infrastructure, interconnected service platforms, and large-scale data systems. These dependencies, combined with the need for uninterrupted service, make it a frequent ransomware target.

## Emergency Communication Networks

The sector is critical to public safety, economic stability, and daily connectivity.

A ransomware incident can disrupt essential services, block emergency alerts, and impact both government operations and private business across the state.

## Top Vulnerabilities

- ▶ Legacy & Hybrid Networks
- ▶ Exploitable Broadcast & Public Interfaces
- ▶ 24/7 Service Pressure
- ▶ Emergency Services Dependencies
- ▶ Under-Resourced Rural Providers



## Notable Incidents

- ▶ **Rogers Communications Outage (2022):** A massive outage cut mobile, internet, & business communications for millions, disrupting emergency services & commerce. This highlighted how failures in large networks can affect Florida users & critical services.
- ▶ **Dish Network Ransomware Attack (2023):** Ransomware disrupted broadcasting & call center operations & online account services. Customers in Florida & nationwide experienced extended outages, billing problems & missed programming.

## State-Funded Resources & Education



### Technical Tools

- **Florida Cyber Risk Assessment Ransomware Readiness**  
(<https://cyberflorida.org/cip/>)
- **FCC Communications Security, Reliability & Interoperability Council (CSRIC)**  
(<https://www.fcc.gov/csric>)



### Templates & Planning

- **Cyber Florida Incident Response Plan Templates**  
*Available Upon Request*
- **NIST Cybersecurity Framework**  
(<https://www.nist.gov/cyberframework>)
- **FCC Cybersecurity Planning Guide**  
(<https://www.fcc.gov/cyberplanner>)



### 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>)