A Fund Manager's Cyber Security Action Plan:

Practical Tips on Preparing, Training, Implementing and Testing

May 2016

Table of Contents

Cybersecurity Risks and the Current Regulatory & Legal Landscape

Cybersecurity has fast become an imminent and pervasive threat to the investment management industry. Investment advisers, including those managing private funds ("Fund Managers") are required to disclose and report a higher quantum of more sensitive and meaningful information than ever before, via Form ADV, Form PF, CPO-PQR and (for some Fund Managers) Annex IV. Cyber-attacks can be manifested in a variety of ways from multiple sources and can lead to direct losses (e.g., theft of funds, data or other property), reputational harm, regulatory actions, third party litigation and other forms of liability.

While it's reasonable to believe that a typical CFO would not respond to a "spear-phishing" email from a fictional Nigerian prince, consider the risks presented by a more realistic cyber-attack wherein a personal email is sent to the CFO, purporting to be from your prime broker, auditor or administrator (information discoverable from your Form ADV), mimicking the patterns and style of previous email communications (discoverable from your email server) and asking for confirmation of a recent wire or some other sinister request. Internal attacks such as this are discussed further throughout this paper, and each one has the potential to cripple a fund and/or damage thousands of investors.

Several of the regulatory bodies that oversee Fund Managers (including the Securities and Exchange Commission ("Commission" or "SEC"), FINRA, the CFTC and the NFA) have highlighted cybersecurity as a critical issue that poses a myriad of direct threats to Fund Managers and have taken a collective position that Fund Managers must take action to design, implement and monitor a program that will protect the confidential information and other data entrusted to them (a "Cybersecurity Program"). In fact, one commissioner recently characterized cybersecurity preparedness as a "defining issue of our time" and, at a later date, instructed Fund Managers and their Boards of Directors who choose to ignore or minimize cybersecurity risks, that they "do so at their peril". The Commission, in particular, has made numerous speeches, conducted roundtables and issued materials on this matter. Moreover, alerts, updates, primers, releases and other purported "guidance" materials abound the Internet and crowd the inboxes of Fund Managers.

By any measure, the investment management community as a whole has been put on notice of the significance of this issue and the severity of the risks it poses and, for those Fund Managers who have not yet designed and begun to implement a Cybersecurity Program, it is accurate to state that such managers have failed to comply with a regulatory hot-button issue that has ranked as one of the Commission's top examination priorities over the last three years.

To be fair, however, the regulatory guidance issued to date does not provide clear standards, checklists or protocols for developing a Cybersecurity Program. Rather, such directives are more 'principals-based' and provide various considerations for Fund Managers to recognize as they develop their Cybersecurity Programs. And although the guidance materials from the SEC, the NFA, the CFTC and FINRA are not entirely in consonance, the common theme among them is an overarching directive that Fund Managers must commit to adopting a culture of cybersecurity compliance that permeates the entire enterprise. The materials do not map out a program, provide draft policies or describe a particular technology or other solution but rather, taken together, they set a regulatory expectation for Fund Managers to:

- do the initial work of assessing, designing and customizing such a program; and
- follow through with continued efforts of integrating, testing and monitoring the program for its effectiveness.

The Commission's position in this regard was demonstrated in its 2015 action against a St. Louis -based registered investment adviser, R. T. Jones Capital Equities Management, Inc. ("R.T. Jones"). In this case, R.T. Jones stored certain personally identifiable information ("PII") of more than 100,000 individuals[1], on its third-party hosted servers, for a period between September 2009 and

Chronology of Key Regulatory Events

2014

1.30.14
SEC Compliance Outreach Program National Seminar

2.26.14
CFTC Cybersecurity/GLB Part 160 Guidance

3.26.14
SEC Cybersecurity Roundtable

4.15.14
SEC 2014 Cybersecurity Initiative Risk Alert

11.19.14
SEC Adopts Regulation Systems Compliance & Integrity (Regulation SCI)

2015

2.03.15
FINRA Report on Cybersecurity Practices

2.03.15
SEC Cybersecurity Sweep Risk Alert

3.18.15
CFTC Roundtable on Cybersecurity & System Safeguards Testing

4.28.15
SEC Division of Investment Management: IM Guidance Update

9.15.15
SEC 2015 Cybersecurity Initiative Risk Alert

2016

3.01.16
NFA's Cybersecurity Interpretive Notice Takes Effect

July 2013. These servers were infiltrated by a cyber-attack, emanating from China.

Although R.T. Jones: (i) promptly engaged more than one cybersecurity consulting firm to take remedial action; (ii) provided notice to all parties that their PII was compromised; (iii) offered free identity theft monitoring to such parties; and (iv) found no evidence that such PII was actually ever stolen or even affected, the SEC still took the position that R.T. Jones had violated the law by failing to adopt policies and procedures reasonably designed to protect against threats to the security of its customer and third-party information. Ultimately, the SEC censured R. T. Jones, ordered it to cease and desist from further violations and to pay a $75,000 fine. And thus, the Commission has made clear that even in the absence of an actual attack or a security breach, the failure of a Fund Manager to design and implement a Cybersecurity Program is actionable.

The Commission's assertion of authority over the data management practices of Fund Managers is derived from Section 30(a) of Regulation S-P[2] (the "Safeguard Rule"), which generally requires all Fund Managers registered with the Commission to adopt policies that are reasonably designed to protect the security and confidentiality of customer records and information from anticipated threats or hazards and unauthorized access or use. The Safeguard Rule thus provides the statutory basis for the Commission's position on devising a Cybersecurity Program. Of course, this simple directive – to adopt policies reasonably designed to protect client information – becomes less simple when applied to each manager's unique business DNA (i.e., its infrastructure, operations, network, staff, client base, trading activity and investment program).

Risks Employees Pose to a Firm's Cybersecurity Posture

With the mounting regulatory pressure outlined above, Fund Managers can no longer afford to sit idly and rely on technology to protect them from the next cyber-attack. Advanced technology systems and infrastructure protocols are, of course, critical in mitigating cyber risk, however, for the prudent Fund Manager, the list of defense mechanisms cannot end there. Even while the sophistication of perimeter security systems and vigilant monitoring tools increases, the greatest vulnerability to a firm remains within its interior: its own employees – the people who use IT systems to conduct transactions and access sensitive data.

Employees – particularly those with unrestricted access to sensitive information and financials – are a hacker's easiest access point into a firm. Every day, more employees fall victim to social engineering schemes and phishing attacks designed to fool them.

Entering a password or financial information. Downloading malicious software. Transferring funds. Hackers are well-versed in how to trick users into committing these acts. And while not malicious (though we'll discuss that also), these employee actions

can end up costing their organizations more than money.

Let's look at unintentional security risks presented by employees – many of which can be addressed through training and creating a culture of security.

Getting Caught by Phishing

The art of phishing has evolved greatly over the last several years. Once a spam-like email asking the recipient to click a link, today's "phish" are targeted, highly personal and sophisticated. Hackers are conducting thorough background research to compile employee names, titles and contact information. Emails that include personal information are more likely to be taken seriously, meaning employees need to be much more vigilant when combing through their inboxes.

In today's world of oversharing, it's become much simpler for hackers to acquire personal information and understand organizational hierarchies. Social media profiles, in particular, are great fodder for would-be cyber criminals. With modern-day ability to obtain private details and observe communication styles and patterns, hackers now have access to a variety of tools to mirror email addresses, website URLs and dialect. The end result is the criminal's identity masqueraded as a legitimate, trustworthy source.

Unintentional Risks Abound Beyond Social Engineering

Social engineering – broadly defined as any act of manipulation designed to obtain the confidential information or property of another party – continues to put firms at risk at the hands of sophisticated hackers. But beyond phishing schemes, there are a number of unintentional threats that can pose danger to a Fund Manager as a result of an employee's actions or inactions, including:

- *Employees being too busy/rushed*. Sometimes users are in too much of a rush to think through their actions. Perhaps an employee is expecting a package in the mail. When they happen to see an email that looks like it's from a postal service, they click the link – without, of course, realizing it's an elaborate phishing scheme.

- *Weak or shared passwords.* Passwords are one of the easiest gateways for hackers to infiltrate a firm's network. Passwords that contain basic user information (names, birthdates, kids' names, etc.) are often easy to guess after a simple search of a user's social media profiles. Organizations should enforce strong passwords, prompting users to change them at least every 90 days and ensuring they contain uppercase and lowercase letters, special characters and other unique requirements.

- *Poorly protected mobile devices.* Users are responsible for ensuring the devices they use on behalf of their company are protected. Laptops and mobile devices should

require strong passwords to access (see previous) and should not be left unlocked and unattended. Additionally, access to computer room infrastructure or backup tapes should be limited to only essential employees.

- *Improper disposal of hard copy documentation.* If financial documents or other sensitive materials are left sitting on a printer or not disposed of properly, this poses another security risk to the firm.

- *Visitor access to the network.* Providing non-password-protected guest Wi-Fi access or allowing visitors to access firm computers also opens the Fund Manager up to security threats. Organizations should keep strict visitor logs and ensure non-employees only have access to necessary information.

- *Lack of knowledge or security awareness training.* The above threats may be unintentional, but they all can easily be avoided with comprehensive information security awareness.

Intentional Risks: Insider Threats & Disgruntled Employees

As outlined above, there are a number of instances in which employees unintentionally put their firm's data at risk. But beyond naiveté and laziness, there are also employees who deliberately choose to attack their firms by way of stealing, compromising or deleting company confidential information. A disgruntled employee may have an axe to grind if he/she has recently been reprimanded or doesn't agree with management decisions. Some employees may look for monetary gain if they have access to company financials such as credit card or wire transfer information. Others may look to share trade secrets or destroy a company's reputation – perhaps for no reason at all. And, of course, there are those employees who will attempt to steal confidential information for their own personal gain.

Consider the high-profile case involving Goldman Sachs and its former employee, Sergey Aleynikov, in which Aleynikov was hired by Goldman Sachs in 2007 and, in conjunction with his acceptance of employment by a competitor, admittedly stole the code of Goldman's high-frequency trading model with the intent to use such code to compete against Goldman itself. The dispute has still, as of the date of this writing, not been entirely resolved and has forced each party to expend enormous amounts of time, resources and money to deal with it. Many similar cases have since been reported, involving both sophisticated enterprises including Highland Capital[3], Société Générale S.A.[4], Citadel[5], and other, less notable, trading enterprises[6].

As has been clearly demonstrated, employees are often overlooked as a significant and visceral vulnerability when it comes to security. Ironically, the case can also be made for a firm's employees to be its greatest cybersecurity asset. With the proper training,

education and firm-wide support, employees can provide the most formidable and effective line of defense against everything from the savviest hackers to simple, everyday security exploits.

How to Make Employees a Cybersecurity Asset

The best way to make your firm's employees a cybersecurity asset is to provide them with comprehensive security awareness training as well as establish clear expectations by way of corporate practices, policies and manuals. Management must instill the importance of cybersecurity preparedness in all employees by making it a top-down priority.

We'll look at these three components in this section.

The Training Component

Whether you design training in-house or leverage the services of an outside training agency, an effective security awareness program should include education on specific threat types, including, but not limited to:

- Malware
- Trojans
- Viruses
- Social engineering
- Phishing/Spear-phishing
- Incident response protocols

Phishing attacks are common in the financial services industry. In 2015, the CFO of a London-based hedge fund was manipulated into granting access to its bank account to a hacker (posing as an officer of the fund's bank) who was able to steal approximately $1,200,000 from that fund's bank account. And thus, phishing defense training and education should detail how employees can take multiple steps and use a checks-and-balances system to avoid succumbing to a cyber-attack. For example, if an employee receives an email that he/she suspects might be a phishing scheme, he/she should use multiple points of verification to identify its authenticity. If the email alleges it is from the firm's CFO, the email recipient should contact the CFO directly for actual verification. This type of verification is especially critical when financials are involved, for instance if the email is calling for a wire transfer.

Additionally, employees should carefully examine URLs and email addresses, as phishing emails often attempt to mirror true contact information but instead display a minor change that often goes unnoticed by the untrained eye.

Security awareness training should also address the importance of password construction and security. We've already highlighted that password cracking can be remarkably easy, particularly for advanced hackers. Therefore, this daily task that most employees consider menial is actually critical to the overall security of an investment firm.

Employee Training Delivery Methods

There are a number of ways firms can go about delivering comprehensive security awareness training to its employees.

- *Face to Face Sessions* – Many organizations find that face-to-face, instructor-led training is the best way to instill a culture of security across the firm. By focusing on what business users need to know to keep IT resources secure and protected, the firm can empower employees to become security assets. Scheduled training sessions of 30-60 minutes in length let users learn visually and practically and send a strong message about the importance of security and the role employees can play in protecting the firm.

- *Video Courses* – If face-to-face sessions aren't practical, on-demand video lessons can fill an important gap. They also allow employees to ask quick questions that may not require full-scale training sessions to answer. Short segments on a variety of key topics can equal great resources for users across all regions.

- *Start Early* – Completing information security awareness training should be one of the first tasks an employee is expected to tackle upon their start at the firm. This underscores the Fund Manager's commitment to security and ensures employees recognize their own roles and responsibilities from day one.

- *Keep it Going* – Regular annual training is great, but what happens the other 364 days of the year? Make sure employees receive a steady stream of information around data security. Keeping them updated with news about emerging threat strategies, for example, will reinforce the company's security-oriented culture.

The Plans, Policies and Penalties Component

Training materials should also review corporate policies and clearly detail consequences for any suspicious or malicious behavior amongst employees. Let's dive deeper on how a Fund Manager can create manuals and policies that empower employees and ensure compliance and accountability.

The written policies of a given fund will depend upon, and should conform to, the size, scale and nature of a particular fund. At minimum, a set of policies should be able to demonstrate a Fund Manager has taken reasonable efforts to protect its fund from

cybersecurity risks. If appropriate, these policies can be combined as a compendium, incorporated into a compliance manual or employee handbook or, for larger funds with additional resources, comprise a dedicated Cybersecurity Manual.

The following are policies firms should consider adopting and implementing as part of a comprehensive Cybersecurity Program:

- *Access Control Policy*. Should provide direction for managing access to internal and external (i.e., client/investor) information systems.
- *Acceptable Use Policy.* Should outline behavior that is considered acceptable and unacceptable with reference to corporate devices, system and network activities and email and other forms of communication.
- *Incident Response Plan.* Details the steps necessary following a security incident, including roles and responsibilities, notification guidelines, evidence handling, mitigation, etc.
- *Information Security Policy*. Explains the firm's policy regarding the protection of confidential employee and client information.
- *Visitor/Contractor Access Policy.* Provides guidance for non-employees visiting company premises.
- *Social Media Policy.* Provides guidance regarding acceptable employee behavior on social media sites.
- *Mobile Device Agreement.* Details expectations and requirements for operating company-owned or operated mobile devices including laptops, smartphones, etc.

Regardless of the breadth and depth of the policies a Fund Manager may adopt, it's critical to understand that the selection and adoption of such policies alone do not meet the regulatory burden at issue. Fund Managers must also be prepared to demonstrate the written policies have been fully implemented and integrated into the firm and are part of a firm-wide initiative to prepare for, prevent and/or remediate any cybersecurity breach.

Management's Role In Creating A Culture of Security

Enforcing these policies and integrating them into the firm's overall culture is the responsibility of the firm's leaders. The tone is set at the top. If the management team is not fully committed to enforcing security practices, there is little hope for the firm's employees to succeed.

This commitment from the top can be demonstrated in many of the ways we've already discussed:

- Implementing sound policies and procedures,
- Delivering comprehensive awareness training, and
- Ultimately fostering a culture that takes security seriously and builds defenses internally and externally to mitigate risk.

Without participation and encouragement from upper management, the walls your firm attempts to build may come crumbling down.

Protecting Against Malicious Employees

As discussed previously, employees can pose serious risks to a firm's security – whether they intend to or not. In most cases, users are unaware of the effects their actions or inactions can have on the greater organization. But there are also times when security lapses are not the result of mistakes or careless oversights. They are, rather, the deliberate result of disgruntled or malicious employees – those with access to sensitive information and the intent to bring harm to the firm. It is during these situations where the need for clear technology and administrative safeguards becomes apparent.

Following are several steps Fund Managers can take to prevent or mitigate the damage caused by malicious employees:

- Lock USB ports to prevent data transfer
- Implement segregation of duties
- Create and implement Access Control policies based on the principle of least privilege
- Utilize file system auditing and alerting software tools
- Perform background and credit checks during the hiring process
- Closely monitor lower-performing employees
- Establish an incident response plan

What's Next? What Regulators Want to See

As this regulatory initiative continues to advance, the standards and expectations of regulators will heighten and Fund Managers will be expected not only to be aware of and informed about cybersecurity, but to have designed and implemented a Cybersecurity Program that is already being regularly tested, tweaked and tailored to the unique needs of that Fund Manager's business and clientele. Fund Managers must also be cognizant of the fact that the Commission itself is gaining, in terms of its size, capabilities and momentum. Consider that in 2015, the Commission filed a record number of 807 enforcement actions and obtained orders for $4.2 billion in penalties and disgorgements[7]. And just recently, the Commission announced the creation of a new division, the Office of Risk and Strategy, in an effort to increase its oversight and examination of investment advisers and other market participants.

It's clear that there is no black box, no singular hire, no outsourcing solution that can, in a vacuum, be a panacea to the cybersecurity epidemic. However, the regulators have made clear that the most egregious action they will pursue is, ironically, inaction.

Conclusion

Recognizing the importance of these risks and both the resources and disposition of the current SEC regime, it becomes clear that the risk of experiencing a cybersecurity examination or review for Fund Managers is higher than ever before. Currently into its second "Cybersecurity Sweep", the Commission is prepared to review your systems, interview your employees, evaluate the responsiveness and effectiveness of your protective measures and determine the extent to which your organization, as a whole, can identify, prevent and remediate cyber-attacks. Addressing this challenge requires a team approach that flows through your entire enterprise. Put simply, designing your Cybersecurity Program, training and incentivizing your employees and committing to periodic assessments will create the proactive culture of compliance that the Commission expects.

Sources:

[1] Specifically, R. T. Jones entered into an agreement with a retirement plan administrator and retirement plan sponsors to provide investment advisor to individual plan participants through a managed account platform.

[2] See 17 C.F.R. §248.30(a).

[3] See *Highland Capital Management LP v. Daugherty*, 12-04005, District Court of Dallas County, TX 68th Judicial District (Dallas) (where hedge fund sues its former General Counsel and Senior Executive for allegedly stealing over 60,000 documents of confidential and proprietary information).

[4] See *United States v. Samarth Agrawal*, 10 Cr 427 (JSR) (former employee convicted of stealing source code and transferring it to his new hedge fund employer).

[5] See *United States v. Pu*, (former employee sued by Citadel for allegedly stealing source code and intending to transfer it overseas in an effort to launch a competing business).

[6] See People of the State of New York v. Vuu, 3869/2013, and People of the State of New York v. Cressman, 3870/2013, New York State Supreme Court, New York County (Manhattan).

[7] This data is based on the Commission's fiscal year which ended Sept 30, 2015.

About Eze Castle Integration, Inc.

Eze Castle Integration is the leading provider of IT solutions and private cloud services to more than 650 alternative investment firms worldwide, including more than 100 firms with $1 billion or more in assets under management. The company's products and services include Private Cloud Services, Cybersecurity & Technology Consulting, Outsourced IT Support, Project & Technology Management, Professional Services, Telecommunications, Voice over IP, Business Continuity Planning and Disaster Recovery, Archiving, Storage, Colocation and Internet Service. Eze Castle Integration is headquartered in Boston and has offices in Chicago, Dallas, Hong Kong, London, Los Angeles, Minneapolis, New York, San Francisco, Singapore and Stamford.

Learn more at www.eci.com.

About Sadis & Goldberg, LLP

Sadis & Goldberg is a leading New York based law firm with practices in hedge, private equity, venture capital, real estate and commodity fund formation, family office, transactional counseling, compliance services, regulatory representation, litigation, derivatives, tax, ERISA, estate planning and real estate.

Learn more at www.sglawyers.com.