COMMERCIAL FACILITIES SECTOR CYBERSECURITY

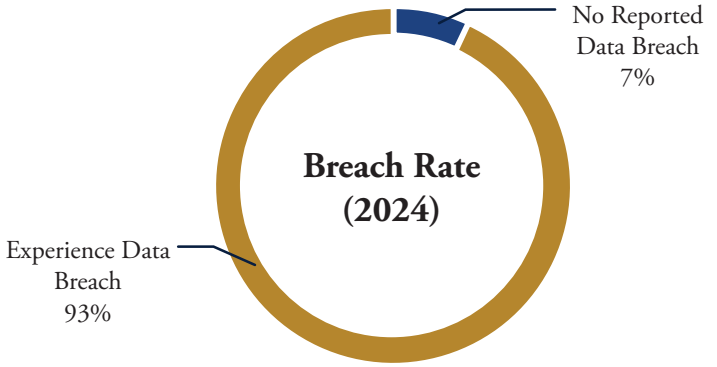
Sector Overview

This resource is for stakeholders in Florida's Commercial Facilities sector, which includes:

- Convention centers
- Entertainment venues
- Hotels
- Office complexes
- Shopping centers
- Sports arenas

These facilities host large public gatherings, provide essential business space, and generate significant economic activity. Many are privately owned but serve public functions. A ransomware incident could shut down reservation systems, disrupt building operations, compromise payment data & create safety hazards during events.

Florida Commercial Construction Firms



Note: An overwhelming 93% of Florida's commercial construction firms have suffered a data breach in the past three years. Many are tied to commercial facility operations. These gaps show the urgent need for stronger planning and access controls as well as improved recovery testing.

Ransomware Threat Profile

Roughly 30% of Florida's commercial facilities meet the Department of Homeland Security's (DHS) basic ransomware readiness standards, which are above some sectors but still leaves considerable exposure. Facilities are increasingly reliant on building automation systems, cloud-based reservations, and digital payment platforms. The combination of public access, high transaction volume, and integration with third-party vendors makes the sector an appealing target for ransomware groups seeking financial gain and large scale disruption.

Notable Incidents

- **Las Vegas Casino & Hotel Breach (2023):** Ransomware disrupted hotel check-in systems, gaming floors & payment operations, forcing manual check-ins & causing millions in losses. Florida's hospitality & entertainment venues face similar risks.
- **Ticketing Platform Ransomware Attack (2022):** An international ticket vendor was hit by ransomware, delaying multiple major sporting events in the U.S., including Florida venues.
- **Florida Resort Chain POS Breach (2021):** Across multiple properties, a ransomware attack crippled point-of-sale terminals, disrupting guest services and exposing payment card data.

State-Funded Resources & Education

Technical Tools

- **CISA Ransomware Readiness Assessment (CSET)**
- **PCI Security Standards Council Resources**

Templates & Planning

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

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

COMMERCIAL FACILITIES SECTOR CYBERSECURITY

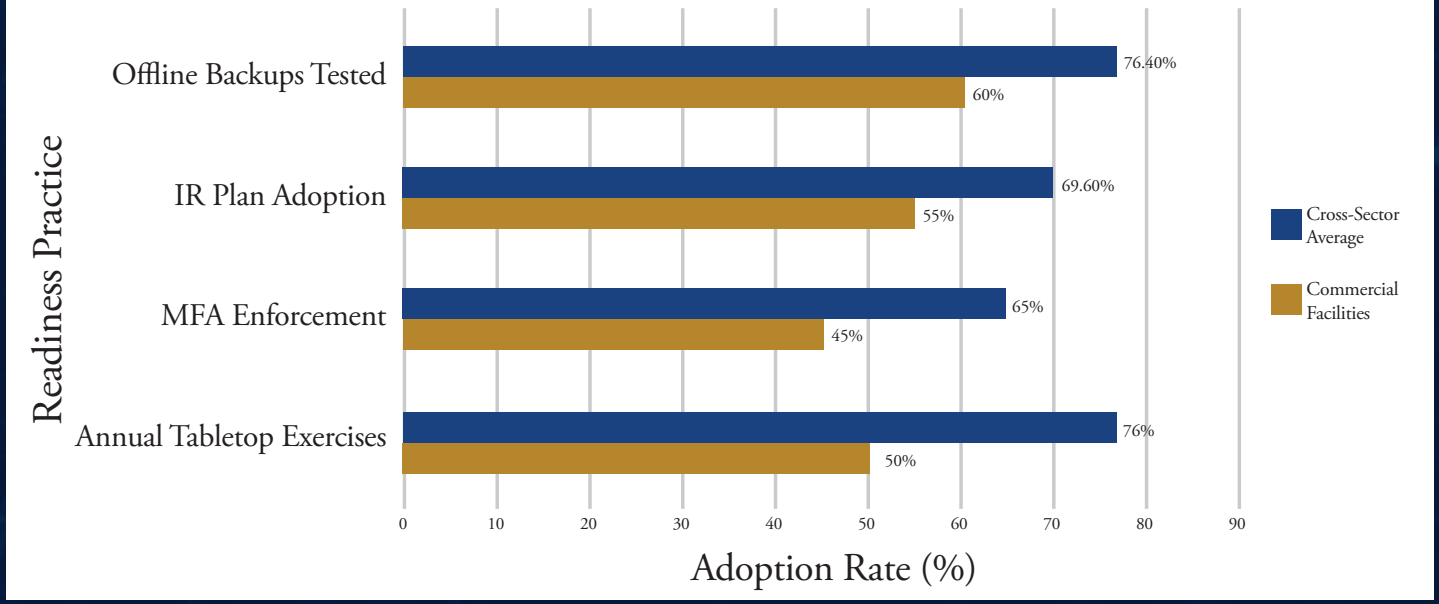
Action Checklist

- Develop and test ransomware-specific Incident Response Plans covering POS, building automation, and reservation systems
- Enforce MFA for all vendor and POS access as well as building management systems using phishing-resistant authentication where possible
- Conduct annual tabletop exercises simulating high-traffic event disruptions, ticketing outages, and payment system compromise
- Segment building automation networks from public Wi-Fi, POS, and administrative systems
- Maintain offline, immutable backups of critical operational configurations, event schedules, and transactional data
- Require cybersecurity clauses in vendor contracts, including 24-hour incident reporting, MFA, and logging

Top Vulnerabilities

- **Building Automation & Access Control Weaknesses**
  - HVAC and lighting systems along with elevators and electronic entry controls often run on legacy or unpatched software, which can be encrypted by ransomware, affecting safety and operations.
- **High-Volume Point-of-Sale (POS) Systems**
  - Payment kiosks, box office terminals, and restaurant POS systems are frequent ransomware targets due to their exposure & potential for mass financial theft or disruption.
- **Event-Driven Operational Pressure**
  - Large events and tourism seasons create "no downtime" windows that ransomware groups exploit to pressure victims into paying quickly.
- **Third-Party Vendor Risks**
  - Ticketing services, property management firms, and payment processors with remote access can serve as indirect entry points for attackers
- **Limited Incident Response Drills**
  - Many facilities have physical security plans but few conduct ransomware-specific tabletop exercises simulating disruptions during high-profile events.

Ransomware Readiness Benchmarks for Commercial Facilities



Note: Commercial Facilities score 50% for tabletop exercises and 45% for MFA enforcement, compared to averages of 76.4% and 65%. Incident Response plan adoption is 55% versus 69.9%, and backup testing is 60% versus 76.4%. These gaps show the need for stronger planning and access controls as well as improved recovery testing across the sector.

FIU Jack D. Gordon Institute for Public Policy

JGI@fiu.edu

CYBER FLORIDA AT THE UNIVERSITY OF SOUTH FLORIDA