Skadden

New Rules, Enforcement Actions Make Financial Institutions' Planning for Cyberattacks Even More Imperative

Contributing Partners

Bao Nguyen / Washington, D.C.

William Ridgway / Chicago

Associate

Danielle Simms / Chicago

Takeaways

- Implementing strong cybersecurity practices helps companies prepare for future regulatory requirements.
- Incident-response plans must enable financial institutions to give timely and accurate notifications to regulators and consumers following a cyber incident.
- Companies should use risk assessments to develop robust cybersecurity programs and test the strength of those programs against known threats.
- Boards must take a leadership role in managing cybersecurity risks.

Growing Threat, Expanding Regulation

A new cybersecurity regulation and recent enforcement activity by federal bank regulators signal heightened regulatory scrutiny for financial institutions in 2022.

In November 2021, the Federal Reserve, the Federal Deposit Insurance Corporation and the Office of the Comptroller of the Currency (OCC) approved a rule that directs banking organizations to report certain cybersecurity incidents to their primary regulator within 36 hours of discovering it, a tighter timeline than current industry standards.

The stricter regulation comes as cyberattacks on financial institutions have grown more frequent and sophisticated. In the first half of 2021, the financial industry experienced a more than 13-fold year-on-year increase in ransomware attacks. Even if attackers are not successful in extracting ransom, these incidents exact a significant toll on financial institutions. The average cost of recovering from a ransomware attack, including those where ransom is paid, stands at $2 million.

Financial institutions should anticipate higher regulatory standards and more cyber-related enforcement actions in 2022. Regulators continue to regard cyberattacks as a major threat to the safety and soundness of individual firms and the broader financial system, and they are using their enforcement powers increasingly to focus the industry and impose discipline to prevent damage.

Institutions can glimpse into the future regulatory environment through recent activity by the New York State Department of Financial Services (NY DFS), the Securities and Exchange Commission (SEC) and the OCC, which have collectively brought over a dozen enforcement actions related to cyber events and assessed over $635 million in fines in the past two years. This activity confirms that enforcement in this space is no longer reserved for outlier cases and serves as a reminder for financial institutions to focus on the following areas in the year ahead.

Establish Processes To Ensure Timely Notifications and Accurate Communications

Given that successful attacks will occur despite preventive controls, key regulators have instructed companies to review, update and test incident-response and business-continuity plans so that they can both quickly recover from a cybersecurity attack and prevent one from impacting the entire network. Response plans should also anticipate attacks against recovery systems and take steps to protect those systems.

Importantly, incident response plans must allow financial institutions to comply with the new notification rule that takes effect in April 2022. These plans should allow companies to quickly:

This article is from Skadden's *2022 Insights*.

One Manhattan West
New York, NY 10001
212.735.3000

- identify and escalate cyber events;
- evaluate the impact of such events;
- contact the primary regulator; and
- for bank service providers, notify banking customers when necessary.

Financial institutions must be able to complete these steps even if a cyberattack renders primary IT systems inoperable.

The 36-hour reporting window under the new federal notification rule is even shorter than NY DFS' 72-hour deadline, and a recent NY DFS action against Residential Mortgage Services, Inc. shows that regulators may penalize organizations that fail to investigate cyber incidents promptly. Financial institutions' incident-response plans must incorporate a process to ensure that incidents are investigated and regulators are notified quickly.

Notifications to Customers Must Be Accurate

Though the new federal notification rule does not require financial institutions to report cyber events to consumers, any misleading or inaccurate communications about cyber events may create liability under other laws. For example, in a recent SEC enforcement action involving compromised email accounts at a group of financial advisory firms, the SEC alleged that the notification to affected customers from outside counsel referred to a "recent" cyber incident and stated that the companies had "learned that an unauthorized individual gained access to" the client's personal identifying information two months prior to the notification, when, in fact, the companies had discovered the breach at least six months earlier.

Routinely Use Third-Party Risk Assessments To Test Cybersecurity Programs

Risk assessments are a fundamental building block of cybersecurity programs. Increasingly, regulators are instructing financial institutions to regularly test the strength of their cybersecurity programs against the particular threats identified during risk evaluations. NY DFS requires periodic penetration testing if an organization does not continuously monitor its systems for vulnerabilities. The OCC likewise recommends that financial institutions use a penetration program that includes periodic internal and external testing of the institution's ability to detect and respond to attacks.

Institutions that conduct these audits should ensure the testing is completed by independent personnel and that the institution addresses any vulnerabilities that are exposed in a timely manner. Indeed, failing to address vulnerabilities identified during testing was one factor cited by NY DFS in a 2020 enforcement action against a title insurance company where hundreds of millions of confidential customer records were disclosed.

Deploy Strong Access Controls

NY DFS requires multifactor authentication for any individual accessing a company's internal network from an external network, unless the company's chief information security officer approves in writing the use of an equivalent or more secure access control. This requirement also applies to third-party applications that access the company's internal network.

Though the OCC does not require one particular technology, it advises companies to have appropriate identity and access management controls that can include using multifactor authentication, limiting user permissions to those necessary for jobs and regularly reviewing the appropriateness of assigned access.

Boards Must Proactively Manage Cyber Risks

Boards should oversee the creation of strong cybersecurity programs, which includes making sure incident-response plans adhere to all relevant laws. Directors must also be involved in decision-making after a cyber event occurs and should hold management accountable for addressing known risks. A McKinsey survey of financial services companies in 2020 suggests best practices. Nearly 95% of the surveyed firms reported that one of their board committees discussed cybersecurity and technology risks four times or more per year. Almost half the companies involved the board in cybersecurity exercises, and nine in 10 provided regular updates on cybersecurity to the full board.

Failing to ensure proper polices are in place to protect the company or issuing misleading statements about the company's preparedness may give rise to personal liability for directors, as reflected in several recent securities class actions. (See our February 3, 2021, client alert "A Practical Guide to the Role of Directors in Fighting Ransomware.")

Companies With Strong Cybersecurity Programs Will Be Better Positioned as New Regulations Are Adopted

As cybersecurity attacks intensify, new cyber-related regulations will continue to be implemented, and not just at the federal level. For example, in 2018, California voters approved the groundbreaking California Consumer Privacy Act (CCPA), which allows consumers to sue companies after certain types of data breaches. Just two years later, voters significantly amended and expanded the CCPA by approving the California Privacy Rights Act (CPRA). The CPRA created a new agency that will issue regulations, including those that require certain businesses to perform annual cybersecurity audits and to submit regular risk assessments.

Financial institutions with strong cybersecurity practices will be better able to adapt to these regulations, and others, as they will already have the foundation required for compliance.