Hedge Fund Law Report
An Acuris company

hflawreport.com

February 4, 2021

CYBERSECURITY

Eleven Lessons From Cyber Hack That Forced an Australian Hedge Fund to Close (Part One of Two)

By Robin L. Barton, *Hedge Fund Law Report*

Telling people that if they do not take certain steps, something bad will befall them may not be sufficient to motivate them to take action. Instead, a real-life example of someone similar suffering from the forewarned harm may be required to get an individual to take the threat seriously.

Case in point: although hedge fund managers have been repeatedly warned by the SEC, other governmental agencies and industry experts that they are attractive targets for cyber criminals, many managers still have not devoted sufficient time and resources to building effective cybersecurity programs. Perhaps those managers will beef up their cybersecurity now that one of their own has been forced to close after being hacked by cyber criminals who used a fake Zoom invite to gain access to the fund manager's email system.

This two-part series provides 11 lessons that fund managers should learn from the incident that cost Australian hedge fund manager Levitas Capital (Levitas) $800,000 and a major investor – and compelled it to close up shop. This first article describes the incident[1] and explains the first three lessons. The second article will lay out the remaining eight lessons. For a look at a similar attack against three British private equity (PE) firms, see "Vulnerable Fund Managers Are Targets of Cultural Engineering Cyber Attacks: How Can Your Firm Avoid Being Next?" (Nov. 5, 2020).

What Happened

According to its website, Levitas is a Sydney-based quantitative hedge fund manager that specializes in equity volatility. It was co-founded by Michael Brookes and Michael Fagan. Because of its strategy and the global economic unrest caused by the coronavirus pandemic, the firm's main hedge fund was up 20 percent in 2020. At the time of the cyber attack, Levitas had $75 million in assets under management.

On September 10, 2020, cyber criminals sent Fagan a phishing email that contained what appeared to be a legitimate Zoom meeting invite. When he clicked on the link, malware was installed on his computer, giving the attackers access to Levitas' email system. They then used that access to educate themselves on the firm's operations.

On September 15, the cyber criminals posed as a representative of the firm and emailed Apex, the fund's administrator, an invoice asking Apex to transfer $1.2 million to a Unique Star Trading account at ANZ, an Australian bank. The administrator called Fagan to verify the transaction, but he was at the gym and said he would be in touch. The hackers – who now had access to Fagan's emails – sent one to Apex approving the transfer. The $1.2 million was sent the next day to the Unique Star account at ANZ. Between September 16 and 26, almost $800,000 was allegedly withdrawn from that account by Muhammad Bhatti, the sole shareholder of Unique Star, in 66 transactions.

On September 22, the cyber criminals sent another fake invoice, which resulted in $2.5 million being sent to an account in the name of Pavelin Limited at the Bank of China in Hong Kong. The same day, AET Corporate Trust (AET), Levitas' trustee, received further instructions from Apex to send $5 million to East Grand Trading at the United Overseas Bank in Singapore. The hackers sent additional emails approving those transactions, but neither AET or Apex received verbal verification from anyone at Levitas.

On September 23, Fagan checked the firm's bank accounts, as he was expecting a large deposit, and he noticed more than $8 million was missing. He began making frantic phone calls and was able to stop the $7.5-million transfers to the banks in Singapore and Hong Kong – but he was too late to stop the first $1.2-million transfer or to recover the $800,000 already withdrawn by Bhatti, who subsequently fled Australia on a Qatar Airways flight.

As a result of the hack, Levitas' largest institutional client, Australian Catholic Super, pulled its previously committed capital and canceled a planned additional $16-million investment, forcing the fund to close. Australian law enforcement officials are investigating the thefts. They reported that the attack on Levitas was just one of almost 2,000 similar hacks over the prior five months.

See "Practical Guidance for Hedge Fund Managers on Raising Capital in Australia, the Middle East and Asia" (Oct. 30, 2014).

Lessons for Fund Managers

Lesson #1: Private Funds Are Attractive Targets

Private fund managers are attractive targets to cyber criminals, confirmed BlackCloak founder and CEO Dr. Chris Pierson. "Cyber criminals are looking for any way into centers where there are large pools of money, so they're targeting hedge funds, financial institutions and wealth managers, as well as high net worth individuals themselves," he said. "Hedge funds are clearly in the sights of cyber criminals."

For further insights from Pierson, see our two-part series on safeguards for the proper disposal of computer hardware: "Risks and Examiner Expectations" (Mar. 19, 2020); and "Effective Inventories, Policies and Due Diligence" (Mar. 26, 2020).

Avi Gesser, partner at Debevoise & Plimpton, added that hedge and PE funds can be particularly vulnerable to the kinds of cyber attacks that are currently being seen.

"Very few cyber attacks are targeted in the way I think of the word 'targeted,' which means that you have picked a specific company or organization that you want to hack because it has something in particular that you want," he said. "Certain defense contractors or government agencies may be targeted. Otherwise, it's mostly opportunistic. Hackers are just going after low-hanging fruit. They have tools that they use for hacking, and those tools are going to be most effective at the places that are least prepared to defend themselves."

"Hedge funds, and to some extent PE funds, can provide pretty good targets because they're not heavily regulated. They haven't had the experience the banks have had with state-sponsored attacks and very sophisticated attacks going back many years," continued Gesser. "So, they haven't been required to harden their systems the way banks and a lot of other financial institutions have. They do, however, have access to a lot of money, and they usually don't have giant tech compliance infrastructures that can quickly respond to increased threats."

"Hedge and PE fund managers obviously take cybersecurity seriously, but sometimes they just can't pivot to handle new threat vectors the way a lot of other organizations can. That can make them targets," Gesser concluded.

For further commentary from Gesser, see "Debevoise Attorneys Discuss AI Regulation With Head of FINRA's Office of Financial Innovation" (Aug. 27, 2020); and "The Current State and Future of AI Regulation" (May 14, 2020).

See also "Surveys Show Cyber Risk Remains High for Investment Advisers and Other Financial Services Firms Despite Preventative Measures" (Jul. 20, 2017).

Lesson #2: Business Email Compromise Is a Successful Strategy

The Levitas incident is an example of one of the most popular strategies currently being used by cyber criminals: business email compromise (BEC).

"The most common – and probably the most successful – tactic that is currently employed, especially for hedge funds, is called BEC. That is when an attacker sends a fake email to the finance department or someone with account access. That email looks confusingly similar to a genuine email," explained Pierson. "The domain name may have an extra letter in it, or it may be sent from a compromised personal email account of the CEO or CFO. Once the attackers have a foothold in the company, they can send the email as the real individual because they've compromised the email system."

As in the case of Levitas, Pierson said the attackers may then email the recipient a fake invoice to an account number where money should not go or change the account number on a legitimate invoice. "BEC is the fastest growing global cyber crime right now. That tactic continues to be tried all around the world – especially in areas of high dollar concentration, *i.e.*, hedge funds," he concluded.

"There are reasons why BEC scams have been going on as long as they have, which is they work and they're a quick way to make a lot of money," Gesser agreed.

See "How Hedge Fund Executives Can Mitigate the Personal and Business Risks of Cyber Attacks" (Apr. 9, 2020); "How Hackers Can Infiltrate Fund Managers Through Executives, and How to Stop Them" (Apr. 18, 2019); and "Business Emails Must Be Secure to Avoid SEC Enforcement Action" (May 12, 2016).

Lesson #3: Cyber Criminals Are Smart – and Learning

Cyber criminals used to attack bank accounts and divert the money or look for large amounts of personal information that they could steal, Gesser said. Attackers have realized, however, those actually are not the most lucrative ways to monetize an attack.

"One of the most lucrative ways to monetize a cyber attack is ransomware," explained Gesser. "The other way is to do what happened here, which is to gain control of an email account; get information about how payments are made and by whom; and trick people into wiring large amounts of money to the attackers."

The cyber criminals do not have to win many BEC attacks, noted Gesser. "If you try 20 and only one of them pays off, it's still a couple million dollars. That's well worth it," he remarked. "They have become skilled at writing those emails in a certain way to convince people to act."

"The attackers are becoming more sophisticated, and technology is going to make it a lot easier for them going forward," continued Gesser. "For example, some attackers have the ability to mimic the voice of an executive using deepfake audio, and machine learning or artificial intelligence will soon be able to write emails that look like they're coming from whomever the attackers want."

For example, Gesser recounted an incident in which a cyber criminal was pretending to be a senior executive on his way to a meeting. The attacker called the help desk, claiming that he was an executive who had lost his phone and needed somebody to email something to his Gmail account. "We listened to the recording [of this call], and it was incredibly good. It sounded real," he said. Gesser recalled the "executive" screaming the following at the help desk employee:

> Do you know who I am? Do you want to keep your job? I'm on my way to a board meeting, and I need this deck. I can't get into my email because I lost my phone, and you just need to email it to my personal account. If you don't do this, I swear to God, you are going to be gone by the end of the day.

"There has been a lot of education around voice verification control, which is fairly well known to cyber criminals. So, they will monitor for voicemail messages, which sometimes are transcribed to email," Pierson added. "If a message you left for someone was transcribed to email, the criminals will review the voicemail transcription and reply via email, saying, 'I got your voicemail. I'm too busy, but yes, everything is approved.'" He concluded, "Naturally, the person receiving that email will think, 'Okay, I did my job' – not knowing the bad guys are watching, monitoring and often controlling the emails."

In addition, an attack may now take place in a series of events, rather than an attempt to clear out an account in one transaction. "If attackers cannot figure out how much money is available, they'll start with some amount that they think is pretty safe. They wait to see if it goes through, and if it does, then it's just a matter of how much can they take out without being caught," Gesser explained. "So, it's very common to see a series of escalating amounts being taken from a firm's accounts."

See "Beware of False Friends: A Hedge Fund Manager's Guide to Social Engineering Fraud" (Mar. 8, 2018).

[1] Our discussion of the incident is based on various media reports, including an article by the *Australian Financial Review*, which broke the story on November 23, 2020.

February 11, 2021

CYBERSECURITY

Eleven Lessons From Cyber Hack That Forced an Australian Hedge Fund to Close (Part Two of Two)

By Robin L. Barton, *Hedge Fund Law Report*

As Australian hedge fund manager Levitas Capital (Levitas) found out the hard way, cyber criminals are targeting hedge fund managers, and the consequences of a breach can be dire. In Levitas' case, a fake Zoom invite ultimately led to its fund's downfall.

This two-part series provides 11 lessons that fund managers should learn from the incident and that can hopefully help them avoid similar outcomes. The first article described the incident that cost Levitas $800,000 and a major investor – and ultimately led to its fund's demise – and outlined the first three lessons for managers. This second article provides the remaining eight lessons.

For other lessons for fund managers from a cyber breach, see "What Fund Managers Can Learn About Cyber-Breach Disclosure From Yahoo's $35-Million SEC Settlement" (May 10, 2018).

Lesson #4: Remote Work Has Heightened Cybersecurity Risks

"The pandemic and the push to remote work has definitely exacerbated and increased the number of avenues of attack for cyber criminals. For example, many hedge funds did not previously use remote-meeting applications such as Zoom, Microsoft Teams, GoToMeeting, etc.," BlackCloak founder and CEO Dr. Chris Pierson observed. "Now that they do, the attack surface has increased that much more. Remote work isn't going away; it is going to be a part of the fabric of every company that exists from here on out." He added, "Furthermore, the home is the key area that must be addressed more globally as it is currently the greatest attack vector to the organization and the financial executive."

"Sending malicious Zoom links is a smart way to deliver malware right now," agreed Avi Gesser, partner at Debevoise & Plimpton, but he warned that "there are lots and lots of ways that criminals are delivering malware by convincing people to click on things or to give up their credentials."

"Maybe Zoom links will work this month and then people will figure it out and be trained or there will be some technological solution that will filter out valid Zoom links from invalid Zoom links," Gesser commented. "Then, hackers will find some other way to convince you to give up information off your computer that gives them control. It's this never-ending technological fight."

Remote work also creates vulnerabilities because people may be working on their own computer systems as opposed to company systems, and they are not just a few steps away from the IT help desk, added Gesser. "One huge issue in the remote environment for business email compromise (BEC) scams is because you're not in the office, you can't walk over to the CEO's desk and ask if this is an authorized transaction," he said. "You have to call the CEO at home – and attackers are relying on your unwillingness to do that as part of their scheme."

See "Companywide Work From Home: Six Cybersecurity Considerations" (May 7, 2020); and "How Fund Managers Can Withstand the Coronavirus Pandemic: Business Continuity and Other Operational Risks (Part Three of Three)" (Apr. 16, 2020).

Lesson #5: Relying on Spotting Red Flags Is Not the Best Approach

In the aftermath of the Levitas attack, Michael Fagan, co-founder of Levitas, acknowledged that "[t]here were so many red flags which should have been spotted." Those red flags included:

- The fake invoices were addressed to Levitas, not its trustee – AET Corporate Trust – as required.
- The money was sent to companies that the fund had no prior relationship with and that were not on its supplier list.
- The invoices claimed to be a "capital call," something the fund had never previously conducted.

Although fund managers should be aware of certain red flags, they should not design their cybersecurity systems based on spotting those anomalies, advised Gesser. "You don't want to create a system based on the attackers' sloppiness."

"You should prepare for situations in which the attack looks perfect: the invoice looks exactly right and comes from a recognized email address, or the call comes from somebody who sounds exactly like the CEO and comes from a recognized phone number," Gesser recommended. "You have to think of what technological and operational checks you're going to implement on your system to defend against those perfect attacks. Your system shouldn't assume that there are going to be those kinds of red flags."

"You want to create a system in which the 'red flag' is the request to send a lot of money to a new account or with new wiring instructions. Something new is the red flag," continued Gesser. "Everything else is gravy in terms of other opportunities to identify illegitimate emails or requests. It's much better to have hard-and-fast rules that don't depend on spotting those kinds of mistakes."

See "Critical Components of a Hedge Fund Manager Cybersecurity Program: Resources, Preparation, Coordination, Response and Mitigation" (Jan. 15, 2015).

Lesson #6: Robust Policies and Procedures Are Effective – and Give Employees Cover

Pierson recommended that fund managers do the following to protect against cyber attacks:

- educate and train employees on things such as phishing, malware and best cybersecurity practices;
- put technological controls in place to scan, in an automated fashion, all incoming emails to make sure that malicious links and code do not enter the environment;
- install anti-malware protections for when users click on illegitimate links that do pass through controls;
- implement operational controls, especially as to financial transactions, such as requiring verbal confirmation from one or more people of transactions over certain amounts; and
- obtain appropriate cybersecurity insurance and fraud (sometimes called cyber crime) insurance.

Having hard-and-fast rules can not only prevent cyber attacks but also give employees cover when put in difficult situations, added Gesser. Returning to the incident discussed in the first article in this series with the fake executive who called the help desk, "suppose the firm had a policy that, under no circumstances are you to give information like that out to anybody – no matter who they are – without a certain piece of verification," he posited. "Even if that were the real executive and she didn't give him what he wanted, she could point to that policy and say, 'Here's the policy. I did my job here. I did what I was supposed to do.'"

"What's interesting is that, for all the talk about how expensive and complicated cybersecurity is, what we often find is that the weakness is human and non-technical – and very cheap to solve," Gesser observed. "It doesn't cost much to create a policy that says before you wire more than $X, you need to make contact with the person – at a number that you have previously verified – to confirm that it is, in fact, a valid wire transfer. That is not an expensive security measure."

Lesson #7: Anything New Should Be Scrutinized

As mentioned previously, Gesser and Pierson agree that anything new should be treated as a red flag, carefully scrutinized and subject to verification procedures.

The default should be that nothing be authorized that is new, such as a new account number or a change in an already existing bank account or wire number, Pierson explained. For example, "Suppose you've been paying [a vendor] $100 a month for five years to a bank account number that has already been confirmed," he posited. "If the vendor asks for payment to go to a new bank or new account number, the answer by default must be 'no.' It will not be approved unless certain steps have been taken." Some firms even require two individuals to make a double verification of any changes, especially for higher dollar amounts, he noted.

The fund manager should be the one initiating the confirmation of anything new, added Gesser. "You shouldn't receive a call from the person saying the wiring instructions have changed. You should initiate the call to a number that you recognize – preferably on Zoom so you can see the person you're

speaking to and have him or her hold up a company ID or the like," he explained. "You should take the extra step because if you wire $5 million to the wrong person, it's probably going to be a really bad couple of days for you."

See our three-part series on how fund managers should structure their cybersecurity programs: "Background and Best Practices" (Mar. 22, 2018); "CISO Hiring, Governance Structures and the Role of the CCO" (Apr. 5, 2018); and "Stakeholder Communication, Outsourcing, Co-Sourcing and Managing Third Parties" (Apr. 12, 2018).

Lesson #8: Culture Can Undermine Strong Policies and Procedures

A robust cybersecurity program can be undercut by the manager's culture.

Fund managers may have a lot of money that moves back and forth all the time, so there is pressure to not slow things down, said Gesser. Thus, employees may feel compelled to please investors, executives, supervisors, etc. by acting quickly to, for example, fulfill an investor's redemption request – even if that means forgoing the required verification procedures.

In addition, attackers may use a believable sense of urgency to convince employees to bypass the usual safety procedures, Gesser added. "The controller may receive an email from what appears to be the CEO's account, saying, 'We've got this deal. It's moving really quickly, and it's secret. I need you to wire this money so that we can complete this before the close of business in Hong Kong,'" he posited.

"The attackers create the atmosphere of urgency in a way that seems plausible. The controller may never have spoken to the CEO, so it may be weird to make that confirmation call – especially if it could delay or kill the deal."

"We have seen companies with the right procedures still have issues because of the speed of work and the pressure on people to finish fast," concurred Pierson. "Employees need to know that their careers will never be in jeopardy if they do not approve something because they were unable to have it properly authorized. The highest-ranking executive that is part of that chain needs to own that issue."

See "SEC Chair Offers Observations on Culture at Fund Managers and the SEC" (Jun. 28, 2018).

Lesson #9: Incidents Should Be Used in Cybersecurity Program Reviews

Fund managers should regularly review their cybersecurity policies and procedures – and they should use incidents such as what happened to Levitas in those reviews.

"Given the speed of cyber crime right now, reviewing your cybersecurity program at least twice a year is necessary. Cyber criminals are making changes to their tactics every day, and if you don't make changes internally, then you might be behind the eight ball," warned Pierson. "You can also use an incident such as Levitas to kick the tires on what you currently have, asking 'Could this be us? How would we protect against this?'"

"There are always opportunities for firms to learn from not only their own incidents but also other firms' incidents about how to become more resilient and be able to defend themselves," Gesser stressed. "That's why good organizations participate in threat-sharing groups in which they swap stories and information about what they're seeing, where they've experienced attacks and what has been successful – and unsuccessful – in defending against those attacks." He continued, "You take a look at some recent successful cyber attack, understand how it occurred and review what technique was used, and you ask yourself, 'What would happen to us if attackers tried this? Where would we be able to defend ourselves? What more could we be doing?'"

Lesson #10: Third-Party Cybersecurity Matters, Too

After the incident, Fagan said that "the entire funds management industry relies on a range of important checks and balances to ensure the integrity of the system – in particular, the role trustees and administrators are supposed to play. . . . This is one example of the manifest failure of these checks and balances with dramatic consequences for our business."

Noting that there have been similar cases in which third parties such as fund administrators have been tricked, Gesser advised fund managers to not only review the cybersecurity measures of outside vendors but also to set strict rules for them. "As the fund manager, you might want to tell your administrator not to send out any money for you unless the request comes from a known person and the administrator calls that person at a previously verified number for confirmation," he said.

"Maybe for particularly high amounts, it must be verified by two people. You want to create requirements that are pretty onerous for significant transfers. You should be willing to sacrifice a little bit of convenience and speed for the certainty that your money is going where you think it is."

See "How Managers Can Identify and Manage Cybersecurity Risks Posed by Third-Party Service Providers" (Jul. 27, 2017).

Lesson #11: Investors and Regulators Care About Cybersecurity

It is important to remember that Levitas was forced to close not because the attackers stole all of its money but because the hack scared away its main institutional investor.

"The longer certain kinds of cyber attacks go on and the more there are established mechanisms in place to defend against them, the more of an outlier you might look like if you don't implement some of those mechanisms," commented Gesser. "The market can move relatively quickly when new attacks are made. Firms that take it very seriously will adapt and add resources; training; or policies and procedures. Over time, investors become less understanding to the extent they believe that there were things you could have done to prevent certain attacks."

Investors are not the only ones interested in fund managers' cybersecurity programs – regulators care, too.

"Regulators are focused on customer protection. They don't want you to externalize those risks to insurance or litigation. It's easier for everybody if you avoid problems in the first place by having techniques in place to prevent attacks," Gesser observed. "Cyber is now one of, if not the biggest, threats to financial firms in terms of protection of customer assets. Regulators expect firms to take this seriously and to be aware of what attacks are out there and what steps have been successful at stopping them."

See "OCIE Risk Alert Provides Cybersecurity Guidance to Investment Advisers and Broker-Dealers" (Sep. 24, 2015).