HEDGE FUND
legal & compliance digest

www.hedgefundlcd.com June 9, 2016

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

By Jon Shazar and Liz Walker

It has become an oft-cited cliché that businesses fall into just two categories: those that have been the victims of cyber attacks, and those that will be—or don't know that they have been. And, as then-FBI Director Robert Mueller put it four years ago, "even they are converging into one category: companies that have been hacked and will be hacked again."

Four years, of course, is an eternity when it comes to technology. And the sagacity of the old saw becomes truer with each passing day: Cyber attacks against businesses are up 144% over the past four years, according to CYREN's 2015 Cyberthreat Yearbook, including an 83% jump last year. No one is immune: Recent high-profile victims have included the Federal Reserve Bank of New York, JPMorgan Chase and, perhaps infamously, the law firm Mossack Fonseca, whose clients' confidential data became the "Panama Papers." According to the 2015 IBM Cyber Security Intelligence Index, finance was the hardest-hit industry in terms of incident rate in 2013 and 2014.

To date, hedge funds have not been among the prominent publicly-known victims of cyber criminals, but that doesn't mean they haven't been infiltrated. For all of the high-profile "macro" attacks on financial and government institutions—often the work of foreign governments and their intelligence agencies—and the work of so-called "hacktivists," politically-motivated and designed to outrage and embarrass, there may be thousands of cyber ransom and cyber extortion attacks perpetrated—and unreported—for very different reasons.

Unlike other forms of cyber crime, cyber ransom doesn't often make the headlines, and for good reason: Victims are usually happy to keep the matter quiet. To some degree, the very success and perceived wealth of hedge funds make them potential targets. Moreover, hedge funds, in particular, face potentially disastrous consequences from a cyber ransom attack. An attack that shuts down, or even delays for a few seconds, high-frequency digital trading platforms could result in millions of dollars in lost gains. Proprietary algorithms or client lists seized could jeopardize hard-won reputations or be financially ruinous.

As cyber attacks become increasingly common, and as awareness of them grows, however, firms increasingly have the means to fight back. It may be impossible to stop cyber ransom and other cyber crime, but hedge funds and others are now better able to defend against them and mitigate the harm they cause. This article, the first in a two-part series, examines why hedge funds may be vulnerable to cyber ransom attacks; the most common entry points cyber criminals exploit to access their systems; and the operational, legal and reputational risks a cyber ransom attack can pose. The second article in this series will discuss 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 Is Cyber Ransom, and Why Should Hedge Funds Be on Alert?

At its core, ransom is a simple tactic with a long history: I take something you value, you pay me to get it back. Cyber ransom is simply the latest and most technologically-advanced iteration of that millennia-old crime, in which a hacker targets a specific individual, company or organization to extort a payment in exchange for returning

something or just going away. And hackers engaged in the practice are getting better at it, often employing other types of cyber attacks to aid their extortionist effort.

Perhaps the best-known instance of cyber ransom occurred earlier this year, when Los Angeles' Hollywood Presbyterian Medical Center paid $17,000 to regain access to its patient records following a malware attack. That incident became public because the Health Insurance Portability and Accountability Act requires notification to affected parties if protected personal information is breached. Most cyber ransom attacks, however, don't involve PPI and therefore don't require public disclosure. In fact, most cyber ransom attacks hit individuals: Every email user has undoubtedly received the official-looking (or attempted facsimile of official-looking) email warning of dire consequences if she fails to follow a link or open an attachment.

As the Hollywood Presbyterian case shows, cyber extortionists aren't limiting themselves to individuals. Increasingly, they are combining malware with other internet-based forms of deception, such as spoofing and keylogging Trojans, to bolster their effectiveness and hit larger targets. And the malware they are using is getting better and better. In May 2014, a massive effort on the part of global and national law enforcement agencies, researchers and security specialists managed to take down CryptoLocker, a malware program that encrypted a computer or system's files before extorting a ransom payment in exchange for a key unlocking those files. Within months, an even more sophisticated ransomware Trojan, CryptoWall, was attacking vulnerable systems.

Indeed, hedge funds may be especially vulnerable to cyber ransom attacks. Especially among smaller and mid-sized hedge funds, the focus on the core of a hedge fund's business—managing clients' capital—has led to substantial outsourcing of middle- and back-office functions, and security experts warn that third-party providers are often a weak link in a hedge fund's security armor. The growth of quantitative trading and the use of digital trading systems have also made investment firms more susceptible: The more reliant a hedge fund is on its technology, the more devastating it can be to lose access to it, even for a period of microseconds.

Hedge funds may also be unusually attractive targets for cyber criminals. The perceived wealth and success of the industry make hedge funds particularly lucrative marks. Reputational and regulatory risks are also at play: Hackers know that hedge funds may be reticent to see their struggles plastered onto the front page of *The Wall Street Journal* for fear of alarming clients and potential clients, and that they may be reluctant to involve law enforcement for fear of giving them unfettered access to their systems and records.

"Hedge funds, if you view them as part of the overall economy, are in the crosshairs," said Bob Parisi, managing director and national cyber product leader for Marsh. "They're also in the crosshairs because they do have significant relationships. The individuals in hedge funds are well-credentialed, have relationships that go deep with other institutions. That's valuable in a way that hasn't necessarily made the press in the same way that lost credit cards have."

How Do Cyber Criminals Access Hedge Fund Networks?

While the tactics of cyber extortionists and the malware they use have evolved and become more sophisticated, there is still a vampyric quality to them, in that they have to be "invited" in. The overwhelming majority of cyber ransom cases begin with human error, namely, a vendor or employee unwittingly opening the door for them.

Third-Party Vendor Vulnerabilities

Experts believe that the most likely point of access is third-party vendors. Even the largest and most sophisticated hedge funds—those likely to have substantial in-house cybersecurity efforts—rely on such outside parties to perform some of their most important functions, including trading, custody, accounting and administration. "We worry a lot about vendors because you could have a fortress-like environment around your own systems, but if your drawbridge is down to a vendor who has authorized access to your system, any weakness in the vendor's system becomes your weakness," Lisa Sotto, chair of Hunton & Williams' global privacy and cybersecurity practice, said.

Often, these vendors—including prime brokers—have direct access to a hedge fund's systems and networks. That makes their technological vulnerabilities their clients' vulnerabilities. The 2014 cyber attack on JPMorgan Chase, which saw data for 83 million accounts compromised, shows that even the largest and safest-seeming counterparties can pose a risk; as of the first quarter, JPMorgan was the third-largest prime broker in the U.S., according to *Hedge Fund Alert*.

"I've got a current client, a small hedge fund," Ken Citarella, senior managing director for investigation and cyber forensics at Guidepost Solutions. "Let's say part of the client's domain

address has a double-T. A vendor received an email from the spoofed domain with a triple-T, and proceeded to execute the instructions. Gutted the hedge fund. Wiped it out."

Employee Vulnerabilities

Cyber extortionists can also be "invited in" by employees. The most common issue here is falling victim to a phishing attack. An employee receives an email with a web link or attachment. Opening either the web page or the attachment infects his or her computer with malware. When the employee then accesses files or systems on the company's network, the malware spreads.

Most computer users have become savvy to the so-called "Nigerian uncle" type of phishing message. To improve their odds, cyber criminals have turned to spoofing or "spear phishing," creating emails that appear to be legitimate—and often from a superior. In a highly-pressurized, fast-paced hedge fund office, an employee might not inspect the email address carefully enough to catch the scam, quickly opening a malware attachment that appears to come from a portfolio manager or the CEO.

Once a cyber ransom malware, such as CryptoWall, is on a hedge fund's system, it makes highly encrypted copies of a firm's files. It then deletes the original files and creates a dialogue box announcing its terms. Generally, a victim is given a certain period of time, often as little as 24 hours, to make a payment in Bitcoin. If the payment is not made in time, the ransom demand can increase—or the files can be destroyed or rendered permanently beyond reach. In many instances, the dialogue box will also offer "proof of life": an encryption key that will decrypt a single file on your system to demonstrate the cyber extortionist's ability to give you back the rest. Newer malware locks files with all-but-unbreakable encryption, making it nearly impossible to retrieve information without paying the ransom.

Keylogging Attacks

Malware contracted via a third-party vendor or a phishing attack remains the most common type of cyber ransom attack. But there are other vulnerabilities. Another type of malware, keylogging, can give bad actors usernames and passwords, giving them direct access to a firm's network and systems. Once in place, hackers can use their access to outright steal money by creating bogus wire transfers, for example. They can also steal sensitive data, including client lists, personal information about investors, confidential internal documents or proprietary trading systems, extorting payments with threats to release the information. The growing reliance on high-speed trading systems could also leave firms with unwelcome guests subject to denial-of-service attacks, preventing or slowing trading and other crucial functions.

What Are the Risks of a Cyber Ransom Attack?

Operational Risks

The risks posed by a cyber ransom attack, or any other cyber attack, are as clear as they are frightening. Hedge funds struck by CryptoWall or similar malware might literally be shut down, albeit temporarily: Without access to technology, there is almost nothing that a hedge fund can do, from trading to valuation to corresponding with investors to filling redemption requests. Though an attack of this sort usually lasts only a matter of hours, given the widespread use of high-speed and high-frequency trading, even a delay of that duration could be disastrous.

"It's not just about, 'Oh my goodness! We lost a million credit cards,'" Parisi said. "It really is the dependence that companies have because of the incredible use and over-reliance on technology." What's more, there are growing signs that individual cyber attacks could beget further incursions.

Legal Risks

Dire as the operational risks are, a cyber attack also opens a potential legal Pandora's box. In addition to questions of liability for losses, cyber attacks also raise questions about notification, especially if hackers get hold of clients' personal data. Forty-seven states, the District of Columbia, Puerto Rico, Guam and the U.S. Virgin Islands have privacy laws that could come into play, some with notification deadlines as short as 10 days. Breaches of protected personal information could also trigger the Graham-Leach-Bliley Act, under which "there's a rule called the inter-agency guidance that looks very much like state breach notification laws," Sotto said. The SEC is not party to that guidance, but it "very much wants you to notify affected individuals. There's really a mandate to do so."

The growing threat from hackers has led to an increasing focus on cybersecurity on the part of regulators. In 2014, the SEC issued a Risk Alert indicating they were taking a closer look at cybersecurity. Last year, the Office of Compliance Inspections and Examinations announced that cybersecurity would remain a focus of its exams. A week later, the regulator fined broker-dealer R.T. Jones Capital Equities Management for violating the "Safeguards Rule" by being inadequately

prepared for a cyber attack. As regulatory guidance becomes clearer—and new rules and requirements are put in place—simply failing to be properly prepared raises the risk not only of a successful attack, but also of a damaging enforcement action.

Reputational Risks

The threat of potentially required disclosure and regulatory enforcement actions leads inevitably to perhaps the biggest risk posed by hackers: reputational. In the wake of the scandals and performance issues suffered over the past decade, investors may be unwilling to tolerate a cyber attack, even if it is dealt with quickly and does not impact their personal information or their investment. “Strong reputations are hard-won and easily lost in the hedge fund world, and being the victim of a cyber attack can prove fatal for businesses,” Baker Tilly warns. And not only through clients lost, but also due to clients never won. “Indeed, investors have increased their due diligence on the issue. Hedge funds are seeing a higher level of focus on cybersecurity within requests for proposals, a sure sign that it’s a priority for their high net-worth and institutional clients.”