Cybersecurity Issues For Financial Industry To Track In 2024

By **Alex Koskey and Matt White** (January 2, 2024)

Alex Koskey

Matt White

Cybersecurity will continue to be one of the most significant challenges financial institutions will face in 2024.

Financial institutions will confront new federal, state and industry regulations that require additional policies and procedures, enhanced proactive security measures, and timely disclosure of security incidents.

Meanwhile, the financial industry continues to be among the top targets of threat actors launching increasingly sophisticated cyberattacks, including using emerging technologies such as artificial intelligence, in what is a quickly and continuously evolving threat landscape.

This article will highlight some of the key issues and critical considerations that will test the cyber resiliency of financial institutions in 2024, and will provide recommended best practices to help financial institutions protect themselves and their customers going into the new year.

New Cybersecurity Regulations

Among many new rules and regulations, there are three new cybersecurity regulations in particular that will be at the forefront of cybersecurity regulatory and compliance for financial institutions in 2024: (1) the U.S. Securities and Exchange Commission's cybersecurity disclosure rules; (2) new amendments to the New York State Department of Financial Services' cybersecurity regulation; and (3) the Federal Trade Commission's security breach notification requirement for nonbanks.

SEC's Cybersecurity Disclosure Rules

The SEC's long-awaited rules went into effect in December and require public companies to disclose material cybersecurity incidents within four business days of determining an incident is material. The rules further require public companies to disclose, among other things, their processes for assessing, identifying and managing material risks for cyber threats, as well as the cybersecurity oversight responsibilities of their board and executive management, in their annual reports.

Although planning for these rules has likely been ongoing for several months, publicly traded financial institutions will continue to grapple with these new requirements into 2024. Notably, financial institutions must ensure that processes for identifying and managing cyber risks are in place and procedures for determining materiality are continually assessed and simulated during tabletop exercises.

Additionally, companies will need to be prepared for additional regulatory scrutiny and even litigation resulting from these new disclosure requirements.

Amendments to NYDFS Cybersecurity Regulation

Financial institutions must also address new amendments to the NYDFS' cybersecurity regulation passed in November. The amendments expand security incident reporting requirements to include incidents where ransomware is deployed to a material part of the covered entity's network and mandate reporting of any extortion payments within 24 hours of payment.

Financial institutions also face comprehensive requirements for enhanced security controls including, among other things, endpoint security, access controls, vulnerability management, and specific requirements for incident response and disaster recovery plans.

FTC Security Breach Requirement for Nonbanks

Following the FTC's recent amendments to the Gramm-Leach-Bliley Act Safeguards Rule, the FTC further amended the rule to require nonbanks to notify the FTC of certain security breaches within 30 days.

The reporting requirement is triggered when the information of at least 500 consumers is acquired without authorization. Nonbanking financial institutions must ensure that incident response plans and procedures incorporate these new reporting requirements, which go into effect May 13.

Evolving Threat Landscape

The threat landscape will undoubtedly continue to evolve in 2024 as threat actors increasingly use emerging technologies to exploit vulnerabilities. Financial institutions should be vigilant in detecting and defending against the following.

Advanced Social Engineering and Phishing Attacks

Threat actors are using sophisticated social engineering attacks to target and manipulate employees, including IT help desk representatives, into disclosing login credentials and other sensitive information.

Financial institutions should ensure that employees are aware of these targeted attacks and further refine policies and procedures regarding the disclosure of such information. Threat actors are also using generative AI technology to create more persuasive phishing email campaigns, and doing so in a variety of languages, making phishing attacks more harmful than ever.

Financial institutions must continue efforts to train employees to avoid these campaigns, and in parallel, should consider new anti-phishing technologies that can reduce the volume of these attacks.

Evolving Ransomware Attacks

While the concepts of encryption and data exfiltration are nothing new for ransomware attacks, threat actors have continued to add layers to their attempts to extort organizations

into paying ransoms.

Notably, many threat actors have so-called leak sites where they publish the names — and data — of their victims and are now sending communications to third parties and customers notifying them that their data is at risk with greater frequency.

In light of new regulatory reporting requirements, financial institutions should be persistent in implementing controls to detect and prevent ransomware attacks along with procedures to efficiently respond to such attacks when they occur. Financial institutions should also be regularly testing these procedures through tabletop exercise to ensure their incident response team is prepared when an attack happens.

Deepfakes and Artificial Intelligence

Threat actors will continue to build on the use of emerging technologies like artificial intelligence to perpetrate financial fraud and other similar attacks against financial institutions.

In particular, threat actors are likely to continue the use of so-called deepfakes to create fake images, audio or videos of individuals to initiate an unauthorized wire transfer or other financial loss.

Financial institutions must continue to consider these issues as a component of cybersecurity preparedness and develop policies and strategies, including the use of AI-based technologies, to combat these fraudulent activities.

Heightened Regulatory Enforcement and Litigation

As cybersecurity regulatory requirements continue to expand, financial institutions should also expect to see heightened regulatory scrutiny and increased litigation. Last year saw a litany of enforcement actions against financial service companies, resulting in millions of dollars of penalties, around alleged violations relating to improperly stored passwords, failure to manage third-party risk, and a lack of risk assessment policies and procedures.

Meanwhile, the exponential rise in data breach class action litigation is likely to continue into 2024. Therefore, financial institutions must account for the significant regulatory and legal consequences that may arise after experiencing a security incident or by failing to implement required controls within their compliance programs.

Vendor Management and Supply Chain Risk

Supply chain attacks dominated headlines last year as threat actors exploited vulnerabilities with critical third-party vendors used by financial institutions. On the heels of the new interagency guidance on third-party relationships, financial institutions must continue to refine third-party risk management procedures.

This includes, among other things, identifying critical vendors, understanding the information shared with such vendors, ensuring that third-party vendors have effective controls in place to protect against evolving cyber threats, and monitoring those vendors on

a routine basis.

Due diligence remains an integral part of this process and, with evolving regulatory requirements, financial institutions must perform a comprehensive evaluation of third-party vendors to assess and understand potential risks. It is also more important than ever for financial institutions to have appropriate contract provisions in place to help protect the institution and their customers' information in the event of a data incident.

Best Practices for Financial Institutions in 2024

2024 is shaping up to be a critical year for financial institutions in addressing new regulatory requirements and being prepared to defend against evolving cyber threats. Below are several best practices that financial institutions should implement going into the new year.

Review incident response plans.

New regulations require financial institutions to report cybersecurity incidents to designated regulators and/or have written incident response plans.

While having an incident response plan has been a best practice for some time, financial institutions should review these plans to ensure that they incorporate reporting requirements under the SEC's cybersecurity disclosure rules, the NYDFS amendments or the FTC's new breach reporting requirements, as applicable.

Develop policies and procedures to evaluate materiality.

Those financial institutions subject to the SEC's cybersecurity disclosure rules should develop and/or refine policies and procedures to evaluate the materiality of a cyber incident. This would include identifying key factors that would make an incident material for the financial institution, the team members involved in assessing materiality, and the requisite chain of communication for relevant information.

It is imperative that financial institutions have sound policies and procedures in place to address these requirements.

Conduct a tabletop exercise.

Financial institutions should also conduct a tabletop exercise to simulate a data incident and test the institution's incident response plan and associated procedures.

Notably, any exercise should emphasize scenarios in which new regulatory reporting requirements may be at issue and test the responsiveness of the incident response team.

Financial institutions must think through these issues during a tabletop exercise in order to be prepared when an actual data incident occurs.

Assess vendor management protocols.

In addition to incident response policies and procedures, financial institutions should also

evaluate existing vendor management protocols to ensure that they appropriately address the new interagency guidelines.

Financial institutions should also review due diligence questionnaires to third-party vendors and current form master agreements used with third-party vendors and update existing language as needed to implement additional requirements for security controls, incident reporting, and audit capabilities. Current vendor agreements lacking appropriate provisions may also need to be amended.

Engage senior leadership and boards.

Engagement by a financial institution's senior leadership team and board of directors on cybersecurity issues is no longer a luxury — it is a necessity. Financial institutions should review and refine processes around how senior leadership is involved in assessing cyber risks and the oversight by the board of directors.

Financial institutions would be best served by providing additional education and training to these respective groups so that they are appropriately prepared to address material cyber risks.

Following the suggestions in this article will help financial institutions prepare themselves to appropriately respond to the litany of new issues they will face this year.

Alex Koskey is a shareholder at Baker Donelson Bearman Caldwell & Berkowitz PC.

Matt White is a shareholder and co-chair of the firm's financial services cybersecurity and data privacy team.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.