PROFESSIONAL LIABILITY

With so much to lose, Financial Institutions face Increased Scrutiny

Financial services firms find themselves uniquely susceptible to cyber attacks due to the confidential and proprietary data they have in their possession. These firms, including registered investment advisors and brokers, are subject to oversight by a patchwork of regulatory authorities keenly focused on the quality of a firm's cybersecurity and privacy practices.

This article provides an overview of the primary United States regulators governing cybersecurity practices, reviews notable U.S. enforcement activity, outlines best practices and, importantly, frames the role of insurance for addressing cyber preparedness.

National Regulatory Bodies Overseeing Financial Institutions

Many of the national regulatory bodies that traditionally oversee financial institutions are applying greater scrutiny to cybersecurity issues. (See box on page 4 for more details.)

- **Securities and Exchange Commission (SEC)** has consistently included cybersecurity protection in its annual list of examination priorities over the past several years.[1]
- **Financial Industry Regulatory Authority (FINRA),** a self-regulatory organization that oversees market integrity through regulation of broker-dealers, is focusing on broker cybersecurity practices.
- **Consumer Financial Protection Bureau (CFPB)** oversees consumer protection in the financial sector and enforces data security violations, including civil penalties and restitution for affected consumers.
- **Federal Trade Commission (FTC)** has promulgated a safeguards rule that applies to the handling of customer information by financial institutions under the FTC's jurisdiction.[2]
- **Commodity Futures Trading Commission (CFTC)** has established rules to address risks of identity theft.

State Regulation

Although there may be some decline in recent federal enforcement of data privacy laws and regulations, a significant surge in regulation has taken place at the state level. In 2017, 42 states introduced 240 bills and resolutions related to cybersecurity, more than double the amount in 2016.[3]

All 50 states have their own data breach notification laws, which generally require businesses to notify affected individuals and regulatory authorities if a business suffers a data breach in which personally identifiable information is compromised. The New York State Department of Financial Services (NYDFS) is noteworthy for its comprehensive cybersecurity regulatory regime for certain financial services firms operating in New York State (state chartered banks, licensed lenders, private bankers, foreign banks licensed to operate in New York, mortgage companies, insurance companies and services providers -- with limited exemptions for small firms meeting certain size thresholds).

The NYDFS Cybersecurity Regulation works by imposing strict cybersecurity rules on covered organizations, including the installment of a detailed cybersecurity plan, the designation of a Chief Information Security Officer, the enactment of a comprehensive cybersecurity policy and the initiation and maintenance of an ongoing reporting system for cybersecurity events.[4]

Noteworthy Enforcement Activity

The following examples highlight the scrutiny (and resulting impact) that financial institutions are facing from regulatory agencies.

- September 2018: **a large provider of investment management, employee benefits and life and annuity products,** agreed to pay a $1 million fine to settle SEC charges brought under the Identity Theft Red Flag Rule. The charges arose from a six-day period when cybercriminals impersonated the company's independent investment representatives to re-set passwords and provide new ones. The SEC's order found that the intruders used

CONTINUED >

customer information to create new online customer profiles and obtain unauthorized access to account documents. The order found that the company's failure to terminate the intruders' access stemmed from weakness in its cybersecurity procedures.

- February 2018: the CFTC entered into a settlement with a registered **futures commission merchant (FCM)** with violations of a CFTC regulation relating to a data breach. The matter stemmed from a failure to diligently supervise an IT provider's implementation of a network attached storage device, which left unencrypted customers' records on the device unprotected. To settle the case, the FCM agreed to a $100,000 civil monetary penalty and to cease and desist from future violations of the applicable Regulation 166.3.
- June 2016: the SEC issued an order finding that a **large banking institution** was in violation of Rule 30 (a) of Regulation S-P, known as the "Safeguards Rule." The SEC found that the company did not have effective employee authorization modules, which allowed a now former employee to download and transfer confidential customer information to his personal server at home between 2011 and 2014. Some of this information was allegedly hacked and offered for sale online. The company agreed to pay a $1 million penalty to settle charges related to the Regulation S-P violation, without admitting or denying the SEC findings.
- September 2015: the SEC issued an order finding that a **St. Louis-based registered investment advisor** was in violation of Rule 30 (a) of Regulation S-P. The SEC found that the company stored sensitive personally identifiable information (PII) of approximately 100,000 clients and others on its third-party hosted web server from September 2009 to July 2013. The server was attacked in July of 2013 by an unknown hacker, leaving the PII vulnerable to theft. The SEC found that the firm failed entirely to adopt written policies designed to safeguard the PII.

Best Practices

Increased regulatory oversight of financial services firms' cybersecurity framework is driving the industry to build more robust cybersecurity practices. As part of the critical infrastructure of the United States, it is important for financial services firms to improve cybersecurity risk management by applying principles and best practices to improve security and resilience. The Cybersecurity Enhancement Act of 2014 tasked the National Institute of Standards and Technology (NIST) with identifying and developing cybersecurity risk frameworks. This operational framework, while not a "one-size-fits-all" approach to cybersecurity management, sets forth several components that can help frame an organization's approach to cybersecurity management at an operational level:

1. Risk Assessment: Risk assessments should be conducted on a regular basis throughout all areas of the organization to ensure compatibility with the operational framework. A risk assessment should include some form of the following: (1) identifying threats to the organization, (2) determining the risk and impact of such threats on systems, (3) analyzing the vulnerability of the environment,

(4) determining the likelihood of such threats and (5) calculating the environment's risk. Based on the ultimate risk calculation, an organization can best determine its acceptable level of risk.

2. Know and Limit Access: An organization needs to identify the confidential information it seeks to protect. Once identified, protection of that information becomes the priority. NIST recommends that organizations: (1) establish verifiable identities and trusted credentials for all users, (2) control physical access to hardware, (3) manage remote access of users, (4) restrict permissions of approved users and (5) segregate the network to prevent lateral movement with the environment.

   Protection requires limiting the ability to access and to modify information, either through physical access or electronic access. To secure a facility, organizations should use electronic access control systems that rely on user credentials and access card readers to track employee access to restricted business locations and proprietary areas, such as data centers. Access control panels (using many different types of login credentials like passwords, PINS or tokens) should restrict entry to rooms and buildings as well as have alarms and lockdown capabilities to prevent unauthorized access or operations. Multifactor authentication (which requires two or more authentication factors) is often an important part of layered defense to protect access control systems.

3. Monitor End User Activity: Software tools are available to monitor and track end user behavior on devices, networks and company-owned IT resources. Depending on the objective of the organization, user activity monitoring tools help detect and stop insider threats. An organization can monitor an end user's system, data, applications and network actions (such as web browsing activity and accessing unauthorized or sensitive files). Monitoring methods can include: (1) log collection and analysis, (2) network packet inspection, (3) keystroke logging, (4) hard drive monitoring and (5) file/screenshot capturing.

   User activity monitoring is an important line of defense against data breaches and other cybersecurity compromises. Many organizations

CONTINUED >

are not monitoring their users' access to sensitive data, leaving them susceptible to insider threats or outside attackers who have gained access to systems.

In addition to implementing user activity monitoring solutions, organizations should establish and enforce data protection policies, such as appropriate file sharing activity, instructions for handling sensitive data, authorized services and applications and other policies outlining acceptable use. Users should be trained on these policies as well as effective cybersecurity habits through ongoing information security awareness programs.

If a risky action is performed (such as downloading sensitive customer information), the security team should have the ability to score the severity of the activity. This way, the focus can be placed on users who are putting the organization at risk on a large scale.

4. Detect and Respond: *It's no longer if you'll have a breach, it's when…* Thus, an organization's Incident Response Plan (IRP) is critical. This is a set of instructions built to support the organization in detecting, responding and recovering from a network security incident. To create an IRP, an organization should: (1) determine the critical components of their network, (2) identify points of failure in the network, (3) create a workforce continuity plan, (4) list roles and responsibilities for the IRP team members, (5) outline and hierarchy the physical resources and technology the organization needs to have in place, (6) list the network and data recovery processes and (7) outline the internal and external flow of communications.

   The IRP should contain specific instructions on who to contact outside the organization to assist with the response including, but not limited to, insurance carriers, breach consultants (a law firm that specializes in cyber), data forensic vendors, breach response vendors and public relations consultants.

   Finally, an organization should ensure that the IRP is accessible in the event of an incident and is updated regularly to include and validate current contacts, test it regularly and train their staff on the importance of the IRP, why it was created and stress the importance that full adherence to the plan will help to minimize any incident.

For more information on NIST's Cybersecurity Framework, please visit https://www.nist.gov/cyberframework.

"Cyber insurance carriers can help insureds identify the elements of and implement a holistic strategy to fortify their cybersecurity framework."

Role of Insurance

No matter the cybersecurity due diligence, it is impossible for any business to become completely free of cyber risk. Cyber insurance carriers can help insureds identify the elements of and implement a holistic strategy to fortify their cybersecurity framework.

Carriers have experience working with key experts to support insureds in advance of and after an event. Pre-breach risk mitigation services utilizing vendors and tools can support the insured by identifying a baseline and building upon internal objectives for compliance, risk management and cybersecurity initiatives.

In the event of a breach, a financial services firm will deploy their IRP, which should include the method for contacting the firm's cyber insurance carrier. The policy will assist the firm in responding to a breach by quickly organizing the necessary response team including breach consultants, data forensic and breach response, and public relations vendors. Further, a cyber policy will defend and possibly indemnify a financial services firm for a claim arising from the breach. These claims take the form of regulatory investigations by state and federal agencies as well as lawsuits filed by aggrieved parties. The damages that flow from such investigations, including fines and penalties, as well as damages resulting from a lawsuit may be indemnifiable under a cybersecurity policy.

Finally, most cyber insurance policies will offer coverage for ransomware loss, business income loss and social engineering fraud loss. In all, a cybersecurity insurance policy can be an effective partner to assist financial service firms build their cybersecurity framework.

Conclusion

While certain aspects of federal regulation may ebb and flow with political tides, financial services firms are also subject to a broadening degree of state regulation. Moreover, firms doing business overseas are subject to international regulation. Considering the intense level of scrutiny, the complexity of organizations sharing oversight and the ongoing risk of cyber attacks, financial institutions need to remain constantly vigilant in their cybersecurity efforts. A robust insurance program can provide coverage certainty, help bolster pre-breach risk management efforts and should a breach occur, provide guidance in navigating the privacy laws, regulatory response and notification requirements integral to incident evaluation and response.

CONTINUED >

WHO IS REGULATING THE INDUSTRY?

Financial Institutions are seeing increased scrutiny and enforcement actions around cybersecurity laws and regulation from:

Securities and Exchange Commission (SEC)

Through its Investment Management Division, the SEC is the primary federal regulator overseeing registered investment advisors, mutual fund companies and variable insurance products. The SEC investigates and prosecutes actions, including those for cybersecurity offenses, through its Enforcement Division.

FINRA

Broker cybersecurity practices are a key focus for FINRA which reviews a broker-dealer firm's ability to protect the confidentiality, integrity and availability of sensitive customer information, including reviewing compliance with SEC regulations, such as Regulation S-P, Regulation S-ID and the Securities Exchange Act of 1934 requirement to preserve electronically stored records.

Consumer Financial Protection Bureau (CFPB)

While the SEC and FINRA regulate cybersecurity for investment professionals, in large part, consumer protection for other areas of the financial services sector is regulated federally by the CFPB. The CFPB's jurisdiction includes but is not limited to banks, credit unions, mortgage lenders, credit card networks, payday lenders, debt collectors, student loan servicers and auto finance companies. Through authority granted under Dodd-Frank, the CFPB can take enforcement action against such companies for data security violations, including civil penalties and restitution for affected consumers.

Federal Trade Commission (FTC)

The FTC is a federal agency charged principally with the promotion of consumer protection and the prevention of anticompetitive business practices. With respect to the regulation of cybersecurity and privacy practices for financial institutions, the FTC seemingly has overlapping authority with the CFPB to regulate those financial institutions not covered by federal banking agencies, the SEC, the CFTC or state insurance authorities. Their authority is derived from the Gramm-Leach-Bliley Act, a 1999 federal law that broadly reformed the banking industry.

Commodity Futures Trading Commission (CFTC)

The CFTC is an agency of the U.S. government that regulates futures and options markets. While the CFTC's scope in protecting individual investors is more limited than the SEC's, the agency has jointly with the SEC established rules to address risks of identity theft, commonly known as the "red flags" rules. The Red Flag rules call for investment firms to maintain an up-to-date program for preventing identity theft, which should provide "red flags" or other warning signs when hackers might be trying to steal customer information. The rule also requires a firm's board of directors or senior leadership to administer the program.

References

[1] The U.S. Securities and Exchange Commission 2019 National Exam Program Examination Priorities can be found at https://www.sec.gov/files/OCIE%202019%20Priorities.pdf

[2] Tannenbaum Helpern Syracuse & Hirschtritt, LLP, Overview of Data Privacy and Cybersecurity Regulatory Landscape for Investment Advisors and Other Financial Services Companies, 2017, citing http://www.thsh.com/documents/May-2017/Overview-Data-Privacy-Cybersecurity-Regulatory.pdf

[3] Edgile, US State Cybersecurity Regulation More than Doubled in 2017, While Federal Regulation Waned, January 29, 2018, https://edgile.com/2018/01/29/us-state-cybersecurity-regulation-more-than-doubled-in-2017-while-federal-regulation-waned/

[4] The DFS regulation, 23 NYCRR 500 can be found at https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500txt.pdf

AUTHORS

David Rock, *Vice President*
North American Claims Department, E&O

Marc Berner, *Vice President*
U.S. Financial Institutions Product Lead

QUESTIONS? Contact your local Allied World Underwriter.

alliedworldinsurance.com