Winget | Spadafora | Schwartzberg | LLP

NY | NJ | CT | FL | CA | TX | IL | CO

www.WSSLLP.com

CLIENT ALERT:

Tangible Measures to Prepare for Intensified Regulatory Oversight of Cybersecurity in 2016

August 4, 2016

Author: Hillard M. Sterling, Esq.

I. SUMMARY

Cybersecurity has taken center stage as a top priority for financial-service firms of all sizes. Hackers increasingly are targeting these firms as proverbial low-hanging fruit of sensitive client data that can be sold profitably on the black market. While firms are getting better at protecting their data, substantial vulnerabilities remain.

As a result, FINRA has made cybersecurity a top exam priority for 2016. Firms need to ensure that they are taking compliant preventive measures in order to address the risks of breaches or incidents. Simply stated, a strong information-security program is not optional.

Set forth below is a description of preventive measures that are mandatory components of every such program. However, it is necessary but insufficient to simply have these measures in place – they also need to be crafted to the unique needs of each firm, and communicated in a meaningful way to all employees involved in the use, transmission, retention, and storage of data. Moreover, outside counsel should be involved to help firms develop these programs under the protective umbrella of the attorney-client privilege, to the extent practicable.

II. INTENSIFIED REGULATORY OVERSIGHT

On January 5, 2016, FINRA published its annual Regulatory and Examination Priorities Letter, which identified central areas of focus for the coming year. Significantly, the Letter discussed cybersecurity as one of the critical "broad issues" in connection with supervision, risk management, and controls. As stated in the Letter, "FINRA remains focused on firms' cybersecurity preparedness given the persistence of threats and our observations on the continued need for firms to improve their cybersecurity defenses."

FINRA specifically noted the continued vulnerabilities and gaps in firms' cybersecurity preparedness. As stated in the Letter: "While many firms have improved their cybersecurity defenses, others have not – or their enhancements have been inadequate."

There is abundant evidence supporting FINRA's critical view of firms' cybersecurity readiness. For example, SIFMA's recent "Quantum Dawn 3" cybersecurity testing found substantial areas in which cybersecurity preparations were lacking. After testing the cyber readiness of 650 participants from more than 80 financial institutions and government agencies, SIFMA's after-action report noted multiple "opportunities to improve response protocols and strengthen coordination among the industry participants." Several of these opportunities were in the area of individual firm preparedness, including the needs to enhance executive leadership, develop incident-response plans and teams, and enhance firms' "internal playbooks" to prepare for "various types of attacks or threat vectors."

Firms, therefore, need to be prepared for expanded and intensified regulatory oversight of their cyber preparedness. But that need is easier to state than address. What tangible measures should firms be developing and implementing to enhance their cybersecurity? Several such measures are set forth below.

III. TANGIBLE MEASURES TO ENHANCE CYBERSECURITY READINESS

There are certain tangible measures that all firms must take to enhance their cybersecurity readiness. FINRA specifically referenced many of these measures in its Letter, and they are discussed in greater detail in FINRA's 2015 Report on Cybersecurity Practices, which is required reading and a ready guide of cybersecurity best practices in the financial-services industry.

a. Preparing or Revising Policies

Strong data-security policies are the backbone of any breach-readiness plan. These policies should cover the multitude of ways that data is received, accessed, stored, transmitted, and used across the entire enterprise. Policies should cover internal and remote access, passwords, encryption, email usage and storage, mobile devices in and outside the workplace, network security, physical security, legal compliance (and its many facets), monitoring and logging, and many other areas depending on the firm and the data it touches. Each firm is unique in all of these respects, and the policies should be crafted and fine-tuned accordingly. Given the complexities, generic policies represent, at best, a start.

b. Preparing or Revising Incident-Response Plans

The same principles hold true for incident-response plans, which should be tailored to each firm's particular structure, data, and legal duties. The plans are roadmaps for acting quickly and effectively in the event of a potential breach and incident. As such, these plans should carefully delineate who gets involved and when, what steps must be taken to investigate and address the potential breach or incident (particularly in the critical early stages), and how information is to be communicated internally and externally. One central commonality is that all of these plans should involve outside counsel, as "breach coaches," to coordinate and quarterback the response and maximize the protection of information where appropriate under the attorney-client privilege and work-product doctrine, as discussed more fully below.

c. Undertaking Risk and Compliance Assessments

Breaches or incidents often are the impetus for firms to focus closely on their legal exposure. By that time, however, the objective is to minimize or mitigate damages. It makes much more sense to analyze risks and assess legal compliance before the damage is done through a data breach or incident. An effective risk assessment requires a comprehensive analysis of potential exposures associated with customer or firm information, including detailed analyses of asset inventories and vulnerabilities. And understanding the governing legal mandates, in turn, dictates the necessary specifics of other preventive measures, such as internal policies.

d. Developing or Improving Employee Training

A comprehensive risk-prevention program is only as strong as its weakest link, and deficient employee training may destroy an otherwise strong program. Employees need to be fully aware of data-security policies, procedures, and protocols. Awareness, though, is only half the battle. Firms need to ensure that employees truly understand, and actually follow, policies aimed at protecting sensitive data. One recent trend is to test employees by distributing cleverly disguised emails that mimic phishing attacks, so that careless employees are identified and trained before they fall for pernicious hacking attempts in the real world.

e. Developing or Improving Table-Top Exercises

As with policies that are not communicated and followed, incident-response plans have little or no efficacy if they are not used and tested before a real breach or incident. Firms should deploy realistic table-top exercises to rehearse the appropriate response to various foreseeable breaches or incidents. It is far preferable to identify and plugs gaps in the plan during a hypothetical exercise than to fall through them when it really counts.

f. Other Steps to Foster Strong Cybersecurity Governance

The underlying theme of all of these preventive measures is to foster a true security culture across the entire enterprise. There are many additional ways to do so. Corporate executives should be leading the charge, and they should be active and visible sponsors of preventive measures across the organization. Regular reminders of governing policies are helpful, particularly if done in creative ways. Consider measures that make corporate security interesting or even fun, such as contests and awards for the safest divisions or departments. Meet and discuss these issues, and encourage active communication.

g. Vendor Management

Firms are only as strong as the vendors on which they rely for a range of services. True cybersecurity requires that firms undertake due diligence on the preparedness of their vendors who hold sensitive client data.

h. Cyber Intelligence and Information Sharing

Firms are better protected if they gather and analyze threat intelligence. The federal government's Financial Services Information Sharing and Analysis center ("FS-ISAC") provides an excellent forum in which to share and benefit from such intelligence and data.

i. Cyber Insurance

Cybersecurity insurance is becoming an important (and increasingly affordable) measure to reduce first-party and third-party exposure. Firms should not rely on their general insurance policies to protect them against breach-related damages and costs, which can be substantial if not debilitating, including potentially monstrous costs associated with complying with multiple notification statutes. Cyber policies, however, vary widely, with potential traps in coverage and sub-limits. Firms should enlist the help of experienced brokers to understand the specifics of policies before buying.

j. Technical Controls

Last but not least is the critical area of technical controls. Firms need to employ the full panoply of technological protections, including firewalls, malware and virus detection, encryption, access and use restrictions, penetration testing, and other software and protocols that are critical components of any technological defense against data loss.

IV. UTILIZING THE ATTORNEY-CLIENT PRIVILEGE AND WORK- PRODUCT DOCTRINE

Promptly upon discovering a potential data breach or incident, a critical first step is to initiate an investigation. The central objectives are to determine the nature and scope of the intrusion or loss, and to take tangible measures to stop or at least mitigate the resulting harm. The incident-response plan is the roadmap for meeting these objectives. Once these objectives are satisfied, additional investigatory measures will be necessary in order to develop and implement strengthened data protections, communicate with regulators and other interested constituencies, and prepare for potential litigation in administrative tribunals and courts.

Firms need to protect their communications as much as possible during these investigations. It is in everyone's interests to communicate openly and often critically, and the incentives to do so are magnified exponentially if those communications are protected from disclosure to regulators and the outside world.

Outside counsel should be retained as "breach coaches" in order to protect associated communications, to the extent desirable and legally possible, under the attorney-client privilege and work-product doctrine. Courts generally recognize the privileged and protected nature of these communications when requested and/or directed by outside counsel for purposes of assessing legal risks and counseling on legal issues. By contrast, courts exhibit increased skepticism when adjudicating privilege assertions over communications that did not involve counsel, or that involved only in-house counsel (whose communications are more easily characterized as undertaken for business purposes rather than legal advice).

These principles also hold true for pre-breach risk-reduction programs. Outside counsel should be involved as "pre-breach coaches" to develop and implement measures aimed at reducing risks and damages from prospective breaches or incidents. Communications should occur at the direction or request of outside counsel, for purposes of assisting counsel to assess and address legal risks. Outside counsel should be central to the chain of written communications – hard-copy and electronic (including of course emails) – to ensure that those communications are appropriately labeled and managed to preempt prospective arguments that potentially applicable privileges or protections were waived.

V. BOTTOM LINE

Firms cannot totally eliminate the risk of a data breach or incident, whether caused by a malicious hack or simply human error. However, firms can – and, given intensified regulatory oversight, must –

identify and address their cybersecurity risks through the implementation of tangible measures that have become an invariable part of the industry landscape.

For more information, or if you would like to discuss this or other issues that affect your business, please contact Hillard Sterling at Sterling.H@WSSLLP.com