In 2014, the SEC conducted a widely-publicized review of over 100 investment advisers and broker-dealers to learn more about their cybersecurity measures and preparedness. See “Seven Cybersecurity Risks That SEC Examiners Will Look for in Examinations of Hedge Fund Managers,” The Hedge Fund Law Report, Vol. 7, No. 17 (May 2, 2014). A recent program presented by ACA Compliance Group surveyed the current cybersecurity landscape; offered insights into what advisers and fund managers may expect from regulators going forward; discussed common misperceptions about cybersecurity; and explored goals of cybersecurity and technology risk programs. The program featured Raj Bakhru and Marc Lotti, both partners at ACA Aponix, the cybersecurity and risk arm of ACA Compliance Group. This article summarizes the key takeaways from that program.

Current Threat Environment

Lotti said that regulators expect companies to take reasonable precautions against cyber threats. He recommended that companies think not only about “cybersecurity” but also about the broader concept of “technology risk.” Bakhru noted that most victims do not even realize that they have suffered a data breach. Technology risk is risk that arises from the complexity of systems and businesses’ dependency on the Internet and those systems. Bakhru said that businesses face three key types of technology risk. The first is operational risk, which arises from attacks or data losses that disrupt or stop a company’s business. The second is the risk of adverse regulatory action arising out of inadequate systems and controls. The third is reputational damage.

Lotti said that industry has not done a good job of defining cybersecurity. He focuses on the much broader concept of technology risk, of which cybersecurity is just one element. As commonly understood, cyber attacks involve malicious intent. For example, hackers may seek to hold a company’s website hostage until a ransom is paid. Some malicious attacks, such as “heartbleed” and “shellshock,” attack systems without the target’s knowing it. In a worst case scenario, an attack can put a company out of business. Lotti cited the demise of Code Spaces, an online repository for software code, whose systems – including all backups – were wiped out when it refused to pay ransom to a hacker. Lotti said that broader technology risks do not involve malicious intent; he noted, for example, that Knight Capital lost $450 million in 45 minutes due to a lack of controls over trading software deployment. Similarly, Hurricane Sandy caused tremendous technological disruption and corresponding damage to business.

SEC Interest in Cybersecurity

Bakhru noted that in 2014, the SEC conducted a cybersecurity review of more than 100 investment advisers and broker-dealers. He said that the SEC has recently released some of the results of those reviews. See “Benchmarking and Best Practices for Hedge Fund Manager Cybersecurity,” The Hedge Fund Law Report, Vol. 8, No. 5 (Feb. 5, 2015). Lotti said that the SEC found that large majorities of broker-dealers and investment advisers had conducted some form of cybersecurity assessment. It was not clear to him, however, how such assessments were conducted and whether those assessments were adequate. Bakhru added that the SEC has announced a new program that will entail a deeper dive into five to seven targeted areas. The SEC has cited vendor management and diligence and password/authentication controls as two likely areas for investment advisers. In his view, other likely candidates are internal controls, custodial controls and incident response planning. See, eg., “SEC Chair White Identifies the SEC’s Top Concerns Arising Out of 2014
It is critical to develop a WISP well in advance of any threat. Some firms use off-the-shelf plans without tailoring them to their own specific operations. Others neglect to put enforcement controls in place. Others have policies that say that they protect data but then fail to regulate the use of portable storage devices. Others prohibit the use of personal email but fail to enforce that prohibition. These are examples of a lack of governance to ensure that existing policies are followed. In short, a firm must verify that its operations are consistent with its policies.

Common Cybersecurity Misperceptions and Mistakes

Bakhru and Lotti discussed a number of common misperceptions regarding cybersecurity and technology risks.

Myth 1: A Firm’s Information Technology (IT) Is Adequate

Bakhru said that most firms believe that their IT is adequate. However, third-party IT vendors can be the greatest source of risk, as they may hold the “keys to the kingdom.” In his experience, there are vendors that retain broad administrator credentials, giving them expansive access to firm systems. Less scrupulous IT administrators have used their access privileges to view executives’ email; others have help desks that reset passwords by phone without validation.

Myth 2: The Cloud Is Safe

Lotti has no doubt that the SEC will hold firms accountable if they fail to take reasonable cybersecurity precautions. He noted that Commissioner Aguilar has spoken about the need for board-level attention to cybersecurity. Lotti discussed a few common shortcomings on cyber risk preparedness. He noted that OCIE found that most investment advisers and broker-dealers have written information security policies (WISP). However, in Lotti’s experience, many are inadequate. Some are too broad; others are not comprehensive enough. He added that many firms have ineffective or incomplete incident response plans.

Lotti refers to the “cloud” as the running of some or all of a firm’s operations through one or more vendors off-premises and outside the firm’s immediate control. A firm can be hacked anywhere, including within the cloud. As an example, he noted that a firm can be exposed to cloud threats by offering a simple web portal for employees. Lotti said that the cloud can be made safe with appropriate transparency and controls. He stressed that a firm should not rely on a single vendor because, in doing so, “your fate is directly linked to theirs.” He recommended caution with regard to shared cloud solutions. If another firm using the same service...

Bakhru noted that the Internet’s domain name system (DNS) is another source of risk. The DNS links the domain name of a business to the numerical Internet protocol address for that business. Most firms use a third-party provider to host the domain name. Such DNS servers can be another source of intrusion if the firm does not properly secure the data on the server. For example, a hacker can redirect email from that server to the hacker and then divert the email to the firm, which will never know that the email was misdirected. A DNS breach can also cause reputational damage through creation of spoofed emails or a false website that steals client login information. Lotti added that firms can use stronger passwords and multi-factor authentication to mitigate the risk posed by domain hosts; multi-factor authentication is becoming the standard.

Bakhru noted that the Internet’s domain name system (DNS) is another source of risk. The DNS links the domain name of a business to the numerical Internet protocol address for that business. Most firms use a third-party provider to host the domain name. Such DNS servers can be another source of intrusion if the firm does not properly secure the data on the server. For example, a hacker can redirect email from that server to the hacker and then divert the email to the firm, which will never know that the email was misdirected. A DNS breach can also cause reputational damage through creation of spoofed emails or a false website that steals client login information. Lotti added that firms can use stronger passwords and multi-factor authentication to mitigate the risk posed by domain hosts; multi-factor authentication is becoming the standard.

Bakhru noted that the Internet’s domain name system (DNS) is another source of risk. The DNS links the domain name of a business to the numerical Internet protocol address for that business. Most firms use a third-party provider to host the domain name. Such DNS servers can be another source of intrusion if the firm does not properly secure the data on the server. For example, a hacker can redirect email from that server to the hacker and then divert the email to the firm, which will never know that the email was misdirected. A DNS breach can also cause reputational damage through creation of spoofed emails or a false website that steals client login information. Lotti added that firms can use stronger passwords and multi-factor authentication to mitigate the risk posed by domain hosts; multi-factor authentication is becoming the standard.

Myth 3: Passing an Intrusion Detection Test Is Sufficient

Bakhru said that some firms believe that, because they passed an intrusion detection or penetration test, their cyber defenses are adequate. He cautioned that passing an intrusion detection test is not sufficient; such tests look at a single point in time. It is more important to be thoughtful about how controls function over time and beyond the firm’s four walls. For example, a firm may pass an intrusion detection test but remain vulnerable if its CFO stores passwords on an unsecured personal computer. Risk assessments can help to identify and eliminate such vulnerabilities. Bakhru noted that there are different levels of penetration testing. The most common involve exploring known vulnerabilities and performing some manual tests. He suggests weekly vulnerability scanning of a firm’s perimeter, which can test for newly-discovered vulnerabilities and address any internal changes that may have affected security.

Lotti discussed the potential dangers of virtual private networks (VPNs), which are used to provide secure remote access to a company’s systems. While connected at the office, a laptop is protected by all of the company’s intrusion detection systems. However, if the laptop is used outside of the office, the connection may no longer be secure. The laptop may be connected to the secure corporate network but may also be able to browse the Internet at the same time. If the laptop is invaded through the direct Internet connection, it may provide a secure back-door entry into the company’s systems. Thus, each VPN connection is a potential back door into the firm. A VPN must be configured so that it is not possible to browse the Internet directly while connected to the secure network. Bakhru added that the theft of such a laptop poses other obvious dangers, including access to the network, passwords, temporary files and similar sensitive material. See The Hedge Fund Law Report’s three-part series, "What Concerns Do Mobile Devices Present for Hedge Fund Managers, and How Should Those Concerns Be Addressed? Part One of Three," Vol. 5, No. 15 (Apr. 12, 2012); Part Two of Three, Vol. 5, No. 16 (Apr. 19, 2012); and Part Three of Three, Vol. 5, No. 17 (Apr. 26, 2012).

Bakhru noted that the Internet’s domain name system (DNS) is another source of risk. The DNS links the domain name of a business to the numerical Internet protocol address for that business. Most firms use a third-party provider to host the domain name. Such DNS servers can be another source of intrusion if the firm does not properly secure the data on the server. For example, a hacker can redirect email from that server to the hacker and then divert the email to the firm, which will never know that the email was misdirected. A DNS breach can also cause reputational damage through creation of spoofed emails or a false website that steals client login information. Lotti added that firms can use stronger passwords and multi-factor authentication to mitigate the risk posed by domain hosts; multi-factor authentication is becoming the standard.

Myth 4: Cybersecurity Is a New Concern

Lotti noted that cybersecurity concerns have existed since the dawn of the Internet. Those concerns have grown as businesses and individuals have become more interconnected and dependent on the Internet. He said that some researchers believe that businesses are a decade behind hackers in security efforts. Cybersecurity is no longer a discretionary item. He added, of course, that some firms, such as large banks and quantitative hedge funds have been aware of these issues for a long time.

Myth 5: Small Firms Are Likely to Be Ignored by Hackers

Bakhru said that some firms mistakenly believe that, because they are small, they are under the radar and less vulnerable to attack. He noted that through automation,
hackers can launch attacks on an extremely broad scale. Investment advisers and other fund managers are particularly vulnerable due to the potential reputational damage they face and the number of third parties they use, each of which is a potential back-door entry point. Many firms believe they do not need to be concerned about vendors. In Bakhru’s experience, there is often a policy mismatch between a firm and its vendors; for example, a firm may prohibit use of USB drives, but its vendors may not. Similarly, SSAE 16 and service organization control audits are not adequate because they do not necessarily address risks specific to a given adviser.

**Cybersecurity and Technology Risk Goals**

Lotti said firms should strive for a balanced approach that considers all areas of technology risk. A good firewall is not sufficient; there should be appropriate security measures on each “picket in the cybersecurity fence.” He noted that companies are good at placing a number of bolts on the front door but are “leaving the garage door wide open.” Regulators and investors expect firms to exercise “due care” with regard to each element. Noting that it is impossible to close holes that a firm has not discovered, Bakhru said that a risk assessment with gap analysis is essential to developing an effective plan. He stressed that a firm must make sure that it has appropriate policies, procedures and controls in place and that it follows them. A firm must plan for incidents rather than wait until an incident occurs to react. See “Critical Components of a Hedge Fund Manager Cybersecurity Program: Resources, Preparation, Coordination, Response and Mitigation,” The Hedge Fund Law Report, Vol. 8, No. 2 (Jan. 15, 2015).

Another key element is staff training. See “Cybersecurity for Hedge Fund Managers: Compliance Best Practices, SEC Examinations and Cyber-Liability Insurance,” The Hedge Fund Law Report, Vol. 7, No. 25 (Jun. 27, 2014). Employees can be the last line of defense. Lotti and Bakhru discussed an incident in which hackers created a bogus email purporting to be from Deutsche Bank and sent it to a $250 million hedge fund seeking wire transfer information. The hackers probably used information garnered from the firm’s Form ADV. The email made it past the firm’s firewall, email security programs and all other cybersecurity measures. It was only when the COO became suspicious that the email was revealed to be a fraud.

The speakers stressed the importance of vendor management and vendor due diligence. Bakhru said that this is likely to be an SEC focus area. Vendors are an extension of a firm, often with access to the firm’s data and systems. Lotti added that firms cannot shift cybersecurity risks to vendors; regardless of its contract with a vendor, a firm will be held accountable for the operational risks it creates. He noted that, in July 2014, the FCA made it clear that banking service firms cannot outsource risk to vendors. A firm’s robust security measures and internal controls may do little good if a “vendor runs a wild west operation” and fails to mitigate its own operational risks. Lotti recommended due diligence of vendors at least annually and whenever there is a material change at a vendor. Automation can make it easier for vendors to respond to inquiries. See “How Can Hedge Fund Managers Identify, Mitigate and Insure Against Cyber Security Threats?,” The Hedge Fund Law Report, Vol. 6, No. 1 (Jan. 3, 2013).

Lotti said that password management becomes harder as passwords become more complex. Many firms store them in a word processing document or spreadsheet. He noted that there are third-party password management solutions that may be safer than storing information in a document on a potentially vulnerable system. Even password-protected computers are vulnerable to key-logging malware.

Finally, Lotti observed that most data is encrypted when it is in transit over the Internet. However, that data may not be encrypted when it reaches its destination or repository. Protection or encryption of such “data at rest” is not common now, but he believes that more firms will seek to encrypt such data in the future.