Critical Cybersecurity Threats & How to Prepare

industry advice and best practices for hedge funds and investment firms

About Eze Castle Integration
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, Technology Consulting, Outsourced IT Support, Project & Technology Management, Professional Services, Telecommunications, 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. Visit us at www.eci.com.
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Industry Today</td>
<td>3</td>
</tr>
<tr>
<td>Cybersecurity Risks and the Current Regulatory Landscape</td>
<td>4</td>
</tr>
<tr>
<td>A Hacker’s Toolkit: Cybersecurity Threats to Financial Firms</td>
<td>6</td>
</tr>
<tr>
<td>Best Practices: Building a Secure Investment Firm</td>
<td>8</td>
</tr>
<tr>
<td>Beyond Technology: Make Employees a Cyber Asset</td>
<td>10</td>
</tr>
<tr>
<td>Cybersecurity Incident Response: What Now?</td>
<td>12</td>
</tr>
<tr>
<td>A Few More Best Practices</td>
<td>13</td>
</tr>
<tr>
<td>Conclusion</td>
<td>13</td>
</tr>
<tr>
<td>About Eze Castle Integration</td>
<td>14</td>
</tr>
</tbody>
</table>
THE INDUSTRY TODAY

The financial services industry has undergone a series of significant changes in recent years. We have seen the proposal and implementation of new regulations, a surge in investor due diligence requirements and a constantly challenging marketplace that has led to a transformation in the way funds do business.

Perhaps of greatest significance to a firm’s IT operations is the focus on cybersecurity – as a result of a number of high-profile security breaches and vulnerabilities and an impactful “hacktivist” community looking to leave their mark on the world. The financial services industry, in particular, remains a target of cyber-attacks, and while engaged in an arms race as security threats constantly evolve, hedge funds and their investors continue to advance security postures to mitigate risks.

The threat landscape changes on a daily basis and requires firms to stay diligent and proactive in maintaining security programs that not only protect from external attacks but also from more likely internal breaches (accidental and malicious). As social engineering tactics reach new levels of sophistication, internal security incidents are far more likely to occur and cause damage to a firm’s operational infrastructure. In other cases, security vulnerabilities (aka bugs) arise that threaten to destroy countless businesses.

Regardless of the method or root location, these security threats are real, and the only true way to thwart an incident is to establish a layered security program to safeguard against attacks and vulnerabilities of all kinds.

This whitepaper serves as a guide to hedge funds and investment firms looking for the latest information on cybersecurity threats to the industry as well as offers practical advice on building and maintaining a secure operational infrastructure and ongoing security program.
CYBERSECURITY RISKS AND THE CURRENT REGULATORY & LEGAL LANDSCAPE

Excerpt written by Sadis & Goldberg, LLP and originally published in May 2016 Cyber Action Plan Paper

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 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.

---

\(^1\) July 2013

\(^2\) Section 30(a) of Regulation S-P
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).

A HACKER’S TOOLKIT: CYBER SECURITY THREATS TO FINANCIAL FIRMS

External cybersecurity attacks come in all shapes and sizes, and oftentimes we never fully understand the root cause or the intended outcome of the threats. As the industry continues to keep its finger on the pulse of cybersecurity and we communicate about attacks and vulnerabilities – new and old – we learn more about what a hacker is really after and, therefore, how best to protect that information.

What types of information are hackers after?

Hackers infiltrate corporate technology environments for a variety of reasons. In the retail arena (such as in the case of Target, TJX and other scandals in recent years) the perpetrator may be seeking customer data such as credit card information or social security numbers. In the investment industry, it is more likely that a hacker will attempt to steal information on a firm’s intellectual property, such as business plans, trading programs, market forecasts and investment strategies.

How are they infiltrating networks?

Experienced hackers – or “hacktivists” – use a variety of methods to infiltrate networks and gain access to sensitive information, including denial-of-service attacks, phishing, malware and software vulnerabilities. Let’s dive into these hacker tools.

**Phishing (Social Engineering)**

An increasingly common tactic, the act of phishing refers to a hacker “psychologically” attacking a victim by tricking them into taking an action that results in the victim either providing personal information (such as password information), opening up an infected attachment or responding to spam.

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.

**Malware & Ransomware**

The term malware encompasses a number of security threats that could negatively affect a business’s network, including viruses, worms, Trojan horses and spyware. While each of these has its own nuances, they are all deployed with the intent to damage systems and networks, oftentimes with very little noticeable interruption.

One example of a malicious ransomware trojan that first caught the attention of firms is Cryptolocker but today new ransomware threats abound. Cryptolocker, as an example, is a variant of ransomware that restricts access to infected computers by encrypting them and demanding that the victim pay a ransom in order to decrypt and recover their files. Some versions of Cryptolocker can encrypt local files as well as external hard drives, network file shares and even cloud storage services that allow local folders to sync with online storage.

Regular file and server backups become critical in cases such as this as infected computers need to be restored back to a point before the ransomware was installed in order to avoid paying the ransom. This highlights the importance of firm’s taking a holistic view when creating security and data protection programs.

**Software Vulnerabilities**

Another vulnerability hackers love to exploit is out of date software. One example was the critical vulnerabilities discovered in the Symantec anti-virus products in June 2016. The vulnerabilities were reportedly triggered by delivery of a specially constructed file to a user, which exploits Symantec when Symantec’s I/O filter intercepts the file for parsing. Delivery of the file can be via email as an attachment or via file download. The user does not have to open the file to trigger the exploit.

---

**Phishing Red Flags: Educate Employees**

- Check the sender email address as well as “to” and “cc” fields
- Is it personalized? Be wary of generic greetings
- Improper spelling and grammar can be giveaways as well
- An overwhelming sense of urgency requesting personal information
- Links! Only click on those that you are expecting (same goes for attachments)
- Roll your mouse pointer over a link to reveal its true destination
- Suspicious emails from trusted sources can happen. If your friend/colleague sends a strange message, their account may have been attacked.
While Symantec fixed this bug, there was still a window of time that firms may have been vulnerable. It is at times like these that employee security awareness training is critical.

Mobile Devices

In today’s smartphone-reliant world, hackers are shifting their focus and resources to mobile devices. With a user’s life virtually captured within a single phone or tablet – everything from contacts and email to documents, passwords and location-based information – hackers recognize the value of such devices. Some would argue mobile devices now hold as much as or more personal information than PCs or laptops, and most do not come standard with anti-virus or malware protection software.

In August 2016 Apple was forced to quickly release a critical update to its iOS addresses multiple security vulnerabilities – namely three iOS flaws that cybercriminals or governments can use to steal confidential messages and eavesdrop using your device’s camera and microphone.

Distributed Denial-of-Service (DDoS) Attack

One more strategy used by hackers is distributed denial-of-service. DDoS attacks are “efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.” Typical DDoS attacks may involve overloading communications through a network to slow down resources or forcing network reboots. While not overly common in the hedge fund and alternative investment industry, these attacks can occur.

BEST PRACTICES: BUILDING A SECURE INVESTMENT FIRM

Hackers are always seeking new ways to gain access to protected systems and accomplish their goals. Anti-virus and anti-malware developers are likewise on the hunt for ways to protect these systems and data from new intrusion methods. To increase protection, hedge funds and investment firms should employ a Defense in Depth strategy. This includes maintaining up-to-date anti-virus and anti-malware software as well as network firewalls, deep inspection proxy and intrusion detection and prevention systems (IDS/IPS) to reduce the amount of traffic on the network.

It also means taking into account physical and virtual security elements. Following are items to consider from a physical security perspective:

- 24x7x365 manned lobby with visual verification of identity
- Two-phase authentication of visitors (card and biometric)
- Secured access doors and elevator banks
- Monitored security cameras
- Additional door, motion and camera sensors
- Visitor logs for cages
- Key-locked cages and cabinets
At the virtual level, monitoring becomes essential. Work closely with your IT department or cloud services provider to ensure they have comprehensive control and extensive visibility over your infrastructure at all times. You need to ensure it is highly secure and cannot be penetrated by external attackers or easily manipulated by internal threats.

**The Other Layers of Defense**
In addition to these layers, investment firms should also employ the following policies and procedures to ensure their critical systems and data do not fall into the wrong hands.

**Principle of Least Privilege**
This involves restricting access to only those employees who need it. Keep access control lists on all applications and data and inbound/outbound Internet access to keep track of who can gain access to what.

Also, it is advised that firms and/or their service providers log the use of audited one-time passwords and minimum privilege shared accounts.

**Secure User Authentication Protocols**
Another layer of security firms should have in place centers on secure user authentication protocols. This includes:

- Assigning unique domain user IDs to each employee
- Limiting access to only active users and active user accounts
- Implementing strong domain password policies, which can include:
  - Enforcing password history, maximum password age, minimum password length, and password complexity requirements.
- Monitoring data security passwords and ensuring that they are kept in a secure location that doesn’t compromise their integrity

**Monitor, Audit and Logging Network Activity**
Whether you handle IT in-house or outsource to a cloud provider, you should ensure there is a central logging system in place that records events including:

- All login/logout events
- Inbound/outbound connections through Internet-facing firewalls
- Email and network traffic

Additionally, firms should look to perform a vulnerability assessment at least annually. It is essential that companies authenticate firewall configuration and anti-virus patching, network device security and evidence of criminal activity. You’ll want to know where vulnerabilities exist before implementing additional security measures.
Conducting a vulnerability assessment is especially important as the SEC’s cybersecurity questionnaire includes the following question: “Please indicate whether the Firm conducts periodic risk assessments to identify cybersecurity threats, vulnerabilities, and potential business consequences.”

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.
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.
Even if you’ve been successful at implementing all of the security measures and protocols above, there is no guarantee your firm will avoid becoming the victim of a cyber-attack.

With the threat of security incidents at all all-time high, staying proactive is the best way to thwart potential damage. That means preparing how to respond to an incident when it does occur is also necessary. Here is a step-by-step guide to follow in the event your firm suffers from a security breach.

1. Establish an Incident Response Team.
   Choose a select group of individuals to comprise your Incident Response Team (IRT). Assign each member a predefined role and set of responsibilities, which may in some cases, take precedence over normal duties. The IRT can be comprised of a variety of departments including Information Technology, Compliance and Human Resources.

2. Identify the type and extent of incident.
   Before your IRT can alleviate any incidents, it must clearly assess the damage to determine the appropriate response. For example, if the incident is a computer virus that can be quickly and efficiently detected and removed (and no internal or external parties will be affected), the proper response may be to document the incident and keep it on file. This task could effectively be handled by the IT department.

   If however, an incident occurs that affects multiple clients/investors/etc., the incident should be escalated to the IRT.

3. Escalate incidents as necessary.
   Certain departments may be notified of select incidents, including the IT team and/or the client service team. These parties should use their discretion in escalating incidents to the IRT. Any event suspected as a result of sabotage or a targeted attack should be immediately escalated.

4. Notify affected parties and outside organizations.
   One member of the IRT should be responsible for managing communication to affected parties. Depending on the severity of the incident, the IRT member will act as the liaison between the organization and law enforcement.

5. Gather evidence.
   When appropriate and necessary, the IRT is responsible for identifying and gathering both physical and electronic evidence as part of the investigation.

6. Mitigate risk and exposure.
   A technical member of the IRT should be responsible for monitoring the situation and ensuring any effects or damage created as a result of the incident are appropriately repaired and measures are taken to minimize future occurrences. The IRT will also need to define any necessary penalties as a result of the incident.
CONCLUSION

The world of cybersecurity continues to change on a daily basis, and there’s no telling where or when the next attack will strike. The best way to protect against an external attack or internal breach is to work with your internal security team or outsourced technology provider to structure and implement a sound security program to protect your firm’s data and information as well as offer peace of mind to your investors. As a final takeaway, following are four tips to remember as you go down the path of shoring up operations and security practices:

1. Establish and implement an Information Security Policy that outlines the layers of security you will put in place from technology and authentication protocols to restricting access and password requirements;

2. Create an Incident Response Plan so you are fully prepared should a security breach or cyberattack occur;

3. Train your employees on Information Security Awareness because a firm’s security strategy will only work if employees are properly trained on it; and

4. Conduct Due Diligence on your service providers so they do not expose you to unexpected risks.

FIVE HELPFUL SECURITY TIPS:

1. Patch applications such as Adobe PDF viewer, Adobe Flash Player, Microsoft Office and Java. Using the latest versions of these applications – and patching within two days – will help to prevent high-risk vulnerabilities. The same goes for your operating system.

2. Minimize the number of users with domain or local administrative privileges. Such users should use a separate unprivileged account for email and web browsing.

3. Employ application white-listing to help prevent malicious software and other unapproved programs from running. Examples are Microsoft Software Restriction Policies or AppLocker.

4. Use a host-based intrusion detection/prevention system to identify anomalous behavior, such as process injection, keystroke logging, driver loading and call hooking.

5. Provide user education regarding Internet threats and spear phishing socially engineered emails. Avoid using weak passwords, password re-use, exposing email addresses, and use of...
ABOUT EZE CASTLE INTEGRATION

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 175 firms with $1 billion or more in assets under management.

When it comes to cybersecurity, we help clients:

- Develop Written Information Security Plans and Policies
- Move their IT to our highly secure Eze Private Cloud environment
- Fortify their existing IT environment.

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.

To learn more about Eze Castle Integration, contact us at 800-752-1382 or visit www.eci.com.

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).
7. This data is based on the Commission’s fiscal year which ended Sept 30, 2015.

1. White House Executive Order -- Improving Critical Infrastructure Cybersecurity, February 2013