Cybersecurity for Finance

As a financial institution, you are entrusted to properly manage and protect clients' assets and remain in compliance with strict regulations and requirements. When extremely sensitive and valuable data is involved, including personally identifiable information (PII), banking and checking, credit card information and financial records, a loss or breach can jeopardize your reputation, customer loyalty and could result in hefty fines and legal repercussions. **There are some alarming stats that articulate cybersecurity risks in finance and banking to be aware of:**

Financial institutions are ***300 times*** more vulnerable to cybersecurity incidents than other sectors. (Boston Consulting Group)

70% of the financial companies have experienced security incidents in the last 12 months, with leading causes being failure to follow security protocol and BYOD. (Clearswift)

The cost of cyberattacks is highest in the banking industry, reaching ***$18.3 million annually*** per company. (Accenture)

Only 31% of financial institutions are good at preventing cyberattacks. (Ponemon Institute)

Attacks on banks and other financial institutions ***spiked by 38%*** between February and March 2020, accounting for 52% of all attacks. (VMware's Carbon Black Cloud)

Solutions to Address Common Challenges and Concerns

Next Generation Firewalls (NGFW), intrusion detection systems (IDS), and intrusions prevention systems (IPS) not only inspect incoming/outgoing network traffic but add crucial security features like application awareness and control, intrusion prevention/detection, and cloud-delivered threat intelligence

Threat Detection and Response (TDR) services recognize and respond to malicious activity fast, offering 24/7 monitoring and threat isolation – the sooner a threat is detected, the quicker action can be taken, lowering the chances of catastrophic results

Security Information and Event Management (SIEM) tools log all incident files, filter out false positives, and present valid warnings and alerts in one central, unified view for quick and efficient triage

Vulnerability Scans identify open ports, vulnerabilities, unusual traffic patterns and can tighten up cybersecurity plans

Strict BYOD Policies and approved whitelist apps help prevent data breaches caused by employees using personal devices; ongoing employee training and education is strongly recommended with human error accounting for 32% of attacks and 24% of unauthorized data shares

Endpoint Security ensures computers, laptops, phones, or tablets, have the latest protection from viruses, trojans, malware, spyware, and other malicious advanced persistent threats

Two-factor Authentication requires two types of credentials for authentication before an end-user is granted access, adding a layer of validation, reducing a threat actor's attack surface and ability to gain unauthorized access to a sensitive data

Managed Security Services lend enterprise-level security expertise, commonly offering 24/7 protection, multi-layered defense approach and specialized compliance solutions following NIST, ISO, ISACA, and FFIEC guidelines and GLBA and SOX standards

Get a professional security assessment. Plans and security postures change and should be reviewed regularly to identify vulnerabilities and avoid data breaches.

Email info@techguidance.com or call 855.898.0655.

techguidance
Powered by TBI