Hedge Fund Law Report
An Acuris company

Cybersecurity

Practical Steps That Commodity-Focused Hedge Fund Managers Can Take to Combat Cybersecurity Threats

Mar. 10, 2016
By Vincent Pitaro, *Hedge Fund Law Report*

Cybersecurity threats against hedge fund managers grow ever more sophisticated. Accordingly, the NFA's Interpretive Notice on cybersecurity (Notice), which became effective on March 1, 2016, calls for NFA members, including hedge fund managers registered with the NFA as commodity pool operators or commodity trading advisers, to adopt an Information Systems Security Program (ISSP) robust enough to guard against these increasing threats. See "PLI 'Hot Topics' Panel Addresses Cybersecurity and Swaps Regulation" (Nov. 5, 2015).

To assist members with those preparations, the NFA recently held a "Cybersecurity Workshop" featuring a number of senior NFA personnel and industry experts. The program, which was moderated by NFA director Amy McCormick, included NFA directors Shuna Awong, Patricia Cushing and Dale Spoljaric, as well as industry participants Patricia Donahue, senior vice president and chief compliance officer at Rosenthal Collins Group, LLC; Buddy Doyle, founder and CEO of Oyster Consulting; and Peter Salmon, a senior director at the Investment Company Institute.

Among other topics, panelists discussed critical cybersecurity threats, cybersecurity response plans, training and other practical cybersecurity measures. This article summarizes the panelists' discussion of these issues.

For additional coverage of the NFA's Cybersecurity Workshop, see "Hedge Fund Managers Face Imminent NFA Cybersecurity Deadline" (Feb. 25, 2016).

Common Threats

The most dangerous hacking is conducted by sophisticated criminal enterprises that run 24-hour call centers and sell malware tools, said Salmon. He observed that a huge number of attacks are never reported in the media, and he challenged the media's frequent use of the term "sophisticated attack."

In Salmon's view, people often do not think before they act; in many cases someone simply "clicked on an email" or "inserted a flash drive" when they should not have. In Doyle's experience, most recent hacking has involved human resources systems. For more on cybersecurity threats, see "K&L Gates-IAA Panel Provides Comprehensive Overview of Cybersecurity Laws and Threats Applicable to Investment Managers (Part One of Two)" (Apr. 23, 2015).

Email Attacks

Salmon explained that hackers do a great deal of "reconnaissance" on potential targets using social media. They may also infiltrate a firm to observe how a particular employee functions and communicates within the firm. They then use that information to create a carefully targeted phishing attack.

The scale of such attacks is huge; Salmon observed that $1 billion has been wired out of banks using compromised business emails. In one common type of attack, said Donahue, a hacker will hijack a customer's email account to learn about how the customer communicates with its broker. It then tries to wire a small amount of money; if that works, it sends a much larger wire.

Once money is wired overseas, it is very difficult to get it back. As a result, firms have introduced strict controls over outgoing wires. One good practice is to request standing wire instructions from customers. A request to use different wire instructions should trigger close scrutiny, such as a request for a signed instruction letter and a follow-up call to the client.

One business owner recounted a harrowing near miss: hackers got into his email, learned about his firm's banking routines and requested a wire from his bank. The only reason that the scheme failed was because the hacker mistakenly addressed the banker using the banker's full name, rather than the nickname that the owner always used. When the banker called the owner to ask why, the owner discovered that he had been hacked. Donahue said that this anecdote illustrates why a confirmatory phone call to a number that a broker or bank has on file for a customer can be so important.

Another audience member called attention to a new "social engineering" scam in which a hacker uses information from LinkedIn to target a recently hired chief financial officer. In an email that appears to come from the CEO – but which actually comes from "CEO@xyz.co" rather than "CEO@xyz.com" – a hacker creates a pretext for an urgent wire transfer.

The audience member added that the FBI is overwhelmed with such matters and may not respond quickly. For FBI perspectives on cyber crime, see "RCA Panel Outlines Keys for Hedge Fund Managers to Implement a Comprehensive Cybersecurity Program" (Jun. 18, 2015).

Malicious Insiders

In Salmon's view, malicious insiders pose perhaps the most insidious risk. One way to minimize such risk is to limit access to only the information that an employee needs to complete his or her job. Even individuals that have administrator-level access should have some limitations on what they are able to do. Doyle added that firms could also run credit checks on employees to see if they are in financial trouble. See also "What Hedge Fund Managers Need to Know About Information and Data Security" (Jul. 1, 2011).

Response Plans

In Salmon's experience, most firms in the financial industry have a good handle on business continuity preparedness but are not fully prepared for cybersecurity incidents. At a minimum, every firm should have a detailed written incident response plan and a detailed escalation procedure, he said. The plan must define what type of incident will trigger a response.

Escalation procedures are essential. For example, a low-level employee of a small firm who discovers an issue late at night might be afraid to call the CEO until the morning. Doyle

concurred that employees must know who to call, and the firm must have a defined response team. See "K&L Gates-IAA Panel Addresses Cyber Breach Response Plans for Investment Advisers (Part One of Two)" (Jun. 25, 2015).

There are many different breach notification laws throughout the U.S. and in non-U.S. jurisdictions, explained Donahue. A firm should have experienced outside counsel that can navigate the requirements lined up in advance. Notification requirements turn on what data has been exposed, so a firm must be able to promptly figure out what happened.

Having outside counsel will also help to preserve attorney-client privilege, said Salmon. For that reason, counsel should usually hire whatever experts are needed to address the situation. Salmon also recommended that firms develop a relationship with local law enforcement. The firm's general counsel should be involved in the process because the law enforcement response will likely require access to the firm's networks. This should all be part of an incident response plan.

Some firms purchase cyber breach insurance. Salmon cautioned that such policies can be a minefield; they have become so specific that they may exclude many incidents. For example, he said, business email fraud may not be covered because the policy is limited to "financial instrument" fraud, and emails are not "financial instruments." See "K&L Gates-IAA Panel Addresses Cyber Insurance Plans for Investment Advisers (Part Two of Two)" (Jul. 2, 2015).

Cybersecurity Measures

Training

Salmon stressed that there must be ongoing training of all employees. Some vendors will "gamify" training to make it interesting and engaging. Everyone from the mail room to the board room must be accountable.

Employees should be encouraged to report when they notice anomalies in their computer or data, Doyle said. Training using scenarios is very effective, he added. He observed that a criminal needs to be right only once, while a firm's information security team must be right all the time. See "Essential Tools for Hedge Fund Managers to Combat Escalating Cyber Threats" (Feb. 4, 2016).

Penetration Testing

The Notice indicates that penetration testing can be used to help evaluate a firm's cybersecurity defenses. Cybersecurity testing is an "exercise in finding gaps," Salmon said. "Testing and failing is a good thing," because it enables firms to improve their defenses.

Some penetration testing firms have a relationship with law enforcement, noted Salmon. Doyle cautioned that cybersecurity vendors should be segregated; a firm that provides security consulting and guidance should not be affiliated with the firm that does penetration testing.

Employees should not be notified when testing will occur, Doyle continued. The cost of testing will depend on the particular circumstances and how extensive the testing will be.

Testing firms usually find some issues, noted Doyle. They may not actually breach a firm's defenses, but even making billions of attempts at getting access without being detected evidences a problem. For more on testing, see "K&L Gates-IAA Panel Addresses Regulatory

Compliance and Practical Elements of Cybersecurity Testing": Part One (May 21, 2015); and Part Two (May 28, 2015).

Passwords

The strength of a password is much more important than changing it periodically in Salmon's view. Frequent rotation of passwords encourages people to use simpler passwords that are easier to remember. Thus, for high-value targets, it may be more effective to require a much stronger password.

Doyle explained that length and complexity of passwords make a big difference. He also cautioned that people should not use the same password for multiple sites, because compromise of one site can lead to access to other sites. Salmon noted that the SANS Institute and the National Institute of Standards and Technology have helpful information on creating strong passwords.

Client Intake and Management

Donahue pointed out that a firm's new accounts department is the key entry point for personally identifiable information (PII), because anti-money laundering and "know your customer" rules require firms to obtain a considerable amount of PII, such as social security and driver's license numbers.

Her firm ensures that its online application exposes such information for only a very short time before it is removed. It also makes that information inaccessible on internal systems. In addition, the firm limits third-party access to PII and obtains written consent from customers prior to providing any PII to third parties. See "Investment Adviser Penalized for Weak Cyber Policies; OCIE Issues Investor Alert" (Oct. 1, 2015).

Customers are very protective of their information but often hesitant to adopt new procedures to protect it, in Donahue's view. The practice of sending out customer statements by email will likely stop. Customers will have to follow more robust procedures to obtain their statements.

Donohue's firm has also prepared a template to help brokers comply with the Notice and their obligation to adopt an ISSP. It covers matters such as software updates, firewalls, antivirus and encryption.

Cybersecurity Resources

The Investment Company Institute has created a chief information security officer working group for industry peers to exchange information, noted Salmon. It has also conducted a detailed cybersecurity survey of its member firms.

Cushing added that there are industry groups that share information on cybersecurity threats, vulnerabilities and incidents, including FS-ISAC [the Financial Services Information Sharing and Analysis Center]. She encouraged firms to contribute to that system to spread word of new threats.

Doyle referred participants to the Privacy Rights Clearinghouse, which tracks data breaches and provides information on why they occurred and who was affected.

contents, or any contents on the password-protected Hedge Fund Law Report website. (Your subscription agreement explains how you can use contents for reports and presentations.) UNAUTHORISED USE OR DISCLOSURE IS UNLAWFUL.

This material has been printed by and is for their consumption only. The full Terms of Use are available at www.hflawreport.com.
UNAUTHORIZED USE OR DISTRIBUTION IS UNLAWFUL