Guarding the gates

GPs know cybersecurity is a must for private equity firms, but the best approach isn't always clear. *pfm* gathered five industry leaders to hear how they try to stay a step ahead of the latest threats

by MARINE COLE

photography by DOUGLAS HOLT

From left: Noah Becker, LLR Partners; **Chris Anderson**, KPS Capital Partners; **Nicholas Barone**, EisnerAmper; **Daimon Geopfert**, RSM; **Eldon Sprickerhoff**, eSentire

Cyber attackers have targeted governments, political parties, corporations, hospitals, and universities across the globe in the past year, costing billions of dollars. The financial services industry, including private equity, has also been a prime target for hackers. Yet despite awareness that cybersecurity is a must-have, general partners are often left wondering how best to approach it.

pfm gathered two GPs and three cybersecurity experts on a fall day in New York to discuss the latest popular forms of attacks, the increased scrutiny from limited partners, legislators and regulators, and best practices related to preparedness and response planning.

All participants were quick to note that attackers are getting smarter and acting faster. One of the major changes in the past year has been the boom in ransomware, computer malware that blocks access to a computer system by encrypting files and demands a ransom to restore the data. Increasingly, hackers are also pursuing data exfiltration as part of ransomware.

"The attacks are sneakier," says Eldon Sprickerhoff, founder and chief security strategist at eSentire. "With ransomware, they're evolving their techniques and tactics. They're asking for higher ransoms based on what they believe the firm may be willing to pay, they are folding in facets of data extrusion, and they're setting shorter timelines to pay before the files are deleted."

Another type of attack becoming increasingly common focuses on e-mail compromise. The attackers ask for money to be wired to a specific account in what, at first, may appear to be a legitimate request from a third party or an investor. A few days before the roundtable took place, fund administrator SS&C Technologies was sued by hedge fund client Tillage

Geopfert, left, and Sprickerhoff: Attacks are becoming more common

Commodities, which alleged the third-party vendor acted on fraudulent e-mails and wired as much as $5.9 million from the fund's account to impostors who sent SS&C the messages.

SS&C says the suit has no merit as the thieves purported to be from Tillage and presented valid credentials.

"Now when our phone rings, it's either a ransomware-style attack, where they're just going to deny data and reach out to get payment, or these high-end sleek reaches trying to get an investor's personal funds," says Daimon Geopfert, national leader at RSM.

Private equity being watched

Scrutiny from investors, regulators, and legislators has also increased. Limited partners are paying closer attention to how GPs are preparing for an eventual attack, both during their due diligence and as part of their ongoing monitoring.

"We get these periodic annual questionnaires [from LPs]," says Chris Anderson, chief compliance office and legal counsel at KPS Capital Partners.

> "You must assume that something bad is going to happen, and prepare for that eventuality"
>
> Eldon Sprickerhoff

"Last year there certainly were some questions about cybersecurity-related items but even more so this year. I think the questions are more in-depth."

LPs typically ask questions related to a firm's IT infrastructure and to third-party vendors, as well as whether a GP conducts regular internal audits and penetration testing, which consist of mock attacks.

That said, it's still unclear what investors actually do with the information once they have it. "In many cases, they're asking questions to ask the questions," says Geopfert. "They don't know how to interpret it themselves."

Legislators are also trying to address the issue. The New York Department of Financial Services recently proposed regulations requiring banks and other financial institutions to establish and maintain a cybersecurity program.

Regulators' concern is rising. In May, Securities and Exchange Commission chairwoman Mary Jo White deemed it the biggest risk facing the financial system. The UK Financial Conduct Authority's director of specialist supervision, Nausicaa Delfas, reiterated the point a few months later, saying "cyber is a threat that is ever evolving and ever increasing."

But the SEC's scrutiny of private equity firms' cyber-preparedness is a recent phenomenon. LLR Partners' chief financial officer Noah Becker says cybersecurity wasn't discussed during mock audits or exams a few years ago. It has since become a much more significant focus, and the SEC now conducts exams focused solely on cybersecurity.

"In our preparation for the next upcoming exam, we've been focused on the SEC staff's latest guidance and checklist," he says, referring to the two cybersecurity initiative risk alerts that the SEC's Office of Compliance Inspections and Examinations issued in April 2014 and in September 2015.

Sprickerhoff says that it's critical when assessing a firm's cybersecurity stance to focus on the details found in the September 2015 risk alert rather than the 28 specific questions included in the April 2014 version. "I strongly recommend that each firm carefully review the sentences from the September 2015 footnotes and turn them into questions," he says. That report didn't have as big of an impact with GPs initially because it wasn't in a question form, he points out – but it's the one firms should be paying attention to.

As the threat of cyberattacks and related scrutiny is increasing, GPs' awareness has also intensified. But some private equity firms can be left struggling to figure out exactly what they should be doing.

"Everybody is planning to do something," says Geopfert, but "there's always something that prevents them from doing it. Often they're in the middle of a big acquisition and that's going to be an initiative for later."

Others are actively trying to address the problem.

LLR Partners, which has more than $2 billion raised across four private equity funds, has taken a number of initiatives to bulk up its cybersecurity program. It has worked on segregating its fund investor data and making it accessible only to a narrow group of employees in the firm.

This lockdown approach is critical because by moving the data into one specific area of a network and granting access only to a specific circle of users, it reduces the likelihood that someone, through a user's laptop, will be able to break through the entire network and access sensitive information.

Nicholas Barone, director at

Becker: Staff training is essential as it's 'the insiders that can fail'

AROUND THE TABLE

Chris Anderson is the chief compliance officer and legal counsel at **KPS Capital Partners**, a mid-market private equity firm based in New York with $5.6 billion in assets under management.

Nicholas Barone is the co-practice leader at **EisnerAmper**'s consulting services group focusing on IT security investigation and audit, including managing responses to data breaches and computer forensics.

Noah Becker is vice-president and chief financial officer at **LLR Partners**, a Philadelphia-based lower mid-market firm with more than $2 billion raised across four private equity funds and a focus on investing in growth companies in software, technology-enabled services and healthcare.

Daimon Geopfert is the national leader for **RSM**'s security and privacy services practice, which addresses firms' IT security risks, vulnerabilities, incidents, and data breaches, as well as compliance with regulations and standards.

Eldon Sprickerhoff is the founder and chief security strategist of **eSentire**, which provides mid-sized enterprises with advanced cybersecurity defense services, including managed detection, remediation capabilities, and advisory offerings.

EisnerAmper's consulting services group, says having layered security controls in place is key to preventing attacks like ransomware.

"Firms need to figure out what's going on after hackers get through the first layer," says Barone. "That's why the whole industry has focused on layered security."

Conducting frequent backups can be helpful with ransomware as well. "My experience working with companies hit hard with ransomware is that if you're running a virtual server environment, you can recover quickly and minimize the damage due to a ransomware attack," says Barone.

A backup can also be a lifesaver – as long as the GP knows what exactly was backed up. Geopfert explains that firms need to look at the delta between their last backup and what may have been encrypted and then decide whether or not they are willing to pay.

"When you're running into groups that are victims of ransomware, quite often it's not that they know what was on the computer that got encrypted," he says. "Often, they don't know. All of a sudden they have to decrypt it because they don't know if it was valuable or not."

Ransomware isn't new, but it has become a bigger threat because hackers have found a way to cash in on their attacks thanks to digital currencies.

"Attacks that encrypt files have been around for years, but bitcoin is really the last piece that has helped make it instant," Sprickerhoff says. "It's helped monetize it."

Firms should start building bitcoin accounts as part of their preparation ahead of a potential request for funds, especially because ransoms are getting larger.

"It's really hard to get bitcoins really fast and not in a ridiculously expensive way while remaining anonymous," says Geopfert. "If you're buying $500,000 of bitcoin right now, everybody is going to know why. It turns into this gigantic headache. So now firms are building a bitcoin wallet over time."

> "Firms need to figure out what's going on after hackers get through the first layer. That's why the whole industry has focused on layered security"
>
> **Nicholas Barone**

First call: Firms should contact legal counsel if they suffer an attack, says Barone

When it comes to preventing attacks coming via e-mails, there are a few steps firms can take. At KPS, Anderson has focused on the firm's internal policies and controls including procedures related to wires and how they are processed.

Cash transfer requests should be double-checked, something that could simply be done by requesting verbal confirmation and a signature in addition to an e-mail request.

"You must assume that something bad is going to happen, and prepare for that eventuality," says Sprickerhoff. "There are a dozen broad cyber incident categories, each of which must be addressed in advance within the context of an incident response plan."

But one of the most important element of readiness is training employees on what they should and shouldn't do. "It is really the insiders that can fail," says LLR's Becker.

Employees may be resentful at first if they have to change their passwords every 30 or 60 days, can't access social media on their laptop, or use their own cell phone for work purposes because of privacy concerns. But after several training workshops, it will sink in, experts say. Anderson adds that a firm's broad IT security policy should also include an incident response plan, internal audits, and periodic testing.

"These are all clear things that the regulators have said," he notes, adding that firms need to identify specifically what types of risks they are exposed to. Firms investing in the healthcare sector are typically at greater risk of an attack

as they often hold sensitive privacy data. Those utilizing third-party vendors and sharing information with them also carry an extra layer of risk.

Responding to an attack

It can take time for a private equity firm to realize it has been hacked. But if a GP has been the victim of ransomware, a pop-up message would usually walk the firm through the necessary steps to pay the ransom.

"The instructions are usually right in the pop-up," Geopfert says. "They have very detailed instructions on how to contact the hackers. They have links out to open-source guides and they will tell you how to communicate with them, whether it's anonymous e-mails, online chat rooms or even in some cases through Facebook or Twitter."

In any type of attack, firms should first determine whether there was technically and legally a breach of their network, the definition of which differs according to the different jurisdictions. If there is an actual breach, firms should contact the following three parties before acting on the request: their external legal counsel, their insurance company and the forensic investigation company they have on retainer.

"The typical thing to do is to contact your outside legal counsel first to cover yourself under legal privilege and create a legally defensible position," says Barone. The external legal counsel will also be able to determine whether there was data exfiltration in a ransomware case, which will later assist when dealing with a GP's insurance company, and whether the firm should pay the ransom. Additionally, if a group requesting a ransom has been attributed to funding terrorism, the firm could be liable if it were to pay the ransom, something to discuss with an external legal counsel.

The mounting cost of cyberattacks has also heavily impacted insurance companies, which are now taking several measures to assure they manage claims and losses.

Action plan: Firms need a response plan, internal audits, and testing, says Anderson

> "It's basically as if [insurance companies] are doing the due diligence exercise on you and your internal controls"
>
> **Chris Anderson**

"The insurance companies are now putting the onus back on their insureds to get more information upfront as part of the claims process. When you call in the forensic investigator and your lawyer, the bill and the clock starts running," says Barone. "Being unprepared leads to higher costs. They're almost saying, 'Now go in and do your own internal assessment. Demonstrate to us that you should be bringing in these people instead of the opposite.'"

Geopfert agrees, saying insurers are becoming a lot more careful of the IT firms GPs may have on retainer in case of an attack and that, increasingly, insurers have a preapproved list of forensic investigation firms.

"Most of them have a list of between three and 15 companies," he says. "If you pull the alarm and a responder comes and starts charging half a million dollars in bills and the insurers didn't preapprove them, they're not going to cover the fees."

As a result, cyber insurance policies are becoming more convoluted, with additional covenants and inquiries to firms on their level of preparedness, and often extra basis points on the policy based on the robustness of a firm's cybersecurity program.

"Even in the application, it's basically as if they're doing the due diligence exercise on you and your internal controls," says Anderson. "It's four, five or six pages long now."

At a time when private equity firms are already being hit by increasing compliance requirements and costs related to business continuity, fees and expenses reporting, and standardization, cybersecurity has emerged as yet another major burden for GPs. But it has also become indispensable as the threat to the industry grows. ■