hedgeweek special report
www.hedgeweek.com
April 2016

Practical steps to becoming cyber secure

In association with Intralinks

Identifying your firm's crown jewels

Developing robust cybersecurity programmes

Planning your firm's response to a cyber breach

"If you see something, say something"

By James Williams

On 5th April 2016, Global Fund Media, in partnership with Intralinks, hosted a cybersecurity luncheon at the Lambs Club, Manhattan, to outline some of the practical steps managers should think about to create a viable cyber threat matrix.

Moderated by James Williams, Managing Editor of Hedgeweek, the panel consisted of: Meghan McAlpine, Director of Strategy & Product Marketing, Intralinks; Buddy Doyle, Founding Principal, Oyster Consulting LLC; Jamie Hadfield, Managing Director -Technology at Gen II Fund Services, a leading private equity fund administrator, and Mike Steed, Founder and Managing Partner, Paladin Capital Group, a Washington DC-based private equity manager that specialises in investing in cybersecurity companies.

The following report outlines the main talking points, based on four core principles, that came out of the event: 1) Identification, 2) Prevention, 3) Detection and 4) Response.

James Williams, Managing Editor of Hedgeweek

Setting the scene

A decade ago, the cyber threat was far less pronounced; but with the adoption of mobile technology and a vast array of digital platforms, thanks to significant advances in technology, the threat that cybercrime poses to global industry and national critical infrastructure (power stations, hospitals, dams, financial services) has grown exponentially. There are nine billion connected devices today. That number is expected to rise to 30 billion by 2022.

"Every time you adopt a digital platform the vulnerabilities to your network and to your data and operations increase tenfold, even one-hundredfold, so much so that it is no longer stealing that is the main threat, it is disruption and destruction," said Steed in his opening comment to the audience, which was largely comprised of fund management senior partners.

When managers think about adding new digital platforms to their business, the first

question should always be: Why? Adopting Blockchain is believed to reduce transaction expenses by USD20 billion so companies are going to embrace it, but, said Steed, "you should always be asking yourself, 'Where's the security? Does this allow the bad guys in?' It's the same with mobile devices. Every connected device becomes an attack surface for the bad guys to get in."

Increased LP transparency

Aside from adopting digital platforms/ solutions to improve business efficiency, alternative fund managers are becoming potentially more vulnerable to cyber attacks due to the amount of information they find themselves having to share with investors and regulators.

McAlpine noted that in a recent survey conducted by Intralinks (www.intralinks.com/resources/whitepapers/2015-gp-survey-reporting-data-security-deal-flow-management) 89 percent of hedge fund investors and 71 percent of PE investors said they wouldn't invest in managers based on transparency concerns.

"This is top-of-mind for managers as they raise assets and they are trying to provide as much transparency as possible. But this opens them up to a wider range of risks including cyber risks and, potentially reputational risks if a serious breach occurs. It also exposes them to regulatory risk. The SEC is cracking down and wants registered investment advisers to have strict cybersecurity policies in place. For those that don't they are issuing hefty fines.

"It's important for managers to think about how secure that information is when sending it out to investors, and how best to protect the most vulnerable data," said McAlpine.

NIST Benchmark

It doesn't help that there are no universal cyber guidelines for managers to refer to within the fund industry. Knowing what is or isn't a robust cyber framework is hard to gauge but the panel agreed that the National Institute of Standards and Technology ('NIST') provides a useful benchmark standard. Following the guidelines can provide a useful roadmap for managers internally to make sure their compliance framework stands up to scrutiny.

"It's important for managers to think about how secure that information is when sending it out to investors, and how best to protect the most vulnerable data."

Meghan McAlpine, Intralinks

"Cybersecurity is not just one device you can plug in to your network to solve the challenge, it's multi-faceted. Following guidelines like those outlined in NIST on a day-to-day, month-to-month basis can assist managers with establishing a good cybersecurity programme," suggested Hadfield.

Identification

The size of the potential cyber threat depends on the nature of the organisation. As such, putting in the right controls ultimately depends on identifying what the manager's most sensitive data is and where it is located. Think of this as identifying what the firm's crown jewels are. The more there are, the more comprehensive the cybersecurity programme will need to be.

"To be clear, you cannot establish a cybersecurity programme without understanding what these crown jewels are," emphasised Doyle. "They will consist of the most sensitive, private data and need to be properly guarded. At Oyster, we use third parties that provide various levels of access to this information. I would recommend that managers look holistically across their organisation to understand where these critical assets reside."

This is effectively digital risk management. As such, managers are minded to place as much importance on this as portfolio risk management or, indeed, operational risk management.

"We are all going to become more regulated. While NIST is out there, and is voluntary, you can expect a full regimen of regulations that fund managers are going to have to comply with in the future. As such, any cyber programme should start with

the simple question: 'What are my assets?' You'd be surprised how often, when we visit companies, the top 50 people in the firm all give different answers to this," said Steed.

The next question is: 'Where are those assets located?'

If some of the critical assets are located in a server that 50,000 people have access to, that's a potential vulnerability. If they are on a cloud platform, do you really know where those assets sit?

And finally: 'Of all the assets, which are the most critical?'

In other words, what are the assets that if stolen, disrupted or destroyed could potentially ruin an organisation?

Logically, identifying these critical assets is an internal consideration. But there also needs to be an external approach, which many managers tend to overlook. Think about private equity: How many GPs ask to see a target company's cyber policies before making an investment? How many ask to see what the company's auditors said about their cyber policies?

Steed was quite emphatic in suggesting that it is "a fiduciary duty of managers to ask serious cybersecurity questions before making investments. "If a nation state or a teenage hacker holds a company's intellectual property, it isn't going to be as valuable as you first thought. Ask before you proceed whether the company's intellectual property is secure and has not been compromised in any way."

All too often, fund managers think they operate in a vacuum. But the ecosystem of which they are a part is ever growing larger. A fund management group will interact with multiple vendors and service providers. Managing that risk means working out where every piece of information is coming from throughout the entire ecosystem.

"If you are going to be working with lawyers on subscription document or deal execution documents, once you receive those documents where are they housed and saved? Often, there will be multiple copies of information held with different service providers. Firms need to understand where those assets reside, not just internally but throughout the entire lifecycle of any kind of transaction," advised Hadfield.

Mike Steed, Founder and Managing Partner, Paladin Capital Group

Prevention

Once the crown jewels have been properly identified, what measures can be taken within a cyber programme to prevent a potential cyber breach?

Data management

Apart from coping with the sheer volume of data today, alternative fund managers are being required to constantly improve transparency. Hedge funds have been adjusting to the demands of institutional investors for a number of years but this is now taking place in the private equity space, with LPs requesting more information on potential deals, valuations, etc. This puts managers at cyber risk, given the sensitivity of that data.

As such, data management is a key consideration when looking to develop a robust cybersecurity programme, specifically in the way that data is communicated to investors and third-party vendors.

Email is by far the standard protocol. That is not likely to change any time soon. Problem is, there's no way of knowing where that information goes once it leaves the manager's network. McAlpine said that once managers have identified their fund's crown jewels, it is important that none of that information is shared using email. It simply isn't secure enough.

"For the most sensitive information it is advisable to have in place a secure communications tool. This will allow you to use information rights management (IRM) so that only certain people in the organisation have access to certain data. Also, it will give you the ability to track what people are looking at.

"A secure communications tool allows fund managers to lock down documents so that people can't print them. Email is never going away but for any information that gives your company a competitive edge you want to make sure you have a secure communications tool to share that information externally," outlined McAlpine.

Electronic paper shredder

To expand on IRM briefly: If, for example, a laptop gets left on a train, IRM technology enables the end user to prevent anyone from accessing the data to print it out, or

to prevent photographing of the screen by using watermarks. Moreover, IRM technology allows the fund manager to remotely revoke access to the data at some later date.

Think of it as having an electronic version of a paper shredder.

The importance of getting off email and moving to something more sophisticated that facilitates greater control and management of data – and which effectively mirrors the digital world we live in today – is not to be underestimated.

Buddy Doyle, Founding Principal, Oyster Consulting

Vendor management

Another critical component of Prevention discussed by the panel is vendor management. Just recently, an international law firm was successfully hacked and sensitive information on a number of M&A deals was stolen for insider trading purposes. Managers have to be 100 percent certain that their service providers, including their legal counsel, are maintaining the highest levels of cybersecurity.

"Our clients and their investors are applying a sharper lens to what cyber processes and controls we have in place," confirmed Hadfield. "Large LPs are insisting on this before making allocations to GPs."

Oyster Consulting's Doyle said that one of the most onerous DDQs the firm had been through comprised a 1,350-line questionnaire that was completed with an onsite visit, auditing all the controls and processes that the service provider said they had in place. This even involved visiting their data centres.

"One of the things we encourage our clients to do with respect to prevention is annual training of their employees. To me that is a vital information-gathering exercise. The two reasons that data often ends up in the wrong hands are because of Bad Guys and Boneheads. Unfortunately, a lot of times it's the Boneheads that accidentally put the tax documents in the dumpster rather than shredding them at the accounting firm.

"It's vital that managers ask their vendors about their cybersecurity training programme so that they can seek reassurances that this is something they are taking seriously," explained Doyle.

As part of their Prevention programme, managers should ascertain which vendors are holding the most sensitive data and then make them the focus of more detailed due diligence; either on a semi-annual or annual review basis.

"When managers assess their service providers they might want to consider how data is stored and protected by their service providers and how it is being transmitted; is the data encrypted for example? You have to manage your vendors in a more detailed way today. Do they have proper certifications? Do they do penetration and vulnerability tests?

"If service providers do not take these precautions it might be advisable for the manager to pass on that vendor relationship," advised Hadfield.

Staff training

No matter how secure a cyber programme might be, staff training is absolutely critical. Humans are, ultimately, the weakest link and often the source of internal cyber breaches. Social engineering methods are becoming ever more sophisticated as hackers use platforms such as LinkedIn and Facebook to build an organisational profile of a firm, the service providers they use, etc.

This information is used to phone employees, whereby the hacker pretends to be the fund administrator to trick them into approving a wire transfer, for example. But still the most common threat is the phishing email, where keywords and phrases, which may have been accumulated via an Advanced Persistent Threat, are deliberately used in emails to trip up employees.

There is no perimeter fence that works to prevent phishing attacks. Some how or other these emails get into the network. All it needs is for somebody to click on the link, which opens up the malware to steal, disrupt or destroy one's network.

"Managers should think about putting in place what we call security awareness training. We found one company, called PhishMe® Inc, a leading provider of phishing threat management solutions. The firm does security awareness training and works with clients and the solution works by allowing a manager's appointed fund administrator to send out a false phishing email to its employees.

"As soon as an employee opens up the phishing email and clicks on the link,

they are presented with a 20-second tutorial. The most important part is at the end where it says, 'You've been reported to the administrator. Don't do it again'," explained Steed.

The psychology here is to put employees on constant alert. Instead of automatically clicking on emails, they start to look more closely at emails and avoid automatically clicking on links because they know there is a Big Brother-type system being used by the administrator.

Solutions like PhishMe are proven to reduce click-throughs in emails by 80 to 85 percent, said Steed.

Become cyber warriors

The mindset of employees should be to become cyber warriors: If you see something, say something.

The other thing to consider, which often gets overlooked, is insider threats within one's organisation. Look at authorisation and authentication processes; are the passwords strong enough, are they alphanumeric? Are people trying to access data that they shouldn't be?

Detection

Most damage is done when malware or an APT enters the network, carefully working in the shadows. Phishing emails are almost impossible to stop on an absolute basis. On average, some 66 per cent of breaches remain undetected for months; according to Steed, it's around 209 days. Imagine how much damage can be done in that time?

Another statistic to consider is that 87 per cent of breaches are discovered by external parties; maybe the FBI come knocking on the door, or customers/investors raise the alarm that something abnormal is happening. Either way, when it comes to the Detection element of a cybersecurity programme, the more employees develop best practices and, essentially, expect cyber breaches to occur, the quicker they are likely to respond to potential threats.

The point he was making was that personal hygiene involves numerous steps and, as such, any good cyber programme should take a similar approach. It should utilise multiple detection tools – end-point protection, intrusion detection and prevention

"Those that guard the critical assets need to avoid complacency or getting fatigued because that's when things will get overlooked."

Jamie Hadfield, Gen II Fund Services

systems, Security Information and Event Management (SIEM) systems, firewalls – in conjunction with regular staff training, getting upper level management buy-in on the training and awareness programme and establishing an incident response team.

"Managers need to think about taking a completely holistic approach to being cyber secure, and detection is just one element of that," said Hadfield. "Part of detection is remaining constantly aware of your work environment and the threats that persist. Those that guard the critical assets need to avoid complacency or getting fatigued because that's when things will get overlooked."

As highlighted recently in an article published by TechCrunch, FinTech companies are springing up to use big data techniques to improve detection, some of which employ machine learning techniques to build a profile of user behaviour within an organisation; examples include Cybereason, LightCyber, Seculert, Vectra Networks.

Digital Shadows offers what it calls 'cyber situational awareness'. The premise is that every company leaves behind a digital footprint that attackers can exploit. Equally, cyber criminals cast their own digital shadow which can be tracked, providing an 'attacker's eye view'. Such solutions are helping companies to better detect threats that might involve loss of data or reputational damage.

"There needs to be continuous monitoring of your environment in order to make sure you understand what's going on. At Oyster, we use two third parties monitoring our data on a full-time basis. Detection should not be viewed as a part-time task," said Doyle.

This is where appointed strong third parties will benefit the manager. After all,

they cannot be expected to monitor these threats internally. McAlpine said that at Intralinks, multi-factor authentication is used on its platform.

"If you are typically logging in from an office in New York and then all of a sudden your user ID is logging in from Beijing, for example, it will trigger a red flag in the system and the system will ask for further information to confirm and authenticate the identity of the user. This is quite an effective early warning system," said McAlpine.

Response

The last element of a cybersecurity programme discussed by the panel was Response.

How quickly someone responds to a breach will have a huge impact on how serious that breach ultimately is. The quicker it can be nipped in the bud, the less collateral damage will likely be caused.

Hadfield suggested that organisations can use segregated networks and have an incident response team in place so that if a serious breach were to occur, the team would be able to take the necessary steps to shut down the affected machines and networks to mitigate the threat.

"If a breach does happen, firms need to have a communication plan in place to alert stakeholders and third-party providers," said Hadfield.

Organisations are advised to have an incident response plan in place. This should detail which staff members are in the team, headed up by a key point of contact. Everyone in that team should go through regular drills, such as war games, where simulated attacks are performed to test the network security. Test the plan. Make sure it works. And afterwards, share any lessons learned with the rest of the organisation. Communicate how the team dealt with a breach and the steps they took in responding to it. This will help build a culture of preparedness.

Doyle said that one important element of a response plan is to involve outside counsel that has expertise in cybersecurity issues.

"Having outside counsel that is prepared to deal with regulators and law enforcement officials, should they come to investigate your operational environment, is worth considering as part of an incident response plan," remarked Doyle.

Community defence

One final consideration for fund managers is to begin building a community defence to cyber attacks.

Creating an industry group within the hedge fund and private equity communities that allows for the instantaneous exchange of data – not proprietary data but attack data – allows managers to be better prepared if a fund manager was being attacked.

"There has to be a certain level of trust that those within such a network were only sharing attack data but we are starting to see more of this 'common defence' approach happening.

"Where the world is going is that, in the past, it was always about forensics – who hit me, what did they take, how long were they in my network? The future is diagnostics so that organisations can predict potential attacks," said Steed. If a CISO at a hedge fund were to share the details of an attack with other CISOs in his community it would allow everyone else to raise the drawbridge, as it were.

"The Investment Company Institute has put together a team of CISOs that communicate with each other. They've developed a trusted relationship, and there's a mindset of 'we're all in this together.' I think industry trade groups coming together to help put together a common defence and response programme will be beneficial," said Doyle.

Conclusion

Managers can take a series of practical steps to build an effective cybersecurity programme that needn't be cost-intensive. This could be from identifying their most valuable assets, doing regular due diligence on their service providers, using secure communication tools to share those valuable assets, to staff training and sharing the nature of breach attacks with their peers.

But as Hadfield emphasised: "It has to be a holistic approach that involves everyone across the organisation singing off the same hymn sheet. And then extending that mindset to the firm's wider ecosystem to ensure that their service providers share the same philosophy." ■