Hedge Fund Law Report
An Acuris company

Cybersecurity

How Recent Data Breaches Have Affected the Cyber Insurance Market for Fund Managers

Aug. 3, 2017

By Michael Washburn, *Hedge Fund Law Report*

As cyber thieves, malware agents and other bad actors become increasingly savvy and data breaches – as exemplified by recent high-profile cases involving Target and WannaCry – continue to multiply, the need for sophisticated technology capable of safeguarding firm and client information grows ever more acute. It is shortsighted, however, to imagine that a strong internal information technology (IT) system alone is a sufficient defense. If a cyber breach occurs, the potential ramifications for a firm are almost incalculable, including possible litigation from clients who feel that their sensitive information has not been properly protected, as well as possible enforcement action by regulators that are paying increasing attention to cybersecurity issues. A cyber insurance policy may be a firm's last line of defense.

The insurance industry has responded to the current climate, providing myriad options to corporate clients and offering plans that focus on minimizing operational and reputational damage. In the last few years, companies in the financial sector, and investment managers specifically, have devoted resources to identifying vulnerabilities from a cyber perspective and adopting safeguards to address these risks, with more of them purchasing cyber insurance than ever before.

To help readers understand these issues and determine which cyber insurance options might be best for them, the Hedge Fund Law Report interviewed Graig Vicidomino, associate director of Crystal & Company. This article sets forth Vicidomino's thoughts on trends in the market for cyber insurance for fund managers, including with respect to costs, scope of coverage and benefits of these policies.

For more on cybersecurity, see "Surveys Show Cyber Risk Remains High for Investment Advisers and Other Financial Services Firms Despite Preventative Measures" (Jul. 20, 2017); and "Navigating the Intersection of ERISA Fiduciary Duties and Cybersecurity Data Breach Protections" (Jun. 29, 2017).

HFLR: Has interest in cybersecurity insurance for financial sector firms picked up recently? If so, what factors are driving this trend?

Vicidomino: Cyber insurance has been a hot topic for the past two to three years. Interest in these policies increased significantly following the data breach in 2013 by the retailer Target. This incident, in particular, caused asset management firms to take notice of the real risks associated with a cyber attack.

Each time the SEC's Office of Compliance Inspections and Examinations (OCIE) issues a risk alert on cybersecurity – the most recent one being in the wake of the WannaCry ransomware attack –

current and prospective clients and buyers reach out to us to discuss cyber insurance. The uptick in interest suggests that the financial industry understands the significant repercussions that can stem from a cyber attack. Our clients want to ensure that they are abiding by not only the measures articulated in these alerts, but also by the spirit of the principles and guidance set forth by the SEC and OCIE.

[See "SEC Guidance Update Suggests a Three-Step Framework for Investment Manager Cybersecurity Programs" (May 7, 2015); "SEC Chair White Identifies the SEC's Top Concerns Arising Out of 2014 Examinations of Private Fund Managers and Alternative Mutual Funds" (Mar. 27, 2015); and "Cybersecurity for Hedge Fund Managers: Compliance Best Practices, SEC Examinations and Cyber-Liability Insurance" (Jun. 27, 2014).]

In 2015, the SEC asked advisers through an Investment Management Guidance Update to consider whether insurance coverage that specifically covers losses and expenses attributable to cybersecurity is necessary or appropriate. Per the SEC rules, advisers are not required to maintain this coverage. A lot of our clients, however, see significant value in these policies once they understand the extent of coverage that is offered. This is particularly true for our clients that do not employ an in-house technology officer, who would typically be the person responsible for overseeing the implementation of an incident response plan and ensuring that the firm returns to working order as soon as possible.

[See "ALM General Counsel Summit Highlights Key Elements of a Robust Cybersecurity Compliance Program" (Dec. 17, 2015).]

HFLR: On average, how much do cyber insurance policies cost?

Vicidomino: From a cost-benefit ratio, these policies continue to be competitively priced. For example, for most hedge funds, on average it costs approximately $5,000 to $10,000 per million dollars of coverage, with the deductible on those policies typically ranging from $5,000 to $25,000 for small to middle-market firms.

Based on the estimates above, an adviser could have to pay $30,000 out of pocket to cover the premiums and deductible. In the event of a breach, that adviser will have access to a million dollars of coverage to cover fines and penalties assessed by regulators; claims brought by clients; and expenses associated with restoring the firm to working order, notifying customers and managing the adviser's image to prevent the firm from losing clients.

One might expect prices on these policies to have increased dramatically or coverage to have shrunk over the past few years as more cyberattacks have been featured in the news and there has been an ongoing focus about how financial institutions – asset managers in particular – are the targets of these attacks. We have seen the opposite, however. Pricing has remained competitive, and the coverage terms are becoming broader.

HFLR: How much on average do clients purchase in cyber insurance?

Vicidomino: It is fair to say most small- to middle-market firms purchase up to $5 million in coverage. Larger firms typically purchase closer to $10 million or more.

HFLR: What sort of expenses do cyber insurance policies cover?

Vicidomino: Depending upon the specific policy, cyber insurance can cover the insured against fines and penalties levied by regulators, as well as potential claims from their clients and employees if their personally identifiable information is breached. The other crucial benefit that many policies offer is the coverage of a broad scope of the adviser's expenses that result from a breach, such as system restoration costs, forensic investigations to determine what happened and the payment of extortion costs.

Another aspect of coverage that is available is the costs associated with hiring a public relations (PR) firm to assist with communications to clients or the public. PR firms are helpful in ensuring that, after a breach, the adviser appropriately conveys that it is managing the breach and taking the steps necessary to contain the situation.

[See "Cyber Insurance Providers May Play a Key Role in Assisting Hedge Fund Managers Mitigate Cyber Incidents" (May 26, 2016).]

HFLR: When you refer to extortion payments, are you talking about ransomware and malware attacks, where companies have to pay money to get back their data?

Vicidomino: That is correct. When an entity is the target of one of these attacks, it typically receives a message on its screen instructing it to wire money to an offshore account, after which the hackers will release the target's system. If that entity has cyber insurance, it can call its insurer to gain access to service providers, along with the broker, to help them through this process.

That is exactly what that coverage is there for. The extortion coverage under the policy is offered so if the insurance company deems that paying that ransom is going to mitigate the loss, then that is a covered cost under the policy.

HFLR: Does it make more sense to invest in an insurance policy for that kind of event, as opposed to developing the IT infrastructure to prevent such an event? Conversely, does a manager really need both – a two-pronged approach?

Vicidomino: We really view cyber insurance as a necessity, but we do not want our clients to view it as a replacement for continuing to invest in the company's infrastructure and in employees who really focus on these matters.

Financial services firms are best served by being prepared and having the right systems and people in place. Even with all of that preparation, however, experts in the cyber industry believe that a cyber breach is inevitable for most firms. Advisers that have cyber insurance coverage should take comfort in knowing that they have a partner to cover what can be very large expenses.

[See "Cyber Insurance Coverage, Pre-Breach Mitigation Efforts and Post-Breach Response Plans Can Reduce Harm to Fund Managers From Cyber Attacks" (Jan. 19, 2017).]

HFLR: Do you see the potential for fraud and abuse of these policies?

Vicidomino: Fraud can occur, but there are checks and balances built into the process to minimize the potential for this type of abuse. For example, the insurance policy will stipulate that the insured receive pre-approval from the insurer before making any payments in connection with a breach. Also, when a client reports a ransomware attack and asks the insurer to make the extortion payment, the insurance company is going to conduct an investigation to make sure that the attack and ransom request are real. As a result, while fraud is always a possibility, it would be very difficult to push that through with the insurance company, provided that the insurer conducts proper due diligence prior to making the payment.

Presently, fraud is not one of the fears of the insurance companies. If it were a material risk, insurers would likely add specific provisions into the policies to protect themselves from the filing of fraudulent claims. In fact, I have seen similar exclusions in E&O and D&O insurance policies, which state that if an insured proffers a false claim, the insurance company can void the policy and essentially eliminate the insurance. Interestingly, I have not seen these sorts of exclusions under the more modern-day cyber policies.

To be clear, fraud exclusions are included in cyber policies, but they typically encompass circumstances where the insured commits fraud in the course of its business activity, as opposed to the filing of fraudulent claims.

HFLR: How do cyber insurance policies mitigate reputational damage? How does this work in practice?

Vicidomino: One aspect of coverage under these policies is crisis management or PR management. The biggest fear of most of our clients is that if a breach occurs, they will lose clients. If an adviser has to issue a publication notifying its clients and investors that the adviser has been the target of a breach, clients are likely to ask, "Is this a place where I should be investing my money? I'm worried now, because the systems have been breached. What should I do at this point?"

This is where PR management comes into play. It grants the adviser access to PR firms that specialize in these types of scenarios. A PR firm can help an adviser craft a message that includes what happened; the steps the adviser has taken or plans to take to fix the issue; and a number that the adviser's client can call to receive an update on the status of the breach or report information if the client believes that, as a result of the breach, a third party has accessed and used its confidential information.

This service gives the adviser a pipeline to disclose the proper information to its clients in a professional way, while being advised by those who specialize in communicating to clients or the public during crisis situations. If an adviser experiences a cyber breach, the goal is to maintain its business; continue moving forward; and to show its clients and investors that the firm is taking the rights steps toward resolving the situation. A PR firm can assist with this process.

HFLR: How do your clients know whom to reach out to if they do experience a cyber breach?

Vicidomino: Most insurers have approved panel providers. By way of example, the insurer AIG has a long list of approved providers who are the best in the business for cyber forensics work, cyber legal work and PR. Consequently, when entities purchase a cyber insurance policy from AIG, they know that policy comes with a list of AIG-preferred service providers and what their specialties are.

This is an added bonus to the client, as it provides them with a template to follow in the event of a cyber breach. A lot of times, clients can take steps to establish relationships with these service providers in advance of a breach. Many of these approved service providers offer complimentary introductory calls where they can walk the policy holder through how the process would work in the event of a breach. This gives a lot of clients comfort, as they have already established a relationship with the firm upon which they would be relying in the event of a cyberattack.

HFLR: Are we going to be hearing more about cyber insurance in coming months, under the new presidential administration?

Vicidomino: I think cybersecurity is going to grow as a focus as we move forward. For example, the New York Department of Financial Services released new cyber regulations a few months ago, bringing additional scrutiny to this issue.

[See "Are New York's Cyber Regulations a 'Game Changer' for Hedge Fund Managers?" (Jun. 8, 2017).]

When things like that happen, it draws increased attention to the issue, and clients ask, "What else can we do to make sure that we are following the right protocols, we are in compliance and we are ready to show the regulators that we are prepared to handle a cyber breach?"

Based on our conversations with clients, it appears that cybersecurity insurance is now being treated like E&O and D&O insurance by many institutional investors. In other words, investors are asking about cyber policies while conducting due diligence, and the expectation is that advisers will have purchased coverage to manage cyber risk.

[See "How Fund Managers Can Prepare for Investor Due Diligence Queries About Cybersecurity Programs" (Feb. 2, 2017).]

Historically, before an institution would invest in a hedge fund, ensuring that the adviser had an appropriate E&O and D&O policy was on the investor's list of due-diligence requirements. Today, cyber insurance is on the list of due-diligence requirements of many of these investors. Institutional investors expect a cybersecurity policy to be included in the adviser's portfolio of insurance. This has led to greater interest and demand in cybersecurity insurance products, and some advisers use the fact that they have purchased these policies to convey to their prospective and existing clients and investors that they care about cybersecurity and protecting the confidential information of their clients.

HFLR: What are some of the recurring questions that you receive from your clients about how cyber insurance applies to them?

Vicidomino: One major topic that keeps arising is social-engineering fraud. For example, clients often ask about the following scenario:

> It's five o'clock on a Friday, and the firm's CFO gets an email from the managing partner of the firm that says, "We need to wire $250,000 to this account to pay an invoice that is due. I need it done in the next 20 minutes. Make sure you send it." The CFO wires the money, and the firm later comes to find out that it was the target of a fraud. A third party stole the partner's email address and credentials and sent the email instructing the CFO to wire the money.

Once that money is gone, it's gone, and it's very difficult to find. Clients want to know if this sort of loss is covered by a cybersecurity insurance policy. The answer to that question is actually, "yes and no." The reason is that usually, a lot of cyber policies do not offer social-engineering coverage, because it's typically found under what is called a fidelity bond, also known as a crime bond.

Most hedge funds also have a fidelity bond in place for their firm. It protects them against internal theft such as embezzlement from management company or customer accounts.

Whether this type of scenario is covered under a cyber insurance policy will depend upon whether the insurance provider offers it as an add-on to the cyber policy. We tell our clients, however, that if they already have a fidelity bond, they should be covered for this type of social-engineering risk if negotiated properly.

I recommend to clients that they confirm that they have coverage for this sort of risk and know where that coverage is located. If a client wants coverage for this sort of risk under both a fidelity bond and its cyber policy, it will need to ensure that those policies will work together, as opposed to each policy assuming that the other policy covers this risk.

HFLR: What is another question that comes up frequently in meetings with clients?

Vicidomino: I am often asked by clients, "How do we correctly handle notification under a cyber policy? For example, if the firm has a breach but does not want to rely upon coverage under our policy, do we have to notify the insurance company? What is the protocol around that?"

As a broker, we always take a very cautious approach and advise our clients that if they have any sort of breach and are not sure whether there will be losses, at a minimum, they should call their broker. At that point, we would loop in our claims team and discuss whether we should notify the insurance company. That is something that we feel is of utmost importance. Clients are buying these policies for a reason, which is to protect themselves against these types of situations. If they do not provide proper notice under the policy, they risk potentially voiding the coverage that would otherwise be available under the policy.

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