# TRANSPORTATION SYSTEMS/LOGISTICS SECTOR CYBERSECURITY

## Sector Overview

This resource is for stakeholders in Florida's Transportation Systems sector. It includes operators of:

- Airports
- Freight logistics providers
- Highways
- Railways
- Seaports

The sector supports commerce, emergency response, and national security. It enables the movement of goods and people across the state. Ransomware disruptions can halt fuel storage, delay supply chains, and create major safety risks.

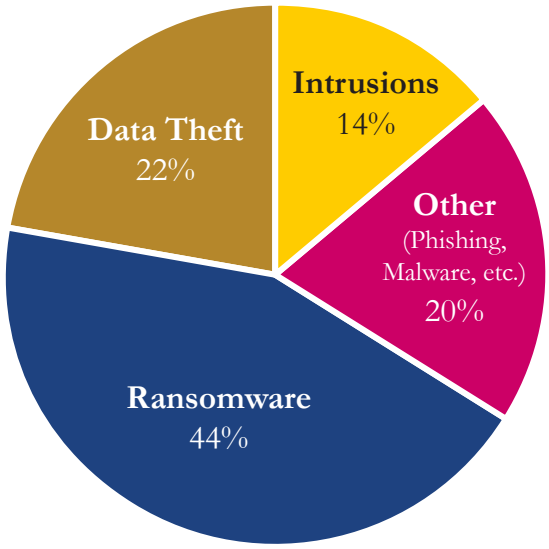
## Top Vulnerabilities

- **Legacy Port & Airport Management Systems**
  - Many facilities run outdated terminal, cargo, and scheduling platforms with unpatched vulnerabilities.
- **Unpatched Rail and Transit Control Systems**
  - SCADA and signaling systems in rail and metro transit often lack modern authentication and encryption.
- **Low Ransomware Drill Participation**
  - Fewer than half of operators conduct ransomware specific tabletop exercises or update incident response plans annually.
- **Third-Party Logistics Platform Risks**
  - Heavy reliance on external SaaS providers for cargo tracking, routing, and freight billing exposes sensitive data if those platforms are compromised.

## Ransomware Threat Profile

Florida's transportation sector ranks below average in ransomware readiness. Only 18.5% of organizations meet the Department of Homeland Security's basic standards. This places it behind Energy (31%) and Emergency Services (19%). Complex and interconnected operations, legacy systems, and the sector's size increase its exposure to ransomware attacks.

## Types of Cyberattacks Reported in Florida Transportation Sector




Note: Florida's Transportation sector meets DHS ransomware readiness standards at only 18.5%. This is well below Energy (31%) and Financial Services (35%). The low score reflects outdated systems and fragmented oversight while also showing limited testing of response plans.

## State-Funded Resources & Education

### Technical Tools

- **CISA Ransomware Readiness Assessment (CSET)**
- **TSA Pipeline Cybersecurity Guidelines** *(Relevant to Transit & Freight)*

### Templates & Planning

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

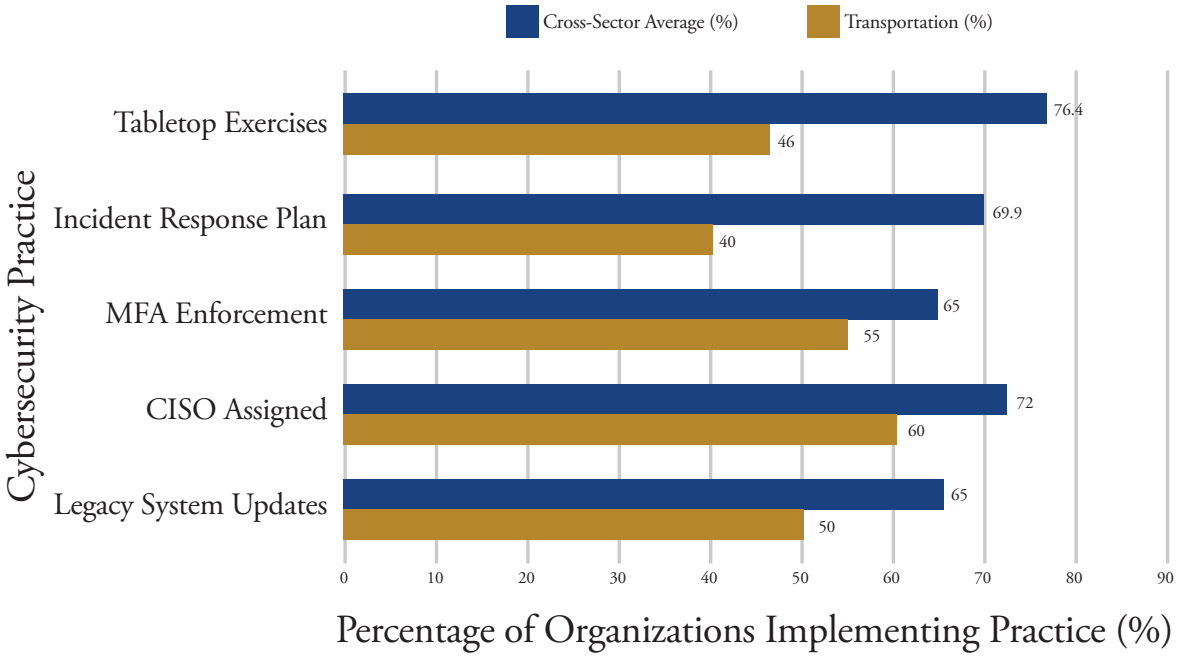
### State-Funded Resources

- **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

# TRANSPORTATION SYSTEMS/LOGISTICS SECTOR CYBERSECURITY

## Ransomware Readiness Gaps Transportation/Logistics (2024)




Note: In 2024, Transportation scored 46% for tabletop exercises and 40% for Incident Response Plans, compared to cross-sector averages of 76.4% and 69.9%. MFA use was 55% (vs. 65%), CISO assignment 60% (vs. 72%), and legacy system upgrades 50% (vs. 65%). The largest gaps are in testing and planning for ransomware incidents.

## Notable Incidents

- **Jacksonville Port Authority (2023):** Targeted ransomware attempt disrupted internal communications; mitigated before major cargo delays occurred.
- **Port of Houston (2021):** Nation-state actors exploited a zero-day in port management software, nearly disrupting critical supply chains.
- **Orlando International Airport Vendor Breach (2022):** A third-party baggage handling software vendor was compromised, briefly delaying flight operations.
- **Fidelity National Financial (2023):** Ransomware disrupted document processing and shipping coordination, delaying property transactions.

## Action Checklist

- Develop and test ransomware-specific Incident Response Plans for port, airport, rail, and freight operations
- Enforce MFA for remote vendor access, logistics platforms, and operational control systems
- Conduct annual tabletop drills simulating disruptions in cargo handling, air traffic & transit scheduling
- Replace or securely segment legacy logistics, cargo & SCADA control systems
- Assign a dedicated cybersecurity lead (CISO or equivalent) with transportation OT expertise
- Maintain offline, immutable backups of scheduling, routing & cargo tracking data; verify restoration quarterly

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