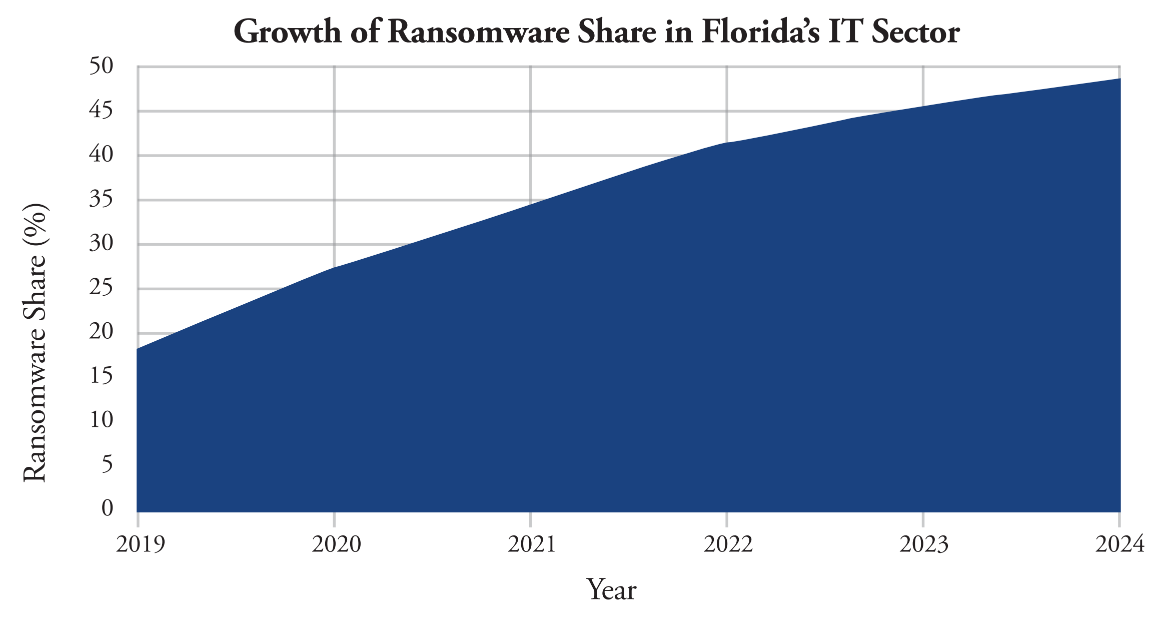
INFORMATION TECHNOLOGY SECTOR CYBERSECURITY

Sector Overview

This resource is for stakeholders in Florida's Information Technology sector. It includes cloud service providers, data centers, software developers, managed service providers (MSPs), telecommunications companies, and IT infrastructure firms. The sector supports economic, government, and security operations statewide. Ransomware disruptions can halt essential services, compromise sensitive data, and threaten both the economy and public safety.

Ransomware Threat Profile

Only 18.5% of Florida IT organizations meet DHS ransomware readiness standards. This places the sector below the statewide average. IT providers face heightened risks due to their links to other sectors, reliance on cloud infrastructure, and the rapid evolution of attack techniques.


Growth of Ransomware Share in Florida's IT Sector

Note: Ransomware made up just 18% of cyber threats in Florida's IT sector in 2019 but reached 48% by 2024, a 167% increase over six years. This trend shows how ransomware has become one of the most common threats facing IT systems statewide.

Top Vulnerabilities

▶ **High-Value Supply Chain Targets**

- MSPs and cloud providers often serve multiple sectors, making them prime targets for ransomware-asa-service (RaaS) campaigns that cause widespread downstream impact.

▶ **Unpatched or Unsupported Legacy Systems**

- Older operating systems, database platforms, and management tools remain active in production environments, exposing known vulnerabilities.

▶ **Inadequate Ransomware Testing**

- Fewer than half conduct ransomware-specific tabletop exercises that simulate multi-client or multiplatform disruptions.

▶ **Weak Cloud Access Controls**

- Gaps in MFA enforcement, privileged access monitoring, and API security expose customer environments to compromise.

▶ **Rapid Exploit Development in RaaS Markets**

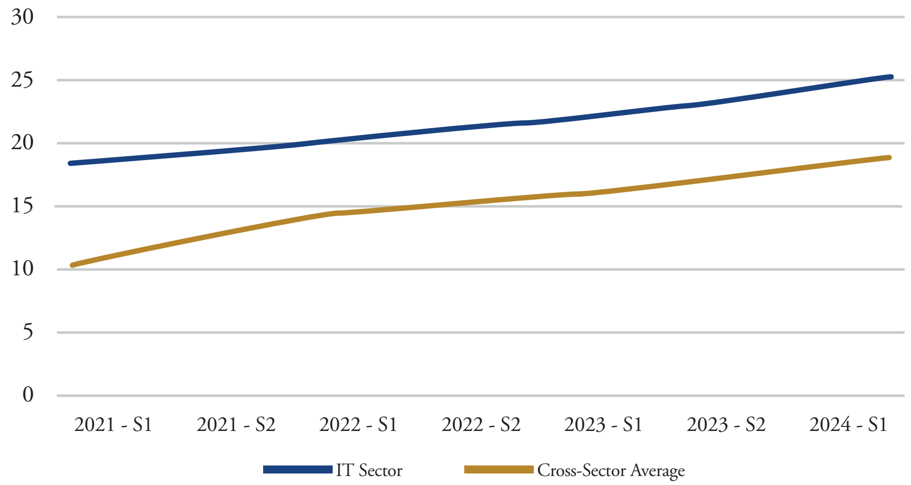
- Criminal groups quickly weaponize zero-day vulnerabilities targeting IT management platforms, forcing providers to reduce patch deployment times.

INFORMATION TECHNOLOGY SECTOR CYBERSECURITY

Action Checklist

- Develop and test ransomware-specific Incident Response Plans that include multi-tenant systems, managed service environments & client recovery coordination.
- Enforce Multi-Factor Authentication (MFA) on all privileged accounts, cloud administration portals, developer repositories, & API endpoints.
- Patch or replace unsupported operating systems, database platforms & management tools in production environments.
- Conduct annual ransomware tabletop drills simulating supply chain compromise or simultaneous multi-client impact.
- Implement continuous vendor risk assessments with contractual requirements for MFA, logging, and incident reporting within 24 hours.
- Maintain offline, immutable backups of client configurations, code repositories & service management data; verify recovery monthly.

Growth in Full Ransomware Readiness Compliance (2021-2024)



Notable Incidents

- **MOVEit Transfer Breach (2023):** Cybercriminals exploited a critical vulnerability in the widely used file transfer software MOVEit, compromising sensitive data from numerous Florida-based organizations across healthcare, government, and education sectors.
- **Rackspace Technology Ransomware Incident (2023):** A ransomware attack caused prolonged outages for cloud-hosted email services. Florida customers in government, healthcare, and education sectors were among those affected, disrupting daily operations and communications.
- **Kaseya VSA Attack (2021):** A large ransomware attack targeted Kaseya's IT management software, affecting numerous MSPs and thousands of downstream customers, highlighting extensive supply chain vulnerabilities.

Note: From 2021 to 2024, the share of Florida IT providers fully meeting DHS ransomware readiness standards grew from 10.0% to 18.5%. During the same period, the cross-sector average rose from 18.0% to 25.0% and remained consistently ahead of the IT sector.

State-Funded Resources & Education

Technical Tools

- **CISA Ransomware Readiness Assessment (CSET)**
- **CISA 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)
- **Cloud Security Alliance Best Practices**

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)