Key Points for Building Cyber Resilience in the Financial Services Sector

For all types of financial services organizations, managing cybersecurity risk and building cybersecurity resilience is a critical necessity given the complex regulatory landscape, rapid digitization, and constantly evolving tactics from malicious actors. Focusing on these six areas can help financial institutions efficiently and effectively distribute their cybersecurity resources to help build cyber resilience.

AUTHORS

Brad Carpenter

FTI Consulting, Cybersecurity Practice

Suzan Rose

Alternative Investment Management Association

IN PARTNERSHIP WITH

AIMA
THE ALTERNATIVE INVESTMENT MANAGEMENT ASSOCIATION

1) Understand Industry Regulation

Several new and updated U.S. regulations – at the state and federal level – have emerged in the past year that present additional compliance requirements for financial services organizations. There is nothing to preclude a municipality from passing additional ordinances related to cybersecurity, much like other areas of regulation.

At a federal level, the Securities and Exchange Commission (SEC) finalized rules in 2023 that require incident disclosure and other increased cybersecurity measures for public companies. The SEC also proposed additional comprehensive rules for investment advisers (February 2022) and for market entities (March 2023) which are pending.

Many states have enacted cybersecurity laws and regulations that must be adhered to if a business or an individual is in scope. Privacy-related protections are most common, but some states have broader cybersecurity rules that reflect many of the concerns addressed by federal rules. For example, in an amendment effective as of April 2024, the New York Department of Financial Services (NYDFS) Part 500 cybersecurity rules require financial services organizations conducting business in New York to

implement preparedness measures including independent audits, risk mitigation strategies for third-party providers, and executive approval of cybersecurity policies.

Understanding what regulation applies to whom, and where, can help organizations prepare in advance of compliance deadlines. Determining a minimum standard to satisfy all regulatory obligations as a starting point for cyber resilience allows organizations to further build out robust cybersecurity programs, positioning them well for the likelihood of additional regulations in the coming years.

2) Identify Critical Assets and Risks

It is challenging to protect against all types of cybersecurity threats. Attempting to do so by spreading finite resources too thin risks all protections being insufficient.

Instead, organizations should determine their most valuable assets, as well as the cybersecurity risks their particular organization is most susceptible to. This is a particularly important strategy for the financial services industry, where small banks and large investment firms are targeted in entirely different ways. Identifying the most critical data and vulnerabilities allows resources to be focused where they are likely to be needed most.

3) Consider Ways to Transfer Risk

When building cyber resilience across an organization, key stakeholders and the C-suite in particular need to determine how much risk their organization is comfortable with owning.

In addition to mitigating cybersecurity risk with proper organizational policies and procedures, investing in cyber insurance can enable an organization to transfer some of the risks posed by cybersecurity incidents to outside parties. When an industry is as highly targeted by threat actors as financial services, cyber insurance policies can reduce the financial and operational risk of a cybersecurity incident.

4) Have an Incident Response Plan in Place

Cybersecurity incidents are an inevitable reality within the financial services industry, but their negative impact can be significantly limited when an organization is prepared to respond immediately. Having a robust incident response plan in place that outlines potential scenarios, the responsibilities of each key stakeholder, all relevant policies and reporting requirements, backup plans for continuing critical operations, and the role of any third parties, such as incident response providers or insurance firms, can save an organization from having to make pivotal decisions under pressure.

Incident response plans should be practiced and refined through incident response simulation training exercises and can be bolstered by having an incident response retainer in place with a third-party firm. Organizations should also maintain a relationship with a cybersecurity contact at the Federal Bureau of Investigation (FBI), which has resources and expertise to assist with incident response.

5) Minimize Risks from Third Parties

As financial services organizations increasingly digitize their operations and rely on third-party service providers who also may do so, new threats and vulnerabilities are introduced to network environments through these connected entities. Organizations must thoroughly vet any potential new external vendors for cybersecurity vulnerabilities before entrusting them with access to valuable data and integrating them into the organizational network.

For current third-party partners, organizations should obtain assurances – or implement contractual obligations - that the entities are regularly updating their cybersecurity policies. Organizations should regularly reevaluate the current access level of third parties to organizational systems and remove any unnecessary access.

By minimizing the risk introduced from external sources, organizations can more confidently build their cyber resilience and properly comply with regulations that have become increasingly focused on third-party cybersecurity risks.

6) Establish a Culture of Cyber Resilience

Boards and senior management should have appropriate knowledge and understanding of cybersecurity issues, taking into account the nature, scale, and complexity of the organization's activities and risk profile.

All three lines of an organization's defense – IT, all other staff, and senior management – should have an effective role in managing cyber risks. Although the second and third lines are not IT-focused, they still should have an appropriate level of knowledge and skill to face threats that challenge the organization. Training is critical to that end, empowering all employees to take an active role in the organization's security. Cyber risk management should not be seen as an isolated responsibility of the IT function but as part of an organization's activities and business as a whole, concerning everyone. It should be a strategic priority.

Cultivating strong culture and awareness among employees also comes down to tone from the top and support from senior management. Engagement by senior management in the development and implementation phases of a cybersecurity program is important. However, such engagement is also essential in the day-to-day operation of that program if it is to be successful. Senior leaders should clearly demonstrate and articulate their commitment to cybersecurity initiatives across the organization.

Without adequate focus on cybersecurity resilience, financial services organizations risk significant financial, reputational, regulatory, and legal consequences. In addition to proactively mitigating risk, a strong cybersecurity program built on a foundation of resilience becomes a value-add. A financial services organization that prioritizes cybersecurity can become more appealing to investors, knowing remediation efforts may be measured and the threat of a significant cybersecurity incident may be reduced. Staying informed on emerging cybersecurity threats and trends will allow financial services organizations to tailor their defenses to the most prevalent risks they face. Using this information to determine where resources are allocated, how incident response plans are formed, and how much risk an organization is comfortable with, all will contribute to enhanced cyber resilience.