December 16, 2014

Weil

Alert
Cyber Security, Cyber Governance, and Cyber Insurance

New York Department of Financial Services Issues Cyber Security Guidance Letter

By Paul A. Ferrillo

Though other more notorious cyber security breaches have recently flooded the news, there can be no question that some of the more startling breaches have involved major financial institutions.[1] Indeed, the cyber threats to the banking industry are real and upon us, and are cropping up in ways we potentially did not think of previously:

> Vulnerabilities in mobile banking pose another new and highly sophisticated danger, as mobile banking vulnerabilities may exist on mobile devices that are not patched, and malware can be developed to specifically target the use of mobile devices. One example of this type of vulnerability is the Zeus-in-the-Middle malware, a mobile version of the GameOver Zeus malware, which itself was one of the most sophisticated types of malware the FBI ever attempted to disrupt. GameOver Zeus was designed to steal banking credentials that criminals could then use to initiate or redirect wire transfers to overseas bank accounts. All told, the malware infected over 1 million computers worldwide and caused over $100 million in estimated losses.[2]

In continued recognition of persistent threats upon the banking industry, on December 10, 2014, Benjamin J. Lawsky, Superintendent of the New York Department of Financial Services (NYDFS), issued a guidance letter to NYDFS-regulated banks outlining specific cyber security-related factors that will be reviewed as part of a bank's annual review. In this release, Superintendent Lawsky stated:

> It is our hope that integrating a targeted cyber security assessment directly into our examination process will help encourage a laser-like focus on this issue by both banks and regulators. Cyber hacking is a potentially existential threat to our financial markets and can wreak serious havoc on the financial lives of consumers. It is imperative that we move quickly to work together to shore up our lines of defense against these serious risks.[3]

With the non-stop breach activity we have seen over the last few weeks, both state and federal regulators are showing their concern, and urging regulated entities to improve their cyber security postures immediately before the "bad guys" can wreak as much havoc on the U.S. financial markets as they have on other U.S. companies, particularly those in the retail sector.[4]

This alert will discuss the recently announced cyber security guidance issued by NYDFS as well as other recent statements issued by various federal regulators concerning their own annual examinations or desk audits.

NYDFS Guidance

Superintendent Lawsky's guidance letter is very specific, and encourages banks to provide comprehensive answers to very important cyber governance issues, including:

- Management of cyber security issues, including the interaction between information security and core business functions, written information security policies and procedures, and the periodic reevaluation of such policies and procedures in light of changing risks;
- Resources devoted to information security and overall risk management;
- The risks posed by shared infrastructure;
- Protections against intrusion, including multi-factor or adaptive authentication and server and database configurations;
- Information security testing and monitoring, including penetration testing;
- Incident detection and response processes, including monitoring;
- Training of information security professionals as well as all other personnel;
- Management of third-party service providers;
- Integration of information security into business continuity and disaster recovery policies and procedures; and
- Cyber security insurance coverage and other third-party protections.[5]

This guidance may be seen as a welcome blessing for the many New York-based financial institutions or financial services organizations (or pieces of them) that are also regulated by the SEC's Office of Compliance,[6] FINRA,[7] or the FDIC, OCC, and/or FFEIC[8] – each of which has announced either guidance or street sweep letters for annual audits/reviews of its respective regulated entities. Thankfully, much of the guidance issued by these organizations to their respective regulated entities is similar to that issued by NYDFS. Conflicting guidance would have only confused the question of "best cyber security practices" even further, and could have caused regulated entities double or triple the compliance work in order to keep up with each involved agency. In the inherently perplexing area of cyber security, we need more good answers, rather than more questions to be answered by regulatory entities.

Good Cyber Governance and Cyber Compliance

The NYDFS guidance is also well-placed in that it focuses not just on "data protection" measures, which are but a piece of the puzzle, but also on "incident detection and response… and on the integration of information security into business continuity and disaster recovery policies and procedures," as well as cyber security insurance coverage. These three pieces go together like a hand in a glove.

As recent major data breaches have taught us, it is more than likely that despite state of the art firewall and anti-virus protection, every day New York-regulated entities are subjected to thousands of cyber security "events" of various intensity and complexity. Those thousands of events require sophisticated incident detection tools to determine whether they are actually "incidents" in disguise, which would then require immediate remediation and/or counter-measures. Unfortunately, despite the best efforts of companies, it is estimated by some that at least 90% of all intrusion detection systems might not be able to catch the most sophisticated hack.[9] The name of today's game is not being "cyber perfect" (because we can't be) but remaining "cyber resilient,"[10] i.e., being able to take a cyber-punch and get back off the canvas through a battle-tested incident response and data recovery plan aimed at getting the organization back in business as soon as possible. Helping maintain resiliency is cyber insurance, which can potentially defray the huge (and potentially crippling) costs of a cyber-breach forensic investigation and recovery efforts.[11]

As noted above, NYDFS-regulated banks, financial institutions, and some insurance companies may not be subject to just NYDFS regulation, but to other federal regulations as well.[12] For these reasons, New York-regulated organizations need to become more culturally "cyber compliant"-based organizations. Essentially, instead of "checking the box" once every audit cycle, cyber security procedures, training and policies (along with incident detection hardware and software) need to be revisited by internal IT departments and outside IT experts more than just once a year. Unfortunately, despite our best efforts, what is state-of-the-art today may not be state-of-the-art tomorrow. Cyber security processes, procedures, and internal discussions need to be documented when necessary to evidence improvements when made. And solid information concerning cyber security events, incidents, and incident responses needs to come to the attention of the board of directors in a timely fashion so that boards can exercise their fiduciary duties regarding enterprise risk management. Good cyber security is a living, breathing concept and needs to be treated as such.

1. See "J.P. Morgan Says About 76 Million Households Affected By Cyber Breach", available at http://www.wsj.com/articles/j-p-morgan-says-about-76-million-households-affected-by-cyber-breach-1412283372.
2. See testimony of Joseph Demarest, Assistant Director of the FBI's Cyber Division, available at http://insurancenewsnet.com/oarticle/2014/12/11/senate-banking-housing-and-urban-affairs-committee-hearing-a-577571.html#.VI4J74E8KrU.
3. See Press Release of NYDFS Superintendent Benjamin Lawsky, available at http://www.dfs.ny.gov/about/press2014/pr1412101.htm.
4. See "Happy Holidays becomes 'Happy Data Breaches'", available at http://thehill.com/blogs/congress-blog/technology/226972-happy-holidays-becomes-happy-data-breaches.
5. *Id.*
6. See OCIE Cyber Security Initiative (which applies to registered broker-dealers and registered investment advisers), available at http://www.sec.gov/ocie/announcement/Cybersecurity+Risk+Alert++%2526+Appendix+-+4.15.14.pdf.
7. See FINRA Targeted Cyber Security Exam Letters, found at http://www.finra.org/Industry/Regulation/Guidance/TargetedExaminationLetters/P443219.
8. See testimony of Office of the Comptroller of the Currency's Senior Critical Infrastructure Officer Valerie Abend, December 10, 2014, available at http://www.occ.gov/news-issuances/congressional-testimony/2014/pub-test-2014-165-written.pdf.
9. See "FBI: Sony hack would work on '90 percent' of public, private firms", available at http://thehill.com/policy/cybersecurity/226657-fbi-sony-hack-would-work-on-99-percent-of-companies. We note that the forensic investigation of the Sony hack is continuing, so the final word is not out yet on the sophistication of the attack.
10. See "Five questions (and answers) about North Korea and the Sony hack", available at http://www.washingtonpost.com/blogs/monkey-cage/wp/2014/12/14/five-questions-and-answers-about-north-korea-and-the-sony-hack/ (noting that "There is really no such thing as a secure system, but there are things one can do to boost protection. Redundancy, resilience and backup networks, as well as decentralization, are all tactics that need to be used by important government branches and corporations.")
11. See "Will Banks Be Required to Have Cyber-Insurance?" available at http://www.bankinfosecurity.com/will-banks-be-required-to-have-cyber-insurance-a-7673 (noting "…what cyber-risk insurance can do is provide some measure of financial support in case of a data breach or cyber-incident"); see generally "Cyber Security, Cyber Governance, and Cyber Insurance," available at http://blogs.law.harvard.edu/corpgov/2014/11/13/cyber-security-cyber-governance-and-cyber-insurance/.
12. See e.g., SEC Regulation S-ID, which generally requires "SEC or CFTC registrants (e.g., investment advisers, investment companies, broker-dealers, commodity pool advisors, futures commission merchants, retail foreign exchange dealers, commodity trading advisers, introducing brokers, swap dealers, and major swap participants) to establish and maintain programs that detect, prevent, and mitigate identity theft, if they maintain certain types of accounts for clients." See PWC Memo "Identity Theft Regulation: Are you under the SEC/CFTC microscope?" available at http://www.pwc.com/us/en/financial-services/regulatory-services/publications/identity-theft-regulation.jhtml.

If you have questions concerning the contents of this issue, please speak to your regular contact at Weil, or to:

Paul A. Ferrillo (NY) Bio Page paul.ferrillo@weil.com +1 212 310 8372