HEDGE FUND
legal & compliance digest

www.hedgefundlcd.com June 15, 2016

What All Hedge Fund Managers Should Know About Cyber Ransom Attacks: Vulnerabilities, Risks and Strategies to Fight Back (Part Two of Two)

By Jon Shazar and Liz Walker

The Federal Bureau of Investigation's 2015 Internet Crime Report cited nearly 2,500 ransomware incidents against individuals and organizations last year. More generally, some 3,300 malware attacks were reported to the FBI, along with nearly 8,000 business email compromise incidents. BEC attacks alone resulted in $263 million in losses. Cyber attacks increasingly are just another calculation in the cost of doing business, and though recent attack statistics are chilling, strategies for fighting back have evolved correspondingly. Hedge funds and others are now better able to defend against cyber attacks and mitigate the harm they can cause. This article, the second in a two-part series, discusses practical steps hedge funds can take to prevent or mitigate the effects of a cyber ransom event, along with strategies for navigating an actual attack.

What Practical Steps Can A Hedge Fund Take To Prevent Or Mitigate A Cyber Ransom Attack?

There is almost nothing a hedge fund—or anyone else—can do to completely inoculate itself from hacking. But there are several ways that attacks can be minimized, and the impact of those that do occur mitigated.

First, it is crucial that a firm know its vulnerabilities and understand the structure of its internal network and systems. Third-party informational technology and cybersecurity experts can help hedge funds get a handle on where they need to focus their attention and on how to build the most secure systems possible. Given the risks posed by a firm's third-party vendors, it goes without saying that risk assessments are key to evaluating the strength of service providers' cybersecurity, especially those with direct access to a hedge fund's own systems.

Such independent risk assessments cannot be a one-off: As a firm's systems change and grow, and as new cyber ransom threats emerge, existing security apparatus must be continually updated and upgraded. Indeed, even between independent assessments, it is crucial that all software, especially firewall and anti-virus systems, are updated regularly. Firms should also have anti-malware software—again, frequently and if possible automatically updated—and script-blockers preventing unauthorized web sites from infecting their systems. Segmented systems, which can prevent malware from moving about a network, are better than "flat" networks which give hackers access to everything, said Lisa Sotto, chair of Hunton & Williams' global privacy and cybersecurity practice. Ken Citarella, senior managing director for investigation and cyber forensics at Guidepost Solutions, suggests that firms consider both sandboxes and whitelists for e-mail systems: The former quarantines all attachments until they've been checked out, while the latter only allows in emails from pre-approved domains. "A whitelist is obviously inconvenient," Citarella allows. For instance, every time a new client is onboarded, their email address has to be added to the whitelist. "It takes 30 seconds, but it can save a great deal."

Likewise, it is important that system monitor logs are active, keeping a record of who enters the system and when. That record can be invaluable during a forensic investigation, but too often, logs are switched off due to the perception that they slow systems down or take up too much storage. "It's a long-term problem," Citarella admits.

Back-Up, Back-Up, Back-Up

A vigorous back-up system is the closest one can get to immunity from a cyber ransom attack: If your data has been sufficiently backed-up and the back-up protected from infection, you can simply ignore the ransom demand, wipe your systems clean and restore your data to its pre-infection state. “These days, there’s nothing cheaper than computer storage,” Citarella said. “You can put it in the cloud for very little expense.” Best of all, Citarella is unaware of any malware attack successfully migrating to a cloud back-up. “Maybe you lose an hour’s worth of data, or 24 hours’ worth,” he said. “In the hedge fund industry, every transaction is very important.” So while back-ups should occur at least once a day, “you want to back-up as often as you possibly can.”

Employee Training

Given that human error is most frequently responsible for cyber extortionists gaining access to a system, the importance of training and limiting the possibility of such “invitations” plays a critical role. Firms should require employees to use passwords with a combination of upper- and lower-case letters, numbers and symbols—and to change them with regularity. Such a policy greatly reduces the risk of “brute-force” attacks, and ensures that, even if a firm is the victim of a keylogging, the passwords obtained by hackers will give them access for only a limited period of time.

“Train, train and retrain,” Citarella said. Prepare your own “spear-phishing emails” to test employees. “It’s no different than training people to perform well. Security is just another type of performance.”

Cyber Insurance

Hedge funds may also wish to consider a cyber insurance policy. Of course, insurance does little to protect one from an attack. But it can help mitigate the substantial costs that can arise from the attack. In addition to loss or damage to databases, software and coverage for vicarious liability, such policies can also cover front-end forensics and legal costs, said Bob Parisi, managing director and national cyber product leader for Marsh. What’s more, simply getting a cyber insurance policy can force an organization to look closely at the risks it faces; indeed, many insurers impose best practices requirements that can greatly improve a firm’s own efforts. Such policies often also include a suite of products and programs that can help a firm bolster its cybersecurity capabilities, especially for small and mid-sized hedge funds. They can also require that a firm maintain incident response teams, or “panels comprised of best-in-class information security forensic vendors, law firms that specialize in handling and advising clients on breaches, crisis management firms that are skilled in dealing with the reputational angle of this,” Parisi added. “Those carriers tend to provide a variety of educational and risk-management tools. They’ll provide educational tools around helping a firm’s employees understand cyber and privacy risks. They’ll help a firm tabletop or bench test its incident response plans.”

Parisi does recommend buying cyber insurance from the same carrier holding a firm’s professional liability coverage. The two can overlap, and going with the same provider can both help ensure a firm is only paying for coverage it needs, and can “avoid any finger-pointing” in the aftermath of an attack.

Incident Response Plan

All of the above requires a buy-in about the importance of cybersecurity at all levels of an organization. Effective governance, both at the fund management firm and among a firm’s fund boards, is key to success in this area. Nowhere is that clearer than in perhaps the most important aspect of a hedge fund’s cybersecurity preparation: an incident response plan. The minutes and hours after an attack can be chaotic; decisions have to be made quickly and without the benefit of full knowledge of the situation. As such, it is critical that people know their roles in the event of a cyber ransom attack and that there is a clear chain of command. It is also important that a firm’s agreements with vendors include policies and protocols for their role in an attack and recovery situation. Bench tests are vital to ensure that an IRP is deliberately designed and that those implementing it know what to do. “If you’re figuring out how to deal with the crisis when you find out about the crisis, things are going to go horribly wrong,” Parisi warns. “If you’ve planned for the crisis and tested your policy, it’s going to go much smoother.”

More and more hedge funds are hiring chief information security officers, a step specifically recommended by the Securities and Exchange Commission last year. Those not large enough to warrant such a hire generally entrust their IRPs to their chief information or technology officers, or an outside IT vendor. In addition to such a point person, the manager, general counsel and potentially a lawyer specializing in privacy matters should be involved. “A larger organization may include somebody from your PR firm, customer service and the security department,” Citarella said. If a firm has cyber insurance, experts on the panel recommended by the insurer should be involved as well.

“You have to decide how you are going to communicate with each other, because if your network is compromised, then your smartphones may be compromised. Or your email may be being

monitored," Citarella said. "I need secure communications. And part of that really has to be done under the advice of counsel, because you may need to be preserving a record of what's going on."

Sotto's recommendations for a strong IRP include "having a breach notification toolkit that you can take off the shelf if you need to. Having a legal incident response procedure that lawyers can turn to to understand the rules of the road."

"The legal department would be responsible for doing their legal analysis after an event has been identified and the forensic investigation is proceeding," she adds. "Under the IRP would fall the legal breach notification procedure that would provide the legal department with the rules of the road for legal notification."

"If the data belongs to humans, we have to break it down by jurisdiction to do the legal analysis. We need to understand what contracts might come into play. Often, contracts now have requirements to notify the contract parties if there's a cybersecurity event. We need to understand what our regulatory obligations are, what regulatory authorities need to be notified and when. How do we involve law enforcement? Those are the kinds of tasks that legal would be charged with."

So You've Been Hacked

Even the best IRP is only as good as its middle word: It is a response, which means that a hedge fund's other efforts to prevent an attack have failed and that the inevitable has arrived. What now?

Firms that have implemented a comprehensive IRP need simply execute it. Key players must be notified. It is crucial—both for insurance purposes and for regulatory and law enforcement purposes—that the response be exhaustively documented.

Still, every cyber attack is different and there will be critical questions that a firm's IRP won't necessarily be able to answer. The biggest, perhaps, is should the firm simply pay the ransom? In many cases, the answer is yes—even from the FBI. Boston Assistant Special Agent Joseph Bonavolonta last year told a cybersecurity conference, "The ransomware is that good. To be honest, we often advise people to just pay the ransom."

"There are some times when there is nothing better to do than pay the ransom," Citarella said. He notes that most malware attacks are numbers games, rather than targeted efforts. As such, "most ransoms are for a couple hundred dollars, $1,500, $2,500, because they're successful enough at that rate that they're earning enough money to make this a worthwhile endeavor."
"For a hedge fund, depending on the volume of activity, the volume of clients, etcetera, you may have a choice to try and fight it. There are some decryption codes that have become known and sometimes you can reverse it. Although that's very rare, it's possible."

The extent of an attack's damage and the information breached may not be immediately apparent. But as the scope of the event becomes clearer, a hedge fund's responsibilities—notably in the area of notification—will also be clarified.

What is clear is that a firm shouldn't notify widely right away, and not only because of the potential reputational harm. Some cyber ransom attacks are inside jobs; broadcasting one's IRP and ongoing efforts could be giving oneself away to the perpetrators of the attack. Initially, only those involved in an incident response should be notified and privy to the firm's plans. Unfortunately, it won't likely be able to end there. Is the firm required to notify any authorities? Has clients' personal information been compromised, requiring further disclosure, both to regulators and to investors? Have third-party vendors been put at risk, requiring their notification?

"There are good things about having law enforcement involved," Citarella said. But there are also potential pitfalls. "Law enforcement may have an attitude that they want to get the guy who did this so they can arrest him. That might be a very secondary concern for the victim organization. There may be some disagreement as to priorities."

"If a client were inclined to bring in law enforcement, I would recommend they bring them in as quickly as possible. Make the call as soon as you can. If you're not inclined to bring them in, then don't. You don't have to."

Whichever way a firm is inclined, it should make sure the decision is part of a broader, well-reasoned and tested plan. Because the question is not if you'll need it, but when. "It is going to get worse," Citarella said. "Even as defenses get better, there are still going to be bigger and bigger successes by the bad guys. The risk is that, in a very interconnected world, every vulnerability point can make everybody else vulnerable."