WHITE PAPER

# Prioritize Security Before the SEC Comes Knocking

## Executive Summary

Between audits by the U.S. Securities and Exchange Commission's Office of Compliance Inspections and Examinations (OCIE) and the increasing savviness of investors, being able to answer tough questions about cybersecurity has never been more important for hedge funds than it is today.

And the penalties for getting those questions wrong is probably only going to get higher — in December 2015, the head of the SEC's enforcement division said the agency plans to be more aggressive in going after investment advisors who fail to protect customer information. While audits can be painful, the fallout of losing the confidence of investors in the wake of a failed audit can be even more so.

In this paper we will explore what firms need to begin the process of organizing their response to cybersecurity audits well before the OCIE comes knocking at the door. Ultimately, that comes down to proper planning, documentation, and having a comprehensive understanding of the firm's cybersecurity posture and risk level.

## Planning for Success

### Establish a Cybersecurity Committee

Proper planning starts with having a group within the firm focused on developing and monitoring the organization's cybersecurity activities, policies, procedures. A cybersecurity steering committee should be established as a standing committee. At a minimum, this committee

> Cyberattacks on financial institutions have become both more frequent and more sophisticated. This is also true of cyberattacks on the infrastructure underlying the capital markets.
>
> — Luis Aguilar, SEC

### Who Should Read This White Paper

- CISO/CSO
- CIOs
- CFOs
- CEOs
- Directors of Security
- VP of IT

should meet quarterly, and consist not only of people from the IT team, but also the CEO and other C-level executives such as the COO and CFO. This not only ensures that the top decision-makers understand the organizations strengths and weaknesses in cybersecurity, but also helps ensure executive buy-in when it comes time to discuss the cybersecurity budget and where money needs to be spent.

The committee should be able to answer fundamental questions related to cybersecurity, such as: what are the organization's critical assets; does the organization have an up-to-date incident response plan; what vulnerabilities exist in the IT infrastructure and how much risk do they pose; and what controls are in place to monitor and manage third-party vendors.

Having answers to those questions — and documenting both the answers and the processes for acquiring them — is critical for the leadership of hedge funds ahead of audit so they can guide the development of security strategy and address any gaps in the protection of systems and data. The OCIE has made it clear there will be a particular emphasis on what firms are doing to protect client information. With this in mind, the steering committee should know the location of all business data — regardless of whether it is located on premise or in the cloud — and ensure that it is properly classified according to its criticality to the business and that the appropriate protections are applied to it. In addition, it should examine policies related to access to data and network resources — something that must be tightly controlled and accounted for, from establishing and enforcing user rights and managing the lifecycle of user credentials as employees are hired and fired.

It is also crucial for committee members to stay abreast of the cybersecurity trends, compliance issues, and cyber threats impacting the organization. While the industry is highly competitive and firms may be hesitant to publicly share information related to cybersecurity, the Financial Services Information Sharing and Analysis Center (FS-ISAC), which can serve as an important resource for firms of all sizes. IT security providers can also provide cyber threat intelligence and consulting services that can help refine its strategy to defend itself.

### Conduct a Risk Assessment

As noted above, a critical part of being ready for an audit is knowing where the firm stands in regards to cybersecurity risks. To do this, firms should undergo periodic cybersecurity risk assessments to test the effectiveness of their controls and pinpoint any vulnerable systems and data. This does not have to be done by the firm itself — there are a number of security firms that provide this kind of service. A security assessment can provide guidance on what specific risk factors to monitor over time to ensure actions can be taken if risks reach an unacceptable level.

The assessment should examine: the sensitivity, location, and classification of data; internal and external security threats; the existing security controls and processes in place; the fallout if systems were to be compromised; and the effectiveness of the governance framework. In addition to basic vulnerability scans of software and systems, assessments can also include penetration tests performed by third-party experts. Organizations should also make sure that whatever methods they use to test security controls are repeatable. Once the assessment is complete, the insight into the IT environment that has been gained can be used to guide a firm's security strategy going forward as well to identify any controls or policies that need to be updated or improved.

## Give the OCIE What It Wants

The most important subject of course to stay abreast of is exactly what it is the OCIE wants. Fortunately, the SEC has provided a list of priorities for organizations to use as a stepping stone. In January, the agency announced it will advance its efforts to examine the cybersecurity and compliance controls used by broker-dealers and investment advisers, particularly in regards to the testing and assessment of firms' implementation of procedures and controls. Going back to the 'National Exam Program Risk Alert' issued in September 2015, the OCIE cited governance and risk assessment; data loss prevention; access rights and controls; vendor management; training; and incident response as the critical areas it will focus on in its examinations.

## Governance and Risk Assessment

In the area of governance and risk assessment, the SEC stated that examiners would be looking at whether firms have cybersecurity governance and risk assessment processes for each of the other five areas mentioned above, as well as whether firms effectively evaluate risks and whether their controls and risk assessment processes are tailored to their businesses. In addition, the examination may also focus on the level of communication to and involvement of senior management and boards of directors in cybersecurity. Meeting the requirements of that part of the exam means having a formalized process for regularly reporting cybersecurity information to the board of directors, and firms would be wise to ensure these reports include key metrics and information about any actions related to policy changes or governance. In addition, the OCIE may require board minutes or reports related to cybersecurity and information regarding lines of responsibility in the organization related to the handling of cybersecurity planning and response, and organizations should be ready to supply those.

## Protecting Data

With the SEC's stated emphasis on protecting data, data loss prevention is especially critical. Well before an audit, a firm should inventory its data and make sure it is classified with respect to its business value and what the impact to the business would be if the data were to be leaked. The OCIE will assess whether a firm is able to monitor data flowing to external sources. To address this, hedge funds should deploy data loss prevention technology that can monitor the movement of data and apply protections based on the data's classification.

Part of any data protection strategy is the assigning of access privileges. Due to the sensitive nature of the information, multi-factored authentication should be a standard best practice for the industry. A multi-factor authentication approach uses two or more independent credentials to authenticate a user: something the user knows (such as a password), something the user has (e.g. a security token), and something the user is (e.g. biometric verification). A firm's access control policies should take into account the various roles and job responsibilities of the users. Organizations should also segment their networks to ensure sensitive systems and data are not exposed to vendors and employees that should not be granted access.

As always, information related to access controls should be well documented. This includes evidence of policies and procedures addressing topics such as updating or terminating access rights due to personnel changes, the tracking of access rights, and the process of getting management approval for any changes in privileges.

## Vendor Management

Just as the front door is not the only way to break into a building, a direct attack is not the only way to compromise security at a hedge fund. Third-party vendors are also attractive targets for hackers as well. According to the OCIE, examiners may want to analyze how firm's monitor and oversee vendors, their approach to contract terms, and whether they exercise due diligence in their choice of partners. In preparation for an audit — and in the name of understanding their true risk — firms should closely review how they handle the vendor management process. Specifically, the OCIE notes in its Risk Alert that examiners may be interested in contractual terms related to third-party vendors that access a firm's networks or data, as well as sample documents or notices required of vendors in the event of significant changes to the vendors' systems or services that may have a security impact on a firm's data.

Remember that not all vendors have the same risk profile, so the approach should be tailored to the individual risk level of the vendor, which could be influenced by facts such as the country the vendor is located in and the level of access the vendor has to a firm's systems and network.

## Training

Training employees to spot cyber threats and policy violations can serve as a force multiplier when it comes to protecting a company. After a firm has established a cybersecurity policy, it is critical for employees and others who access its network to be trained not only on the policy itself, but the identification of cyber threats such as suspicious emails and social engineering. Firms should be ready to provide examiners with the details of their training program, how it works, and any metrics that demonstrate its effectiveness.

## Incident Response

Being unprepared for the aftermath of a cyber attack can cost a firm time, money, and investor confidence. Having a Computer Incident Response Plan is critical, and is almost certainly something the OCIE will want to have a close look at. Ideally, the plan should be periodically tested and refined, and the results of the test should be documented. Among other things, an incident response plan should:

- Create a Computer Incident Response Team and outline the chain of command in the event of a breach and clearly delineate responsibilities
- Provide plans and procedures for monitoring systems and logs, conducting incident investigations, and prioritizing security events
- Establish policies around the containment and eradication of the threat
- Establish policies for the recovery of the business
- Create a plan for contacting and notifying any affected customers, media, law enforcement, security service providers or other relevant parties

# Conclusion — Get Ready

## Implement Best Practices

Just like for other types of businesses, the name of the game is defense in depth. That means not only implementing the type of 24x7 security monitoring and incident response capabilities that auditors will demand, but doing it in combination with practices such as multi-factor authentication and smart physical security. From network firewalls to intrusion detection/prevention systems, the approach to security for hedge funds has to be multi-layered. That includes having access policies built upon the principle of least privilege to ensure employees have the minimum amount of access they need to do their jobs as well as endpoint monitoring that can detect both malware as well as malicious activity by stealthy attackers.

While the prospect of an audit can be daunting, firms are not alone. There are a number of security firms that are able to provide both consulting and technology that can help firms meet their cybersecurity needs. By developing a cybersecurity steering committee, firms can make sure the cybersecurity challenges facing the organization reach its top decision-makers as those leaders develop a strategy to protect their network, systems, and information. As a reminder, a cybersecurity risk assessment will provide information about any weak points that could expose firms to attackers and auditors alike. Taking these steps and following the guidance from the OCIE about what its examiners are looking for could be the difference between a pat on the back and a potential penalty from the SEC.

For more information, call **(877) 838-7947** to speak to a SecureWorks security specialist.

**www.secureworks.com**