Upping the ante

Staying ahead of the curve on cybersecurity is no easy feat, especially as hacking methods grow ever more insidious. pfm gathered six industry leaders to discuss best practices, managing third-party risk and keeping up to snuff with the regulator

by MARINE COLE

photography by LEA RUBIN
When three mid-market private equity chief financial officers and three cybersecurity experts met in New York in late September, cyberattacks were making the headlines.

The hack on credit reporting company Equifax and its dire consequences for Americans were being exposed to the public. And just days after our roundtable, Securities and Exchange Commission chairman Jay Clayton disclosed that its public-company electronic filing system, EDGAR, had been hit last year, resulting in illicit trading. On the same day, Clayton reiterated the importance of constant vigilance to protect against intrusions as the scope and severity of risks that cyber threats present have increased dramatically.

The private equity industry has taken the threat seriously, upping preparedness and increasingly responding to inquiries from investors and regulators alike. But with restricted resources, both human and financial, and attackers that are always honing their skills, it has become a constant challenge for mid-market firms in particular to stay up to date on proper cybersecurity readiness.

Take CCMP Capital Advisors. To stay up to speed, the mid-market private equity firm – whose most recent fund raised $3.6 billion – has conducted penetration testing to verify the vulnerability of its network through a third-party provider. It continues to train new and existing employees and it has bought cybersecurity insurance in the past 12 months after more than two years of mulling the...
purchase, among several additional new steps.

“This year we really ramped up a lot of our policies and documentation,” says Dina Colombo, CFO of CCMP. “The thing that’s most challenging is that it’s constantly changing. As the hackers get smarter you have to navigate what’s next and try to be ahead of the curve and it’s very difficult to do that.”

Indeed, hackers have kept refining their work and continue to focus on ransomware – but with added twists.

Daimon Geopfert, national leader for RSM’s security and privacy services practice, explains that ransomware is shifting from simply encrypting data on the first system it touches into a process in which attackers spend time in a network to identify the most critical systems and processes and then manually deploy malware on those systems.

“The second you realize you have a ransomware issue, it’s already in the most painful spot it could get to in the environment,” he says. “It’s still ransomware but with a completely new devastating twist on it. We’re almost in the worst-case scenario right now. We’re watching the higher-end hacking skills mixed with ransomware and it’s creating a new hybrid model that’s designed to force organizations to pay a ransom or face end-of-going-concern type of damages.”

In the spring, a major ransomware attack dubbed WannaCry demonstrated the increasing sophistication of hackers as it infected hundreds of thousands of computers in at least 150 countries. It’s not known whether private equity firms were victims of the attack.

Third-party risk

Ivane Chou, CFO at lower mid-market firm High Road Capital Partners, in addition to making sure the appropriate systems are in place, also spends an increasing amount of time focusing on third-party risk. When High Road registered with the SEC in 2012, it produced a one-page, 15-question
checklist annual certification for its service providers, but she quickly realized her firm might have to do more to monitor data breach risk coming from third parties.

“Monitoring our service providers is constantly on my mind,” she says, adding that feedback has been mixed. “In the last year, we’ve been trying to probe them. Some of them are getting up to speed and providing more information, but some of them are pushing back. It’s a tough point.”

The risk isn’t limited to service providers, but also extends to fourth parties who also have access to sensitive information, as vendors usually outsource parts of their business.

There are some tools at firms’ disposal to monitor third-party and fourth-party risk but they have their limits.

“The industry is coming around to a cybersecurity score, like a credit monitoring score,” says Anurag Sharma, principal with Withum Smith+Brown.

“There are a couple of companies that have come up with a similar concept where they would give an organization ratings on their security. The score in not an industry standard yet but it is better than nothing. It gives you some insight on the service provider.”

That said, the score is only an indicator, and it takes into account all attacks – even those caught by a firm’s security system and those occurring on a firm’s guest Wi-Fi network – when determining the provider’s score.

The American Institute of Certified Professional Accountants also provides a reporting framework called system and organization controls, or SOC. Part of that is the SOC 2 report, which provides detailed information about an organization’s controls relevant to the security, availability and processing integrity of the systems it uses to process user data. The report

### AROUND THE TABLE

- **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 the vice-president and chief financial officer at LLR Partners, a Philadelphia-based lower mid-market firm with $3 billion in assets under management and a focus on investing in growth companies in software, technology-enabled services and healthcare.

- **Dina Colombo** is managing director and the chief financial officer at CCMP Capital Advisors, a mid-market private equity firm. CCMP was established in 2006 and typically invests $100 million-$500 million in companies ranging from $250 million-$2 billion in size.

- **Ivane Chou** is the chief financial officer and chief compliance officer at High Road Capital Partners, a lower mid-market firm that seeks to acquire controlling positions in niche-leading manufacturers, service providers, and value-added distributors in the US and in Canada.

- **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 and regulations and standards.

- **Anurag Sharma** is a principal at Withum Smith+Brown’s cybersecurity consulting and service organization control practices, and is also a designated SOC 1 and SOC 2 specialist by the oversight task force of the American Institute of CPAs’ peer review board.
also assesses the confidentiality and privacy of the information in these systems.

In addition, since April the SOC has also allowed organizations, including third-party providers and portfolio companies, to communicate relevant information about the effectiveness of their cybersecurity risk management program.

“A [certified public accountant] can come and look at your cybersecurity practices and issue an opinion,” says Sharma. “It is very much in line with how an opinion is issued on a financial statement. I think that’s a tool that will see a lot of traction in the market in the next couple of years.”

In addition to focusing on securing fund and investor-related data that can be attacked directly and via vendors, private equity firms need to monitor new and existing portfolio companies and third-party vendors they may be using. Cyberattacks could incapacitate a portfolio company’s proper business function and prompt losses for a private equity investor, which means that more than ever, deal teams need to incorporate cybersecurity into their due diligence of companies.

**Regulatory watch**

Over the years, the cost of maintaining proper cybersecurity at private market firms has also been driven upward due.
to heightened scrutiny from regulators around the world.

In May 2018, the EU will start implementing its general data protection regulation (see p. 33), which is applicable to all firms with links to Europe, including operations, business or employees in Europe. It dictates securities and controls around personalized identified information and imposes stiff fines for violators.

As the implementation date inches closer, US firms are actively considering whether they would fall under the GDPR’s scope. At LLR Partners for example, CFO Noah Becker plans to assess the firm’s limited but expanding connections to Europe to determine to what extent the regulation applies and if so, to what extent modifications to existing data security are needed.

In the US, the SEC and state regulators have also reinforced their work on cybersecurity.

“The SEC and the state regulators are increasingly questioning fund managers,” says Nicholas Barone, co-practice leader in EisnerAmper’s consultancy services group, adding that he’s seen fund advisors as small as those with $250 million in assets under management being targeted. “They want more transparency into operations. They’re focusing on policies and procedures. They’re focusing on third-party and fourth-party risk.”

Barone explains that the first question typically coming from regulators is whether a firm has an incident response policy, followed by whether a firm conducts readiness tests. Firms often fail to answer those questions appropriately, he says, leading to remediation and fines but rarely to enforcement.

With so many moving parts, it can be a challenge to keep abreast of the changes, even as a private equity firm’s cybersecurity programs mature.

Like many of its peers, LLR Partners has been focused on cybersecurity since registering with the SEC in 2012 and has mainly focused on completing specific point providers and on documentation but more recently it has taken its cybersecurity plan to the next level.

“Now we’re looking to evolve our masterplan, by formalizing the cadence of different internal controls and more fully documenting our organization-wide cybersecurity protection strategy,” Becker adds. Nevertheless, “the more you work through this, the more comfortable you get, but also the more nuances you realize you still have to address.”

“ The industry is coming around to a cybersecurity score, like a credit monitoring score... It gives you some insight on the service provider”

Anurag Sharma