HEDGE FUND
legal & compliance digest

www.hedgefundlcd.com

Best Practices for Hedge Fund Managers Conducting Cybersecurity Due Diligence on Their Service Providers (Part One of Two)

"Every organization is a target," a phrase which had little to no meaning just 20 years ago, is now a familiar adage warning organizations to build and evolve their cybersecurity defenses in the face of ever-present, external cyber threats. And most have. Only recently, however, have businesses realized that they are also vulnerable to a form of "friendly fire," threats posed by third-party vendors whose inadequate or lax cybersecurity controls can be exploited to gain access to their clients' systems and networks. One survey on third-party risk management published last year estimated that 63% of cybersecurity breaches over the last few years were traceable to third-party vendors. The exposure is staggering, particularly for hedge fund managers, which rely on a web of third-party service providers—independent administrators, prime brokers and law firms, among others—to conduct their day-to-day business activities and that may have access to sensitive information, including portfolio holdings, and employee, firm and client financial data. As such, this newest horizon of cybersecurity defense requires that managers conduct due diligence on their third-party vendors in order to cultivate a deep understanding of their cybersecurity capabilities and to protect the firm's devices, data and networks.

This article, the first in a two-part series, reviews the most important reasons hedge fund managers should conduct cyber due diligence on third-party service providers, regulatory requirements related to third-party due diligence and the service providers whose protocols it's most critical for hedge fund managers to assess. The second article will address how hedge fund managers can effectively identify and assess the risks third parties pose to their systems and networks, what protections managers can put in place to protect themselves and ongoing due diligence procedures.

Importance of Conducting Due Diligence on Service Providers

Vendors have been a particular vulnerability point for hedge fund managers, noted Joseph Facciponti, special counsel at Cadwalader, Wickersham & Taft, "Third parties have traditionally been a blind spot for cybersecurity risks to businesses. But over the years, there have been a number of wakeup calls, so firms are paying more attention to third parties now. With the potential risks in mind, effectively managing cybersecurity risks from third parties has become imperative for firms and is something they are expected to do."

Interestingly, investors have contributed to highlighting the importance and advancing the development of third-party cybersecurity due diligence. As the nature of cyber threats to hedge funds' systems has evolved, so too has investors' understanding of those risks. Sophisticated and tech-savvy investors today often insist that hedge fund managers have treated diligence on service providers with the same seriousness that the investor employed during due diligence on the hedge fund.

"There is a great deal of investor focus on cybersecurity," said Richard Maloy, managing principal in the Asset Management Practice at Integro Insurance Brokers. "They want to see that the managers are taking the appropriate steps to protect themselves, which includes having cyber insurance in place to protect the firm if a breach occurs, either within the firm or at a vendor, and they want to see the manager has conducted thorough due diligence on the service providers to make sure they aren't being exposed to more cyber risks."

Conducting cyber due diligence on third parties is practically and legally important as well, noted Aaron Schlaphoff, a partner at Kirkland & Ellis. "Cyber due diligence is important because hedge fund managers rely intensely on third-party service providers. To conduct their business activities, they use administrators, custodians, prime brokers, data and research providers, and law firms. All of those are people who have access to sensitive data for the hedge fund manager and are essential to the manager's ability to operate its business."

"In some cases," he continued, "Those service providers will have information that is subject to regulation. For example, under Reg S-P and Reg SID, there are obligations that a hedge fund manager has to protect the information of its clients, and that information may be held by the administrator or another third party. To the extent the hedge fund manager does not take reasonable steps to implement policies and procedures to protect that information, it could face regulatory liability. So, they really need to be focusing on what vendors are doing with the information and what they do to protect the information."

"A manager should protect its business and its proprietary information, advised Cadwalader, Wickersham & Taft partner Dorothy Mehta, and summarized the reasons why. "With a registered investment adviser there are also regulatory concerns and pressure from the [Securities and Exchange Commission] and [National Futures Association] to have appropriate policies and to conduct proper cybersecurity due diligence on the service providers. There's pressure from investors, who are worried about their information being leaked out to the world. Conducting proper cybersecurity due diligence on service providers is important to managers because that's where most of their information lies."

Regulatory Requirements Related to Cybersecurity

Both federal and state investment industry regulators have issued guidance governing cyber due diligence on third parties, though in certain cases guidelines are not as specific as those that apply to hedge funds' internal practices. Where gaps exist, sources recommended that hedge funds extend to third-party vendors the regulatory requirements that apply to their own cybersecurity protocols.

"The Commission has become increasingly focused on cybersecurity over the past several years, with particular attention on the use of third-party vendors," said Schlaphoff. "I think initially it was difficult for the industry to figure out what the SEC's expectations were, and it was difficult for fund managers to get the vendors to agree to work with them on due diligence and cybersecurity. We've seen a shift over time, such that vendors generally are more willing to work with managers now on these issues so that managers can meet SEC expectations and regulatory obligations."

"The SEC hasn't been very specific about what they expect from managers regarding due diligence on third-party vendors, but I do think that best practices and standards are starting to emerge," he continued. "The SEC has indicated that a hedge fund manager has responsibility for the activities of its vendors with respect to cybersecurity. While there hasn't been a lot of specific guidance from the SEC on vendors, it has produced a fair amount of guidance for asset managers on what they should be doing generally with respect to their own internal cybersecurity—things like governance and oversight, and physical protections. A lot of what the SEC has said managers should be doing internally can be applied to the service providers as well."

In fact, in some regard, certain of the SEC's rules for firms' internal cybersecurity, when read strictly, should extend to third-party practices. Additionally, hedge fund managers themselves are required to protect sensitive information from cyber attacks under Regulation S-P, known as the "Safeguards Rule," which requires registered broker-dealers, investment companies and investment advisers to adopt policies and procedures to prevent unauthorized access or use of customer data that could result in substantial harm or inconvenience to a customer. Compliance with the rule may obligate hedge fund managers to ensure that client financial and sensitive information is protected from unauthorized access or use—a cyber attack—on third parties' systems as well.

Some specific guidance on third-party cyber due diligence does exist, however. The SEC's Division of Investment Management guidance on cybersecurity states, "Because funds and advisers rely on a number of service providers in carrying out their operations, funds and advisers may also wish to consider assessing

whether protective cybersecurity measures are in place at relevant service providers. For example, service providers may be given limited access to a fund's technology systems that may inadvertently enable unauthorized access to data held by the fund. Funds, as well as advisers, may wish to consider reviewing their contracts with their service providers to determine whether they sufficiently address technology issues and related responsibilities in the case of a cyber attack. Funds and advisers may also wish to consider assessing whether any insurance coverage related to cybersecurity risk is necessary or appropriate."

Fund managers may also have to comply with various state cybersecurity regulations, and managers can, and potentially should, subject their service providers to the same requirements. According to Kenneth Citarella, senior managing director for the investigations and cyber forensics practice at Guidepost Solutions, "If the hedge fund operates in New York state, they are probably bound by the new cybersecurity regulations from the Department of Financial Services. Even if they are not, that regulation is setting the bar for what is acceptable and what is deemed best practices going forward. That regulation requires the regulated entity to ensure the cybersecurity of their third-party vendors."

NY Department of Financial Services Regulation 23 NYCRR 500 requires banks, insurers and other financial services firms to meet minimum cybersecurity requirements "to protect consumers and ensure that its systems are sufficiently constructed to prevent cyberattacks to the fullest extent possible." Under the rule, firms required to comply must formally designate a chief information security officer who can "maintain a cyber security program" that can "protect the confidentiality, integrity and availability" of the data through appropriate governance structures and policy frameworks. The program must have detection and response capabilities and, among other controls, it also instructs firms to analyze security at third-party vendors.

Service Providers in a Manager's Cyber Nexus

The service providers that have the most access to a manager's networks, and therefore present a high degree of cyber incident risk, include administrators, prime brokers, custodians, technology providers and law firms.

Law firms, in particular, increasingly are facing more scrutiny of their cybersecurity practices. The Association for Corporate Counsel recently released model best practices for law firms' protocols that recommend that outside counsel "shall have in place appropriate organizational and technical measures to protect Company Confidential Information or other information of a similar nature against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and nature of the information to be protected. Outside Counsel shall have in place internal security and privacy policies designed to protect the security, confidentiality, and integrity of Company Confidential Information or other information of a similar nature that include: security policy; organization of information security; asset management; human resources security; physical and environment security; communications and operations management; access control; information systems acquisition, development, and maintenance; information security incident management; business continuity management; personnel training; and compliance."

The report also suggests that law firms should have incident response plans "that allow for the reasonable investigation, response, mitigation and notification of events that implicate the confidentiality, integrity and availability of Outside Counsel's technology and information assets, or events that cause the unauthorized or unintentional disclosure of Company Confidential Information."

Mehta said that law firms present a clear area of cyber risk. "They have sensitive information, such as financial information and investor information. Lawyers have access to subscription documents, particularly for PE firms. If one of those service providers is tapped, then all of that information can be out there."

In response to the threat, clients are more frequently conducting some form of cyber due diligence on law firms, said Schlaphoff, and he expects hedge fund managers to follow this trend. "Our client base in general is more often asking about what steps we take as a firm with respect to cybersecurity and data protection. I wouldn't say hedge fund managers are focused more on this than other clients, and we still do not see most managers focusing on it.

However, I do expect it to become more common."

Martin Sklar, a partner at Kleinberg, Kaplan, Wolff & Cohen, agreed that law firms have access to and house some of a manager's most important and sensitive information. "Lawyers and auditors are really episodic in what they do. Law firms tend to know the most sensitive information about a manager. The law firm is privy to investigations, merger discussions and client issues. But, lawyers are heavily regulated as to how they handle this sensitive information. Cybersecurity is a relatively new concern and should be addressed. For the manager to mitigate risks, they could inspect the premises and see how things are secured and/or they could get representations from the law firm."

Administrators also pose a significant cyber risk, said Sklar. "The nuts and bolts of the hedge fund service providers is really the administrator. Managers are concerned about their systems and cybersecurity and disaster recovery." The lawsuit filed by Tillage Commodities Fund late last year against its fund administrator, SS&C Technologies, the parent of global financial services software provider, SS&C GlobeOp, provides an example of the potential risk administrators pose. Among other things, Tillage alleged that SS&C authorized the transfer of nearly $6 million from a client's commodities fund to Chinese hackers without adequate checks in place to ensure the request was legitimate.

Mehta agreed the administrator presents a significant area of risk for hedge fund managers. "The key service provider a manager needs to look at is the administrator. They have subscription agreements, they have the NAV calculations and any interim financial reporting. It's super important for hedge fund managers to make sure they have the proper security measures in place and have done proper testing of systems, and they keep on top of that."

Managers should conduct cybersecurity due diligence on other service providers as well, said Mehta. "The other service providers that are important to a manager are the prime broker, or the FCM. Those are where the positions are, so it's important those entities have proper controls around the hedge fund's information."

Sklar added, "With respect to your prime broker, you want to speak to the IT department and see how well protected their systems are. Get representations that they will have cybersecurity protections in place, that they will report breaches and remedy breaches, and that they will handle personal and sensitive data with the utmost care."

HEDGE FUND
legal & compliance digest

www.hedgefundlcd.com

Best Practices for Hedge Fund Managers Conducting Cybersecurity Due Diligence on Their Service Providers (Part Two of Two)

Just last week, "a global hacking assault" that reportedly "crippled computer systems around the world" hit major companies, government agencies, hospitals and universities in over 150 countries in what to date has been the world's largest cyberattack. Analysts have just started to assess the damage—a process that likely will continue for months to come—but what is known already is that hackers remotely spread the ransomware by taking advantage of a Windows vulnerability that could have been cured if the entities and individuals attacked had updated their computers and networks with a security patch Microsoft released in March. It's not clear yet whether and which hedge fund managers directly were affected by the attack, but it's hard to imagine that none were at least indirectly exposed, since managers rely on a web of third-party service providers—independent administrators, prime brokers and law firms, among others—to conduct their day-to-day business activities and that house managers' sensitive information, such as portfolio holdings, and employee, firm and client financial data, on their systems. The attack highlights the point that now, more than ever, it's imperative that hedge fund managers conduct thorough due diligence on their third-party vendors in order to cultivate a deep understanding of their cybersecurity capabilities and vulnerabilities, and to protect the firm's devices, data and networks.

This article, the second in a two-part series, addresses due diligence practices to effectively identify and assess the risks third parties pose to systems and networks, protections managers can put in place to mitigate those risks and ongoing due diligence procedures. The first article in this series reviewed the most important reasons hedge fund managers should conduct cyber due diligence on third-party service providers, regulatory requirements related to third-party due diligence and the service providers whose protocols it's most critical for hedge fund managers to assess.

Due Diligence

Compiling a Profile of a Vendor's Cyberattack History and Fluency in Hedge Fund Business

Although the specific cybersecurity threat posed by each vendor will vary—common threats range from failures to adequately integrate multiple data sources to employees that inadvertently authorize access to phishing and malware attacks to aging infrastructure, among others—the due diligence that hedge managers should conduct on service providers generally entails the same comprehensive review, designed to root out specific potential threats, across all vendors. For instance, managers should always review whether and how often the vendor has experienced cybersecurity incidents in the past, the severity of those incidents and the quality of the vendor's response. Managers should also review whether the vendor maintains cybersecurity policies—the compliance and IT personnel who wrote the manager's policies and procedures should review the vendor's for adequacy—and has sufficiently trained personnel to protect data and respond to incidents. Best practices also dictate that managers review the service provider's access controls to ensure they uniquely identify users and monitor attempts to access restricted data.

Darren Huber, controller and head of ERM at Fintan Partners, said managers have a fiduciary obligation to review the cybersecurity practices of their service providers. "You can't outsource you fiduciary responsibility, so you need to understand the oversight that goes on at your

various service providers. Cybersecurity is a huge concern, so you want to go through a service provider's full program to see if they are following IOSCO and FSB standards and industry guidance relating to cybersecurity. You want them to walk you through their program."

According to Cadwalader, Wickersham & Taft partner Dorothy Mehta, finding out what cybersecurity policies and procedures vendors have in place is "the first level of diligence. That can be done by an RFP or DDQ to that service provider. You want to ask about any breaches, the nature of those breaches and how those breaches were addressed and rectified."

Huber added, "The core cyber oversight for each service provider is the same, and what you're looking for is where there is potential for attacks or other issues and how the firm can address any problems. "

Martin Sklar, a partner at Kleinberg, Kaplan, Wolff & Cohen, advised that hedge fund managers compile a broad profile of a vendor's overall business and prior experience. "Generally, you want to look at their experience and their ability to handle the instruments you're trading and your fund's strategy. You want to look at geography, and where they are doing business and if they are operating in countries that you trust."

Richard Maloy, managing principal in the Asset Management Practice at Integro Insurance Brokers, agreed that managers should measure service providers' understanding of hedge funds' business. "You want to know how well the service provider understands the hedge fund's business and how well they understand the particular cyber risks the fund faces, especially as a result of the relationship with that vendor."

Specific Due Diligence Topics

Once managers have compiled a profile of the vendor's business, prior cyber attack history and competency in hedge fund trading and strategy, they should assess the existence and strength of specific security measures the vendor has in place. Huber explained, "I want them to go through the different threat scenarios to see what security measures they have in place. I want to see network and email security, and if there is an enabled enterprise security control that prevents and detects unauthorized network activity. I want to see end-point security to see their standards and capabilities. I want to see data and cloud protection to make sure these services are as protected with a service provider as they would be within the firm. You want to see that there are vulnerability assessments and training that's being done periodically on different threats you face, the latest techniques, policies and procedures."

He added, "You want to see security event and incident management logs on threats, incidents that were inbound that they identified and outbound as far as protections against these threats."

Aaron Schlaphoff, a partner at Kirkland & Ellis, listed other specific cybersecurity measures hedge fund managers should verify vendors have in place. "You want to know if they inspect activity on their systems to see who has logged in to various aspects of the system and who is using the data. Do they have the ability to determine whether files have been manipulated? Do they have monitoring and control over devices? Do they have measures in place to prevent data from leaving the firm without proper authorization? Do they have their own backup and recovery systems?"

How service providers control who has access to their system and information, and the hedge fund manager's system and information is particularly important to determine, said Kenneth Citarella, senior managing director for the investigations and cyber forensics practice at Guidepost Solutions. "How do you know that only the people that need access to it can access it? How are they monitoring that? How are employees accessing data? Is it always going to be through a corporate-issued device? Is the device controlled by a username and password? Is the data only stored on the company's network or cloud? Unless you ask all of these questions, you can't determine where the risks are."

Schlaphoff observed that vendors often engage their own outside providers to perform services, and hedge fund managers should probe the cybersecurity policies and procedures the vendor has in place to protect against threats from its third-party service providers. "I would look at whether the vendor uses vendors. I think people are surprised to learn that their vendors may be using their own service providers who have access to data relating to the hedge fund manager or its clients. Then

you need to talk to the vendor about their own processes for overseeing cybersecurity at their own service providers."

Citarella agreed and explained further, "You want to know what their cybersecurity practices are and the contractual relationship as it addresses cybersecurity between your vendor and their vendor," Citarella advised. "You may be exposed to unforeseen risks if you don't look at these relationships and how they can affect you. Managers need to discuss with the vendor how they look at their cybersecurity and what they look at. They should also ask to see any reports on breaches or testing that was done. The manager must take the proper steps to ensure the safety of their data even when it moves down the line to another third-party vendor."

Huber underscored the premium investors place on knowing managers are conducting fulsome cybersecurity due diligence on their third-party service providers. "When I look at a manager, I want to know what they're looking at on a daily, weekly and monthly basis to prevent any issues with their service providers and if they are getting reports about attempted or actual attacks, where they came from and how the issue was handled. I think firms should be looking at all things cyber, from when their internet goes down to hacking attempts or actual hacks, to really understand what the issue was and how it can be prevented. As they're looking at these issues within their own firms, they should be getting periodic reports from their key service providers to understand what's happening with cyber on their ends."

At bottom, hedge fund managers must treat their vendors—whether they're law firms, HR companies or administrators—and other third parties' computer systems and cybersecurity programs as if they're part of their own system, advised Citarella. "The same rules must apply. The hedge fund manager's obligation, at a minimum threshold, is to have that conversation with the service provider to make sure the appropriate protections are in place."

Identifying and Mitigating Service Provider Red Flags

After obtaining information related to the specific cybersecurity measures vendors have in place, the risk the vendor could pose to a manager should be rated. Performing a risk assessment is a key aspect of conducting proper cybersecurity due diligence on a service provider. The objective of the risk assessment is to determine which of the vendor's practices (or lack thereof) present a red flag and what protections should be put in place.

The most important red flag, Schlaphoff said, is a vendor's inability to give clear answers to any of the due diligence questions asked by the manager. "I would expect a reputable vendor to have gone through the process of answering due diligence questions from hedge fund managers before and to be cooperative and help the manager understand the vendor's practices. Vendors should understand why this is necessary, and if you're dealing with a vendor that doesn't appreciate that and is unwilling to provide information, then that is a definite red flag."

Huber concurred that vendor's should always know the answers to due diligence questions hedge fund managers ask. "A red flag for me is when I ask them about where a server is located, and they can't tell me, or can't tell how many attempts there were to hack the system over a period of time or what kind of attacks they were."

Once red flags and cyber risks have been identified, they must be mitigated if a manager intends to engage a vendor. Mitigation best practices generally are similar across vendors, irrespective of the red flag posed.

Unexpectedly, the first step in mitigating vendor risk starts within the hedge fund manager, Huber said. "The key is you need to start at the top. You need to make it clear from senior management that as a fiduciary you have extreme responsibility to protect firm and client information. Then you need to make sure you have the proper systems in place to do this."

Joseph Facciponti, special counsel at Cadwalader, Wickersham & Taft, pointed out the importance of risk mitigation across all vendors a manager engages. "Your own cybersecurity program is only as strong as your weakest link. If you're sharing sensitive data with a number of different service providers, you want to make sure you apply the same standards to all of them to make sure each of them is doing their job to protect their data."

Citarella agreed that firms need to instill their own cybersecurity awareness ethic into all of their vendors. "You have to create a culture of

cybersecurity awareness from the board of directors down, and you have to spread that awareness to all of your vendors."

At the vendor level, Huber advised an initial high-level mitigation assessment. "You want to require that your third-party service providers that have access to client information are following the same level of security policies and standards and regulatory obligations. If they can't do that, then you need to evaluate whether you can continue or even execute that relationship."

According to Facciponti, "The things you want to do to manage third-party risk are similar to the things you want to do for your own business. You want to understand what data you're sharing with the third party or what access you're giving them to your systems. You want to understand the policies, procedures and controls they have in place for protecting your data. You want to have contractual assurances in whatever engagement agreement you have with them that they're going to adopt these policies and procedures, and that they're going to provide you with notice if there is a data breach. You want to reserve the right to audit them. You want to know that generally they are taking cybersecurity seriously."

Schlaphoff added that negotiating specifics terms and notifications into the vendor contract can be helpful as well. "In order to protect yourself, your contracts with your service providers can include specifications as to the types of data they will retain and what they can and cannot do with it; specifications about how they will protect that data; specifications that if the contract is terminated, they will delete the data or return it. You want notification of breaches. If possible, you even want to know about breaches that didn't directly affect your data but affected other clients, because that speaks to the vendor's overall cybersecurity framework and infrastructure. You also want your contracts to include allocation of liability, appropriate indemnification provisions and agreements to cooperate in the event of a cybersecurity breach."

Getting the appropriate protections from vendors is an important part of risk mitigation, Sklar said. "From the cybersecurity angle, it really comes down to receiving representations from the administrator as to their policies, particularly how they will respond to a security breach, and their architecture. Where there are security breaches, the manager wants representations that those will be reported. These provisions would go into the agreement with the vendor."

He added, "The representations you get from your various service providers should contain a provision that the cybersecurity protections continue. Managers may also ask for annual certifications that the cybersecurity program is being maintained and, where needed, strengthened, and that there haven't been any security breaches."

Cyber insurance is another method of protection. Maloy said managers should not only have their own insurance but review the policy of the vendor, if it has one, to see what is covered and how the firm will be either protected or redressed in the event of an attack at the service provider. "You need to know what is covered and what is not, so you know how your own insurance should be structured. There isn't a lot of variation and negotiation in the terms of the policies, but what you want to be sure of is that the vendor will be responsible for breaches that occur on their end."

Citarella agreed managers should look to see if the vendor has cybersecurity insurance. "You want to know that you're covered from data loss and other breaches. In order to protect yourself, you need to have in the contract with your vendor cyber insurance and incident cooperation spelled out."

Post-Contract Due Diligence and Cyber Risk Abatement

After managers have conducted due diligence, decided to hire a service provider and negotiated contractual protections, they should take steps to ensure that vendors have adequate cyber protections in place throughout the engagement, which includes conducting follow-up due diligence on service providers.

Citarella said the level of follow-up due diligence depends on the manager's comfort level with the service provider. "I would also look at the regulations that are governing you and your cybersecurity and apply the periodicity of that testing to your vendors."

Annual follow-up due diligence is a good idea, agreed Schlaphoff. "If you have a lot of vendors, you may want to do a risk analysis to decide whether some vendors should be reviewed

more frequently than others. If there were weaknesses with a particular vendor that concerned you, you may want to follow up with them more often. The follow-up due diligence could be a full reassessment or a targeted reassessment based on particular areas of concern."

Exactly how often and how thoroughly a manager reviews a particular service provider will depend on that service provider's cyber threat level. According to Huber, "For every service provider, you should have a grade and a review date. You want to look that they are meeting their SLAs and their protections are reasonable. You want to make sure the contract has enough flexibility to be able to adapt to the changing requirements as needed. If you have a hard-coded agreement on what programs are required, and things change, then you have a gap in your program and responsibilities."

When reassessing a service provider, Huber advised, "You need to have a plan that is risk-based and comprehensive. You need to determine which risks are highest to your firm. It has to be an evolving process, because even when you think you're ahead of the game, you're probably way behind, because the threats are constantly evolving. Your service providers need to be partners in this defense. You need to keep them up to date on how your business has changed, how regulations have changed and how your protections need to change to make sure their policies and procedures can change to complement yours."

Facciponti added, "You need to make a risk-based decision about how often you should go back to them for follow-on due diligence. As a practical matter, the landscape is constantly changing, so you're going to want to be in regular contact with your vendors to make sure they're reacting to the latest developments and following best practices."