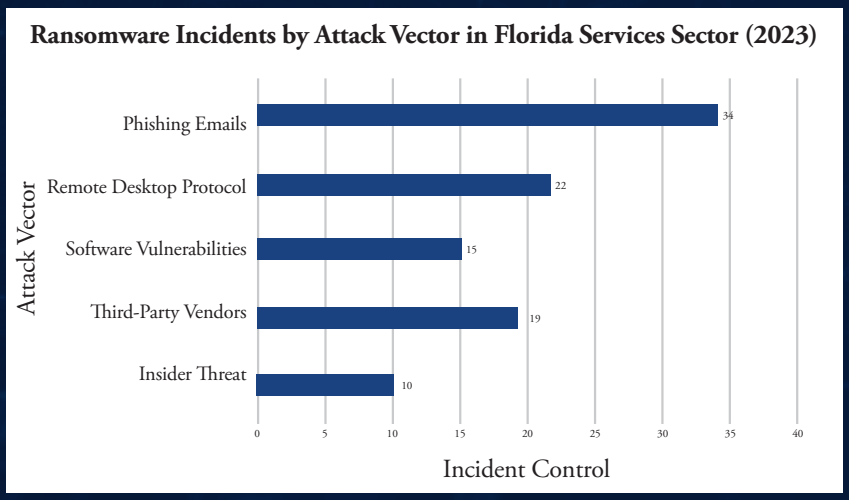
FINANCIAL SERVICES SECTOR CYBERSECURITY

Sector Overview

This resource is intended for stakeholders in Florida's Financial Services sector. It includes banks, credit unions, insurance companies, investment firms, and financial transaction processors. This sector supports the state's economy and daily financial activities. Services range from personal banking to large-scale economic transactions. Ransomware attacks can lead to major financial losses, data breaches, and loss of public trust. This sector is a frequent ransomware target because of its access to liquid assets and time-sensitive financial operations. It is seen as a high-reward opportunity with strong pressure to pay quickly.

Ransomware Threat Profile

Around 35% of Florida's financial organizations meet the Department of Homeland Security's basic cybersecurity standards. This is a relatively strong level of readiness compared to other sectors. Even so, the sector remains a frequent target. It handles critical financial data and operates on complex, connected digital networks. These conditions make it attractive to ransomware groups. Attackers are increasingly focusing on staff who handle payments, loans, or wire transfers. These employees are often targeted through phishing emails or fake login portals that mimic internal systems.



Note: Phishing accounted for 34 incidents, making it the top entry point for ransomware in the sector. RDP vulnerabilities followed with 22 cases, while third-party vendor compromise led to 19. Insider threats and software flaws contributed to 10 and 15 incidents, showing that both technical and human factors remain key risks.

Top Vulnerabilities

- **High-Value Data Targeting**
  - Financial institutions store large volumes of sensitive personal and transactional data, making them especially lucrative targets for extortion-based ransomware attacks.
- **Payment System Exposure**
  - Ransomware can disrupt internal banking systems that support ACH, payroll, or trading operations. These outages can halt core financial transactions and damage business continuity.
- **Regulatory Complexity**
  - Complex and evolving compliance standards (e.g., GLBA, PCI-DSS) can dilute focus on proactive ransomware defenses, as resources are diverted toward audit preparation and reporting.
- **Customer Service Dependencies**
  - Online banking portals, mobile apps, and ATM networks are frequent ransomware targets due to their public-facing nature. Outages can trigger widespread customer panic and reputational damage.
- **Fraud and Insider Threats**
  - The sector is susceptible to internal misuse of privileged access. Ransomware gangs have increasingly recruited disgruntled employees or monetized access gained through financial phishing campaigns.

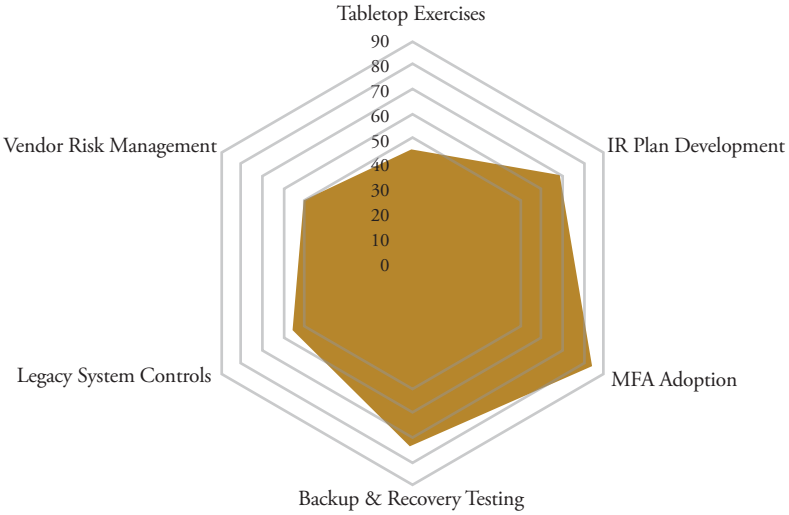
FIU Jack D. Gordon Institute for Public Policy
JGI@fiu.edu
CYBER FLORIDA AT THE UNIVERSITY OF SOUTH FLORIDA

FINANCIAL SERVICES SECTOR CYBERSECURITY

Action Checklist

- Develop and test a ransomware-specific Incident Response Plan
- Enforce Multi-Factor Authentication (MFA) across all systems
- Conduct ransomware tabletop exercises at least once per year
- Audit all third-party vendors for cybersecurity compliance
- Secure and regularly test backups of financial and customer data
- Patch and update all systems involved in transaction processing
- Assign a dedicated cybersecurity lead (CISO or equivalent)

Basic Ransomware Readiness by Category in Financial Services Sector (2023)



Note: MFA adoption reached 85%. Backup testing scored 75%, but only 45% conducted tabletop exercises. The lowest category was vendor risk management at 50%, showing gaps in external oversight compared to internal controls. These scores remain mixed compared to national targets, where 60% adoption is considered the minimum standard for readiness in each category.

Notable Incidents

- **Suncoast Credit Union Service Disruption (2024):** A cyberattack caused several days of outages for online banking and ATM services across the Tampa Bay area. The cause was not confirmed, but the pattern matched typical ransomware activity.
- **Municipal Credit Union Phishing-Ransomware Hybrid (2023):** A credit union in Central Florida was hit with ransomware following a phishing email. Internal records were encrypted. Online banking and loan services were temporarily disabled.
- **Diebold Nixdorf Attack (2023):** A ransomware incident disrupted ATM and payment systems nationwide, including many in Florida. As a core third-party service provider to banks and credit unions, the disruption had downstream effects on customer access and financial operations.
- **Travelex Ransomware Attack (2020):** Travelex was hit with ransomware in 2020, disrupting global currency exchange services. Florida airport kiosks are an example of those affected. The attack exposed financial networks to international ransomware threats.

State-Funded Resources & Education

Technical Tools

- **CISA Ransomware Readiness Assessment(CSET)**
- **Financial Services Information Sharing and Analysis Center (FS-ISAC)**

Templates & Planning

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

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