Cybersecurity: What every Compliance Officer Should Know

By Giselle Casella, Senior Principal Consultant , ACA Compliance Group

I. Regulatory Background

The 1990s saw the evolution of the Internet and related technologies which would dramatically change society and the way people do business. However, it also opened up a whole new world for criminal activity, i.e. cybercrime. During that time, the U.S. Securities and Exchange Commission (“SEC”) frequently used anti-fraud statutes to prosecute financial services industry cases involving cybercrime. Then, with the adoption of Regulation S-P in June 2000, the SEC began to establish regulatory statutes indirectly addressing cybersecurity. 1 Subsequently, the SEC adopted Regulation S-AM in August 2009 2 and Regulation S-ID 3 in April 2013, which further protect individuals’ non-public personal information (“NPI”) and require consideration of cybersecurity risks. The SEC also issued guidance in October 2011 regarding disclosure obligations related to cybersecurity risks and cyber incidents (See Policies and Procedures).

Concurrent with the SEC’s cybersecurity initiatives, FINRA and various states began taking notice of the increasing risk of cybercrime in a world growing increasingly dependent on technology. In July 2005, FINRA (then NASD) issued guidance to member firms reminding them of their obligations under Regulation S-P, specifically addressing risks associated with the use of technologies related to Wi-Fi and remote access. 4 Meanwhile, most states began to adopt some form of data breach notification laws that required either individual and/or state notification (California) in the event that a data breach compromised NPI. Certain states, such as Massachusetts and Nevada, also established standards for the protection of residents’ NPI.

II. Recent Developments

No doubt prompted by the recent wave of cyber-attacks against a handful of large retailers and a large hedge fund, cybersecurity is now officially an SEC exam priority. In January 2014, Jane Jarcho, the Associate Director of the SEC’s Investment Adviser Exam Program, announced that the SEC will be conducting its review of cybersecurity policies as part of its routine examinations of registrants. Specifically, the SEC will be looking to see what policies are in place to prevent, detect and respond to cyber-attacks, as well as policies on IT training, vendor access, vendor due diligence, etc. In March, the SEC held its first ever roundtable on cybersecurity. Panelists recommended, among other things, that firms should focus on high risk areas and systemic risks, adopt policies and procedures that include senior management accountability and firm-wide preparation and coordination, prepare an incident response plan, and share information on cybersecurity with other firms within the industry. It should be noted that there appeared to be consensus among the panelists that cybersecurity is not just one person or department’s responsibility and that employee training and “tone at the top” are critical. Finally, in April, the SEC issued a Risk Alert on cybersecurity preparedness and announced that it would be conducting sweep exams on over 50 registered advisers and broker-dealers. 5 The SEC even released a sample of its document request list signaling the areas in which the SEC would focus on and is most concerned about in regard to cybersecurity. The sample document request list covers information related to identification of risks/cybersecurity governance, protection of firm networks and information, risks associated with remote customer access and transfer requests, risks associated with vendors and other third parties, and detection of unauthorized activity.

Aside from the SEC, FINRA announced on its website in January 2014 that it would be conducting cybersecurity sweeps to better understand how firms are handling cybersecurity threats. Certain states, such as Massachusetts and Illinois, have also announced that they will be polling advisers registered in their states on cybersecurity policies and procedures. Both state and federal regulators are certain to be looking at any best practice guidance available concerning information technology and cybersecurity.

Firms should consider the following resources with respect to their cybersecurity programs:

ABOUT THE AUTHOR

Giselle Casella is a Senior Principal Consultant with ACA Compliance Group. Prior to joining ACA in 2010, Giselle was previously Vice President in the Core Advisory Compliance area at Deutsche Asset Management and a Senior Compliance Officer at Allianz Global Investors. Giselle began her career in compliance in 1999 as an investment adviser examiner for the US Securities and Exchange Commission.

1 Rule 30 of Regulation S-P (referred to as the “Safeguard Rule”) requires registered broker-dealers, investment advisers and investment companies to establish written policies and procedures that address administrative, technical and physical safeguards for the protection of customer records and information, and that are reasonably designed to (a) insure the security and confidentiality of customer records and information; (b) protect against any anticipated threats or hazards to the security or integrity of customer records and information; and (c) protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.

2 Regulation S-AM allows a consumer, in certain limited situations, to block affiliates of a person subject to Regulation S-AM that the consumer does business with from soliciting the consumer based on certain “eligibility information” (i.e., certain financial information, such as information regarding the consumer’s transactions or experiences with the person) received from the regulated person.

3 Regulation S-ID requires, among other things, that financial institutions adopt written identity theft prevention policies and procedures that (a) implement reasonable policies and procedures to detect, prevent, and mitigate the risk of identity theft; (b) are updated periodically to reflect different types of changes in identity theft-related risks; (c) senior management reviews and approves; (d) provide training on relevant risks and program implementation; and (e) allow for oversight of service providers.


• National Institute of Technology Framework for Improving Critical Infrastructure Cybersecurity ("NIST Framework").

The NIST Framework is a voluntary, risk-based set of industry standards and best practices to help organizations manage cybersecurity. The NIST Framework addresses core cybersecurity activities, implementation tiers based on risk, and a profile that measures “current” versus “target” for specific cybersecurity activities.

• International Organization for Standardization ("ISO") - Standards for Information Security Management. ISO specifies requirements for establishing, implementing, maintaining, and continually improving an information security management system within the context of the organization.

• SANS Institute's ("SANS") 20 Critical Security Controls. SANS focuses on prioritizing security functions that are effective against the latest advanced targeted threats and standardization and automation to gain operational efficiencies while also improving effectiveness.


III. Enforcement Action Implications

Firms should consider looking at recent enforcement cases to identify potential areas of risk and get an idea of what the SEC and other regulators may look for. A few good examples include: GunAllen Matters, NEXT Financial Group Matter, Commonwealth Equity Matter and Syndey Mondschein Matter. In each case, violations of Regulation S-P were cited. Firms should pay particular attention to the following deficiencies noted in these and other recent enforcement cases:

- Inadequate policies and procedures;
- Failure to enforce cybersecurity policies and procedures;
- Failure to conduct adequate periodic cybersecurity assessments;
- Failure to respond to cybersecurity deficiencies;
- Failing to protect firm networks and customer information;
- Failing to encrypt NPI;
- Inadequate anti-virus software and/or firewall;
- Inadequate user access restrictions;
- Inadequate vendor oversight; and
- Inadequate response to cybersecurity breaches.

Based on the level of enforcement activity in recent years, as well as the regulatory exam sweeps and comments made during the SEC roundtable, it seems likely that there will be an increase in cybersecurity regulation and/or guidance along with additional enforcement actions. All firms, regardless of size, should be prepared.

IV. What Should Your Firm Do?

Risk Assessment

In order to develop and/or maintain an effective cybersecurity program that is tailored to an individual organization, it is critical to perform periodic risk assessments. On at least an annual basis, Compliance should work with IT to identify moderate and high risk vulnerabilities. Any such vulnerabilities should be eliminated where possible or mitigated through policies and procedures. The risk assessment process should consider, among other things:

- The type of information the firm maintains, i.e. consumer data, trade secrets, confidential and/or proprietary data, etc;
- Technology currently in use such as hardware, software, mobile devices, email server, anti-viral protection, firewalls, web-based applications, remote access tools, security/authentication protocols, etc;
- Systems in place for monitoring and detecting breaches;
- Accessibility to devices, data, bank accounts, wire transfers, etc;
- Relationship with third parties, such as customers, business partners, vendors, affiliates, etc;
- Cybersecurity incidents experienced by the firm or others in the past;
- Individuals or entities that may pose a threat such as former, disgruntled or careless employees, organized crime, hackers and vendors;
- Use of personal and/or unauthorized devices by employees;
- The potential impact on the firm such as financial loss, disruption of business, reputational damage, etc;
- Resources in place for disaster recovery and business continuity; and
- Employee awareness of their roles and responsibilities related to cybersecurity.

b. Policies and Procedures

Once the risk assessment has been developed and/or reviewed, written policies and procedures must be implemented or updated accordingly. It should be noted that when it comes to cybersecurity, there is no one-size-fits-all approach. Firms should develop and maintain policies and procedures based on their size, risk assessment, cost considerations, etc. However, any written policies and procedures must broadly cover the following:

- **Roles and Responsibilities**: A firm's cybersecurity program should clearly identify the employees charged with overseeing the program, as well as their roles and responsibilities. Depending on the size of the organization, at least one senior individual who is knowledgeable on information security should be tasked with overseeing the cybersecurity program. Larger firms may want to consider dividing the responsibility among multiple employees. In either case, the regulators will expect senior management involvement and participation in the cybersecurity program. Any vendors employed to assist with implementing the cybersecurity program should also be noted.

- **Accessibility**: A firm's cybersecurity program should consider who has access to the firm's data and devices and how they are able to access information. As a best practice, employees and third parties should only be given access to the data they absolutely need. And there should be a documented approval process in place. With respect to terminated employees, all access to firm data and devices should be revoked as of their last day of employment. Firms may also want to consider limiting employees’ physical access to company issued desktops, laptops, USB/Flash drives and mobile devices as needed. Firms may also want to carefully monitor employees’ use of any such devices, as well as their ability to gain remote access to company data or devices.

- **Security Protection**: Firms should have adequate security protocols for protecting company data and devices as needed. This includes, where applicable, password protected devices and systems, encryption of devices and electronic communication containing NPI, firewalls, anti-viral and anti-malware software, software for filtering websites and/or blocking website downloads, intrusion detection systems, security involving cloud computing, website security, etc.

- **International Considerations**: A firm's cybersecurity program should take into account any international requirements that may apply. To the extent business is conducted overseas, Compliance and IT personnel should be aware of any local jurisdictional requirements. For example, the European Union (“EU”) has established data protection and reporting regulations for companies established within the EU. The EU has also proposed additional regulations regarding data breaches which would impact companies outside the EU.

- **Monitoring, Identifying and Responding to Breaches**: Firms should have adequate controls in place for continuous monitoring of employee and third party access to devices and systems, as well as identifying potential breaches. This includes not only surveillance on use of devices, systems, networks, programs, etc., but also monitoring of employees’ email, instant messages and use of social media. Ideally, firms should be able to quickly detect and respond to potential breaches, thereby mitigating the risk of harm. Further internal or external investigation may be warranted when there's a potential breach, depending on the circumstances. A firm may also be required to report the incident to customers and/or regulators. As discussed earlier in this article, the firm may consider whether it may need to notify the SEC and other regulators. Finally, firms should consider their whistleblower policies within the context of internal reporting of cybersecurity breaches.

- **Vendor Oversight**: Many financial service firms outsource key functions to third party vendors. These vendors may be subject to cyber-attacks that can provide access to the firm that is linked to the vendor. As a result, vendors are increasingly employing standardized contracts that limit their liability. Firms should consider negotiating for stipulations that require vendors to provide prompt reporting and remediation of data breaches, keep apprised of legal and regulatory changes, use additional layers of information security, engage in cybersecurity testing, and use the most up to date security protocols. Firms should also include cybersecurity in the vendor due diligence process.

- **Insurance**: Most standard insurance policies used in the financial services industry, such as director and officer (“D&O”) liability, do not cover threats posed by cybercrime. Losses associated with cybercrime can be high and may include lost revenue, investigate costs, regulatory reporting expenses, damage to data and systems, etc. Therefore, firms may want to consider obtaining a cyber-liability insurance policy if the potential loss may be significant.

- **Identity Theft**: In many cases, cybercrime can lead to identity theft if NPI is compromised. Therefore, cybersecurity programs should contemplate identity theft and Regulation S-ID. Regulators will expect firms to have information security protocols in place to protect NPI and promptly identify and respond to attacks.

- **Disaster Recovery**: Cybercrime may have disaster recovery/business continuity implications to the extent data or systems are damaged and/or rendered inoperable. A firm's written disaster recovery plan should consider the potential impact of cybercrime particularly with respect to data backup, recovery of...
mission critical systems, communication with third parties and assuring customer access to accounts and funds. FINRA’s Business Continuity Plans and Emergency Contact Information requirements are a good resource for any financial service firm to consider.15

- **Testing:** Firms should consider implementing procedures for regularly testing the effectiveness of their cybersecurity programs. This includes: testing incident response capabilities, vulnerability testing, penetration testing, data and system backup testing, testing to verify that systems, hardware, software and networks are functioning properly, etc.

- **Training:** Employee training is required under both Regulation S-P and Regulation S-ID. Based on recent comments and sweep exam requests, the regulators expect firm employees to have received training and be knowledgeable on information security.

- **Documentation:** All documentation related to cybersecurity programs including the risk assessment, policies and procedures, testing and training should be maintained and easily accessible for regulators.

V. Conclusion

The Internet has brought about a new era for both business and crime. Unfortunately, current regulations have not quite kept pace with the evolution of technology and cybercrime. Amidst the wave of recent cyber-attacks, regulators such as the SEC have made cybersecurity a priority. Based on recent comments made by the SEC and FINRA, as well as the focus of the cybersecurity sweeps, it is clear that the regulators expect firms to implement risk based, cybersecurity programs. Firms should take into consideration recent regulatory enforcement actions, as well as external resources of information such as NIST and ISO, when developing their cybersecurity programs. Ultimately, cybersecurity programs should be tailored to the specific needs of the firm. However, regardless of size, no firm will be exempt from having a cybersecurity program.

---