KEYNOTE INTERVIEW

Meeting cyber-risks from third parties head on

Third-party service providers and portfolio companies present some of the greatest cyber-risks. But firms can protect themselves, says Agio's Kirk Samuels

Anyone managing money has a target painted on their backs when it comes to cyber-attackers. The Securities and Exchange Commission knows this, and has made it clear that it wants private funds to be on the top of their cybersecurity issues.

But, of course, it isn't just the firms themselves that cyber-criminals target – third-party service providers and portfolio companies present risks to firms, as well.

Kirk Samuels, executive director of cybersecurity at Agio, spoke with *Private Funds CFO* about what compliance with the SEC's cybersecurity expectations means, and how to identify and mitigate risk stemming from third-parties and portfolio companies.

SPONSOR
AGIO

Q How does Agio help clients approach compliance with SEC expectations?

Agio offers an SEC governance program for our clients, which is in line with the SEC Division of Examinations' Risk Alerts. We make sure that firms are discussing what the SEC is reviewing in the risk alerts, and have solid governance with respect to them. We also ensure that the firms are progressing in their cybersecurity maturity. So if we performed a security risk assessment or penetration testing, we will ask if and how they plan to address them with corrective actions. We further partner with our clients by holding monthly governance calls led by a virtual chief information security officer, who will discuss general threats that we're seeing across the industry and ways that other firms are dealing with them and how they protect investor data.

Q How can firms monitor and mitigate risks from third-party service providers?

Outside of the firm, vendors and other third parties are the two biggest risks overall. Vendors and other service providers who manage any type of investor data need to really be examined to understand how they're securing that data in transit, when it's being stored, what

happens to it when the contract with the vendor expires and how has it been safely destroyed or transferred back to the firm. At Agio, we often address this through multiple controls depending on the level of risk involved, but at the very least a due diligence questionnaire with the vendor. The more sensitive the data or the more critical the services that they're delivering, the more questions they need to answer with regard to the safeguard of those data and systems.

Mitigating third-party risk is not a simple task. For instance, a vendor may not carry out their written policy such as always anonymizing data when they move it into a test environment. All it takes is one person not doing that one time. We've seen breaches like that happen, so you need to be aware of who's following their procedures. Also, pay attention to the breaches that are out there that can impact the firm and make sure that there are agreements within the contract about when you're notified of any potential breach.

Another layer of risk is added when there is a fourth party involved with the service provider. In order to understand what risk exists, some firms will ask to perform external scans on third parties who have critical data, or make sure they're reviewing periodic penetration tests or Service Organization Control 2 reports.

Q How about at portfolio companies?

When it comes to firms' investments, different firms take different levels of involvement in their portfolio companies' cybersecurity. Fortunately, we are seeing an overall increase in that involvement due to the risk that threats like ransomware or non-compliance with regulations like CCPA or GDPR can pose to their overall investments.

To that end, there's a growing need for cybersecurity due diligence throughout the investment life cycle – not just during the initial due diligence period, but once the firm has taken an ownership stake in that company. The firm should be monitoring the risk of a cybersecurity breach or gaps in cybersecurity compliance at the portfolio company. It's especially important to make sure that, when the risk is at its highest, the greatest controls are put in place. Typically, that's when you're getting ready to sell the company or do an IPO, since a breach before an exit would have potentially very serious consequences.

Agio offers portfolio company assessments for our private equity firm clients. We can offer to set up a program with the portfolio company to help them with their on-going governance, which includes an initial 24-month period to meet the SEC requirements, then continued governance to maintain compliance and mature their cybersecurity to address evolving threats.

We also have a team focused on the payment card industry data security standard, which really benefits a lot of the portfolio companies we work with. Additionally, we have a healthcare-focused team who can help some of the portfolio companies that are working in health or medical technology, and we also have teams focused on higher education and municipal government.

Q As many firms start to head back to their offices, what should they be aware of?

Firms will need to identify changes in behavior through an extended detection system to account for the shift from the way things were happening to the way they are now – making sure that that new behavior is accounted for and addressed – to validate that it is legitimate.

With extended detection and response, we look at all of the sources of data logs across the enterprise – whether it's from laptops or servers, from the cloud or from email systems – and we aggregate all of those logs and data and look for activity. We then determine whether those activities are standard, normal activity for the firm or abnormal activity. When we see something that deviates from what we would expect, we alert the appropriate person and sometimes go through an incident response process, identifying how to handle that particular alert.

Q What cyber-threats do you see in the private funds market most often?

When it comes to portfolio companies, ransomware is one of the main threats we're seeing, and that can obviously impact the private equity firms themselves. Any organization's best protection against ransomware is to ensure that the portfolio companies have strong backups that have been tested. Additionally, it's crucial for firms to institute some form of network segmentation, limiting how that ransomware can spread throughout the company.

The next largest threat we see are phishing and business email compromise attacks. When it comes to the alternative investment area, wire fraud is the end result of a lot of these attacks. In BEC attacks, there's often a bad actor impersonating a C-level executive, in order to get someone to transfer large sums. Often the bad actors will insert themselves into the conversation and divert those funds to their own accounts.

The best protection against these threats is to never trust email, especially for anything that's sensitive or that involves a large amount of money. If you're a private equity firm and transferring large amounts of funds, use some other method to verify the information. Set up your process ahead of time with all the parties involved and have secondary methods to communicate with each other. We have one client firm that will only authorize large payments with a video call, and they establish ahead of time what the relevant party looks like, and the number that they're going to communicate with them on. The reason they've gone to that extreme is they fell victim to a wire fraud. We see that the firms that are maturing the most are either learning from their own mistakes or, hopefully, learning from other people's mistakes. ■