Navigating Cybersecurity Challenges in the Financial Services Industry: A 2024 Overview

March 28, 2024

Ransomware payments hit $1.1 billion in 2023, a record high and twice what they were in 2022. We see similar activity in early 2024 as the number of ransomware gangs continues to increase. In 2024, the financial services industry continues to face formidable cybersecurity challenges, spurred by the relentless evolution of technology and the persistent ingenuity of cybercriminals. As financial organizations increasingly rely on digital platforms and data-driven processes, they become more susceptible to cyber threats ranging from ransomware attacks to data breaches.

The key cybersecurity issues confronting the financial sector in 2024 will include emerging threats, the evolving regulatory landscape and strategies for safeguarding sensitive information and maintaining trust in an interconnected world.

Evolving Threat Landscape

The evolving threat landscape is varied and becoming more sophisticated by the day. Here are some of the most insidious threats:

- Ransomware: Ransomware remains a significant threat to financial firms, with cybercriminals employing sophisticated techniques to encrypt critical data and demand hefty ransom payments. In 2024, ransomware attacks have become more targeted and coordinated, leveraging advanced encryption methods and zero-day vulnerabilities to infiltrate systems. Also on the rise are “triple extortion” techniques where not only is the data encrypted and held hostage for ransom, it is exfiltrated and sold on the dark web and finally key regulators are being informed by the attackers as an additional means to extort payments due to non-compliance.
- Social engineering*:* Social engineering is the psychological manipulation of people into performing actions or divulging confidential information. It is a more sophisticated form of phishing in that it is often one of many steps in a more complex fraud scheme and is designed to build trust in a target rather than simply catch someone unaware. Social engineering attacks aimed at companies in all industries, including the financial sector, are rapidly growing.
- Use of artificial intelligence (AI) and other emerging technologies: Cyber criminals are increasingly using generative AI technology for social engineering efforts, to create more realistic and convincing phishing email campaigns and using it to generate more advanced and effective ransomware codes. Some other effective use of technology is to evade multi-factor authentication (MFA) which includes SIM-swaps, token capture or just overwhelm employees who have MFA fatigue.
- Insider threats: Insider threats pose a persistent challenge to the financial industry, as malicious insiders or negligent employees can exploit their access to sensitive information for personal gain or inadvertently compromise data security. Enhanced monitoring tools and robust access controls are crucial for mitigating insider threats and preventing unauthorized access.
- Supply chain vulnerabilities: Financial organizations are increasingly reliant

on third-party vendors and service providers for various functions, exposing them to supply chain vulnerabilities. Cyberattacks targeting supply chain partners can have cascading effects on the financial ecosystem, underscoring the importance of vetting vendors and implementing rigorous security standards. Financial organizations must continue to identify critical third-party vendors, understand the data and information shared with vendors and ensure that vendors have stringent controls in place to protect data shared between the organizations. Controls must also include regular monitoring of vendors.

Regulatory Landscape

Compliance with growing cybersecurity regulatory requirements, both at the federal and state levels, will continue to be a major focus for financial companies in 2024.

- Regulatory agencies: SEC rules that went into effect in December 2023 require financial organizations to disclose material cybersecurity incidents within four business days. The rules also require public companies to disclose their processes for assessing, identifying and managing material risks, as well as the cybersecurity oversight responsibilities of their boards and executive management, in annual reports. Financial organizations must ensure that processes for identifying and managing cyber risks are in place, and procedures for determining materiality are constantly reassessed.
- NYDFS regulations: Amendments to the New York Department of Financial Services cybersecurity regulations, passed in November 2023, expand security incident reporting requirements to include ransomware attacks that hit a material part of a covered organization’s network, and further require reporting of any extortion payments within 24 hours.
- FTC reporting requirement: The Federal Trade Commission made recent amendments to the Safeguard Rule under the Gramm-Leach-Bliley Act requiring non-banks to report certain breaches within 30 days. The reporting requirement is triggered when the information of 500 or more consumers is acquired without authorization. Nonbanking organizations must ensure that incident response plans and procedures include these new reporting requirements, which becomes effective on May 13, 2024.

Increased Enforcement and Litigation

Regulatory agencies are ramping up their oversight of cybersecurity practices in the financial sector, conducting regular audits and assessments to evaluate companies' preparedness and resilience against cyber threats. Non-compliance with regulatory requirements can result in significant fines, reputational damage, and legal consequences, prompting organizations to prioritize cybersecurity investments and governance.

Enforcement actions, which skyrocketed in 2023, are expected to continue rising around such issues as improper password storage, failure to manage third-party risk and lack of proper risk assessment policies and procedures.

Additionally, the rise in class-action lawsuits stemming from large data breaches can be expected to continue. Financial organizations must account for the significant regulatory and legal consequences that may arise after a material incident or by failure to implement required controls.

Cross-Border Considerations

As financial transactions increasingly transcend national borders, regulatory compliance becomes more complex, requiring financial companies to navigate a patchwork of international regulations and data privacy laws. Harmonizing compliance efforts across jurisdictions while accommodating regional nuances poses a formidable challenge for multinational financial organizations.

Cybersecurity Best Practices

A number of strategies to protect against cyberattack have become standard operating procedure in many organizations, inside the financial industry and outside, including:

- Partner with cybersecurity consultants who can bring expertise and an outside perspective to your organization and identify weaknesses and vulnerabilities.
- Review incident response plans regularly to ensure they are up to date with

changing regulatory and legal requirements.

- Develop policies and procedures to determine materiality.
- Conduct exercises that run a variety of scenarios and determine if your incident response plan is adequate.
- Assess vendor management protocols.
- Engage senior leadership and board members with cybersecurity training and briefings on the organization's incident response plans and procedures.
- Create a risk assessment and management plan to identify potential threats, vulnerabilities and impact scenarios.
- Engage in collaboration and information sharing among industry stakeholders, government agencies and cybersecurity experts.
- Implement cybersecurity awareness training for all employees on a regular basis, including cyberattack simulations.

How Anchin Can Help

The cybersecurity landscape in the financial services industry continues to evolve rapidly in 2024, driven by emerging threats, regulatory developments and technological advancements.

For further information on how your organization can protect itself from cyberattacks, please reach out to Russ Safirstein, President and CEO of Redpoint Cybersecurity, or your Anchin Relationship Partner.