

SOUTH FLORIDA CYBER THREAT OUTLOOK

Key Trends. Emerging Risks.
Practical Strategies for a More
Resilient Tomorrow.



REAL-WORLD THREAT TRENDS

Insights from global
and regional data



INDUSTRY RISK ANALYSIS

Key considerations
for South Florida
businesses



PRACTICAL RECOMMENDATIONS

Actionable steps
to strengthen
your security posture



A MORE RESILIENT FUTURE

How Acordis helps
organizations
stay ahead

PROTECTING TODAY.
EMPOWERING TOMORROW.

MIAMI | FORT LAUDERDALE | SOUTH FLORIDA

01 / THE LANDSCAPE

EXECUTIVE OVERVIEW

For organizations across Miami-Dade, Broward, and South Florida, cybersecurity is a business continuity priority.

Cloud adoption, distributed systems, remote access, and expanding vendor ecosystems create opportunities for growth while increasing the importance of layered security.

This report translates national threat research into practical considerations for the region's healthcare, hospitality, maritime, public-sector, and commercial organizations. It is not based on proprietary Acordis endpoint telemetry or a locally representative incident dataset.

SIGNALS FROM NATIONAL RESEARCH

44%

of breaches involved ransomware (Verizon 2025 DBIR)

\$2.77B

reported U.S. BEC losses in 2024 (FBI IC3)

What the numbers mean

National data does not establish a South Florida attack rate. It does show why organizations should focus on recovery, identity protection, vulnerability management, and employee verification procedures instead of relying on a single defensive tool.

Regional perspective

South Florida's mix of healthcare providers, tourism businesses, cruise and maritime operations, public services, and professional firms creates varied technology environments. Security controls must be adapted to each organization's operations and risk tolerance.

02 / THREAT CATEGORIES

Five risks to prioritize

- **01 Ransomware & business interruption**

Maintain protected backups, tested recovery procedures, endpoint detection, segmentation, and an incident response plan.

- **02 Business email compromise**

Use phishing-resistant MFA, out-of-band payment verification, email controls, and targeted staff awareness.

- **03 Unpatched infrastructure**

Maintain asset visibility, prioritize exploited vulnerabilities, and track remediation across servers, network devices, and remote access.

- **04 Cloud & identity exposure**

Review privileged access, cloud configurations, dormant accounts, and centralized authentication policies.

- **05 Third-party access risk**

Assess vendor access, require appropriate safeguards, and establish notification and response responsibilities.

Leadership question

If a critical system were unavailable tomorrow, would your organization know who owns recovery, which services are most important, and how quickly they can be restored?

03 / BUSINESS IMPACT

Industry-specific considerations

- **Healthcare**
Protect clinical operations, connected devices, patient-facing systems, and access to sensitive information.
- **Hospitality**
Secure guest-facing technology, payment environments, property networks, and distributed locations.
- **Cruise & maritime**
Address remote connectivity, segmentation between operational and business systems, and geographically distributed infrastructure.
- **Public sector**
Prioritize continuity of essential services, legacy systems, and documented recovery responsibilities.
- **Professional services**
Focus on account compromise, confidential client information, payment fraud, and secure collaboration.

Important interpretation

These are sector-specific risk considerations—not a ranking of which South Florida industries experienced the most attacks.

ACORDIS ACTION PLAN

Your next steps

- **First 30 days**

Inventory critical assets and privileged access; review backup health, patch exposure, and MFA coverage.

- **Days 31–60**

Close high-risk gaps, improve monitoring visibility, and formalize escalation and response ownership.

- **Days 61–90**

Test restoration and incident response, review third-party access, and establish a leadership reporting cadence.

LET'S BUILD A SMARTER TECHNOLOGY STRATEGY

Talk to an Acordis expert.

Explore the right next steps for your organization's security, infrastructure, and technology priorities.

www.acordiscorp.com

RESEARCH NOTES & LIMITATIONS

References: Verizon, 2025 Data Breach Investigations Report (verizon.com/business/resources/reports/dbir/); FBI IC3, 2024 Internet Crime Report (ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf). Statistics are U.S./global research findings, not Acordis or South Florida-specific telemetry. General guidance only.