Why Cybersecurity Matters for Investment Advisors

By Cary Kvitka, Esq., and Max Schatzow, Esq.

In early 2013, a number of large U.S. banking websites were disabled by hackers over and over and over again. The hacks, known as Operation Ababil, were perpetrated by the Qassam Cyber Fighters. Countless other hacking events, data breaches, and cybersecurity threats also took place in the late parts of 2012 and early part of 2013.

Though these hacks targeted the banking industry, they have generated vigilance among regulators with regard to the entire financial services sector, investment advisors included. Specifically, recent actions by the Securities and Exchange Commission (SEC) have made it abundantly clear that investment advisors need to take explicit steps to comply with the commission’s heightened expectations regarding cybersecurity.

Background—The Framework

The events of 2012 and 2013 apparently led President Barack Obama to take executive action to deter hackers and prevent cyber threats to the nation and its critical infrastructure. On February 12, 2013, Obama signed Executive Order 13636, “Improving Critical Infrastructure Cybersecurity.” It was an attempt to improve the nation’s infrastructure to prevent and detect cyber risk by keying in on critical participants in the U.S. economy and requesting that they adopt comprehensive cybersecurity practices. Critically, it appointed the National Institute for Standards and Technology (NIST) to work with the public and private sector to develop standards and practices and a voluntary cybersecurity framework.

In response, NIST has released “Framework for Improving Critical Infrastructure Cybersecurity Version 1.0” (the Framework). NIST has specifically acknowledged that the Framework is not a one-size-fits-all approach to managing cybersecurity risk for businesses and critical infrastructure. Importantly, NIST has recognized that business interests and the government will continue to face unique risks based on sector or market and therefore will be subject to different threats and vulnerabilities. NIST further acknowledged that participants will be able to implement policies under the Framework in different ways. The Framework allows organizations to determine activities that are important to critical service delivery for their specific industries or businesses and allows them to prioritize investments in cybersecurity defense to maximize the impact of each dollar spent.

The Framework is aimed at reducing and better-managing cybersecurity risks by identifying risks of the participant and the participant’s industry, allocating resources to detect and prevent those risks, and then taking measures to regularly test and prevent those risks from occurring.

The Framework consists of three distinct sections: the Core; Implementation Tiers (the Tiers); and the Profile.

The Core

The first part of the Framework, the Core, is a set of activities specific to the business or organization that provides detailed guidance for developing organizational profiles. This is where businesses and organizations come to look for industry standards and best practices in setting cybersecurity agendas. The Core also contains various citations to other cybersecurity frameworks, such as the ISACA Cobit 5 and the Council on Cybersecurity’s Critical Security Controls.

The Core has five functions, which the Framework describes as follows in Section 2.1:

1. Identify: Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
2. Protect: Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
3. Detect: Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
4. Respond: Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
5. Recover: Develop and implement the appropriate activities to maintain plans.
for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

The Tiers
The Tiers are most easily understood as a resource allocation stage of the Framework. The Tiers describe the degree to which the organization’s cybersecurity risk-management practices reflect the characteristics described in the Framework. Specifically, the Tiers characterize an organization’s practices over a range, from partial (Tier 1), to risk-informed (Tier 2), to repeatable (Tier 3), and finally, adaptive (Tier 4).

By reference to the Tiers, the business or organization may determine whether it will take a reactionary approach to a cyber threat or will implement more robust and ongoing practices to prevent certain cyber threats. NIST recommends, and best practices dictate, considering the organization’s current risk management practices, threat environment, legal and regulatory requirements, and the business’s objectives and constraints during this stage of the Framework.

The Profile
The final piece of the Framework is the Profile. The Profile is best understood as an ongoing grading system where the organization compares its current practices with its target practices. At this stage of the Framework, the organization can consider re-allocating resources and reprioritizing its Tiers.

Why Is This Important to Investment Professionals?
On April 15, 2014, the SEC’s Office of Compliance Inspections and Examinations (OCIE) released a Risk Alert, which notified investment advisors that its examinations in 2014 would focus on cybersecurity as an area of importance.3 The Risk Alert favorably referenced the NIST Framework and relies heavily upon the Framework in the Sample List of Questions attached to the Risk Alert (discussed below).

The Risk Alert followed OCIE’s 2014 Examination Priorities identifying technology as a significant initiative and the SEC’s March 26, 2014, Cybersecurity Roundtable, which emphasized the need for stronger partnerships between the SEC and the private sector to address cybersecurity threats. These recent actions unmistakably signal that the SEC is focused upon cybersecurity as a critical public threat.

As SEC Chair Mary Jo White remarked during the March 26, 2014, Cybersecurity Roundtable:

> Cybersecurity threats come from many sources: criminal and hired hackers, terrorists, state-sponsored intruders, and even misguided computer experts to see what they are able to penetrate. Cyber threats also pose non-discriminating risks across our economy to all of our critical infrastructures, our financial markets, banks, intellectual property, and, as recent events have emphasized, the private data of the American consumer. This is a global threat. Cyber threats are of extraordinary and long-term seriousness.

Shortly after releasing the 2014 Risk Alert, the SEC began conducting examinations of financial institutions including investment advisors to gauge “cybersecurity preparedness.” These examinations ostensibly were designed to help the SEC identify the areas in which SEC-registered entities are addressing cybersecurity threats, and of course, those areas where cybersecurity measures could be improved.

For these examinations, the SEC provided and requested responses to the Sample List of Questions, which was attached to the Risk Alert. The Sample List of Questions addressed a broad range of issues and technical complexity. For example, one of the simpler questions was whether the investment advisor maintains an inventory of the physical devices and systems it uses. Notably, this question is reflected in the Framework Core under the Identify section: “ID.AM-1: Physical devices and systems within the organization are inventoried.”

Some more complex and technical questions include: whether the investment advisor maintains protection against Distributed Denial of Service (DDoS) attacks for critical Internet-facing IP addresses; whether the investment advisor maintains baseline information about expected events on its network; and whether the investment advisor aggregates and correlates event data from multiple sources to assist in detecting unauthorized activity on its networks or devices.

Other questions address whether the investment advisor allocates liability for cybersecurity breaches that adversely affect clients. In particular, one of the questions asked whether the investment advisor maintains insurance specifically covering losses and expenses attributable to cybersecurity incidents. In addition, another asked investment advisors to provide sample copies of any vendor agreements that incorporate requirements relating to cybersecurity risk. These questions provide incentives for investment advisors to develop policies and procedures, obtain cybersecurity insurance policies, and update third-party vendor/confidentiality agreements to specifically address liability for cybersecurity breaches.

Despite the absence of more formal regulation on this matter, it is clear that investment advisors should develop policies and procedures to reduce the risk of cybersecurity breaches. The policies and procedures that investment advisors develop in this respect should be tailored to the Sample List of Questions. They also should be resource-driven, meaning that the investment advisor should only adopt policies and procedures to the extent that they are necessary to protect clients and are tailored to actual business practices. Given the complexity of the Sample List of Questions, it would be reasonable for investment advisors to consult with information technology staff or third-party vendors before drafting these policies and procedures.

Conclusion
If OCIE’s 2014 Risk Alert did not convince advisors to take cybersecurity seriously and begin focusing on these issues, OCIE released its Examination Priorities for 2015 in January 2015.4 In that release, OCIE

Continued on page 51 •
WHY CYBERSECURITY MATTERS FOR INVESTMENT ADVISORS
Continued from page 46

specifically stated: "Last year, we launched an initiative to examine broker-dealers’ and investment advisers’ cybersecurity compliance and controls. In 2015, we will continue these efforts and will expand them …"

For those advisors who have not yet taken the SEC’s warnings seriously, we strongly recommend beginning a review of current cybersecurity policies and procedures and bolstering them. At a minimum, we recommend that investment advisors implement cybersecurity policies and procedures that: (1) identify the cybersecurity risks to the advisor’s systems, assets, data, and capabilities; (2) limit or contain the impacts of potential cybersecurity events; (3) identify the occurrence of cybersecurity events; (4) identify appropriate activities to combat detected cybersecurity breaches; and (5) restore any capabilities or services impaired as a result of a cybersecurity event.

Cary Kvitka, Esq., is a shareholder and member of Stark & Stark’s Securities Practice Group, where he focuses on counseling financial services entities including investment advisors, broker-dealers, public and private investment companies, insurance brokers/agents, and CPA firms and their employees about registration, compliance, liability, and litigation issues. He earned a BA from Tulane University and a JD from Villanova University School of Law. Contact him at ckvitka@stark-stark.com.

Max Schatzow, Esq., is an associate and member of Stark & Stark’s Securities Group, where he concentrates on counseling financial services entities including investment advisors, broker-dealers, and private investment companies about registration, compliance, liability, and litigation issues. He earned a BA from the University of Maryland and a JD cum laude from the University of Miami School of Law. Contact him at mschatzow@stark-stark.com.

Endnotes
2. See http://www.nist.gov/cyberframework/