PRIVCAP REPORT/

Sponsored by
RSM

Cybersecurity:
The New Due Diligence

THE NEW DUE DILIGENCE

Private equity firms continue to include cybersecurity as part of their overall risk assessment

By Marc Raybin

For private equity investors, cybersecurity is quickly becoming a significant part of the portfolio company acquisition process. Not only must firms ensure the protection of customer data and sensitive, proprietary company information, but neglecting the threat of a data breach can also run afoul of several federal agencies.

"What we try to coax a lot of our clients into understanding is, there's the security at the fund level itself, at the portfolio level, and then the interaction between the two," says Daimon Geopfert, national leader, security and privacy consulting, at RSM. "A lot of funds will come back and say, 'We don't contain a lot of sensitive data. We don't have access to a lot of sensitive systems.' Usually, on review, they have more than they think, and they always seem to forget that they are also an entry into some of the portfolio companies."

Geopfert says most cyber attacks are crimes of opportunity, and private equity firms that think they're not targets should think again.

"Most breaches are actually targets of opportunity," he says. "They didn't come looking for you specifically; you just happened to be vulnerable. They took a shot at you and then realized later who you were."

One of the most common misunderstandings of cyber attacks is that organizations assume they will know very quickly that they've been breached. But Geopfert says the number of days it takes to discover a breach is between 200 and 300 days. By then, lot of the damage is already done.

"It is an emerging focus of businesses around the world," says Prakash Mehta, a resident expert on cybersecurity at international law firm Akin Gump.

According to Scott Larson, a former FBI special agent and founder of Larson Security, private equity firms are trending toward making cybersecurity part of the early stages of due diligence. In fact, he predicts it will become the norm in the next two to three years industry-wide.

Larson, who led the FBI's computer investigations and infrastructure protection program as a supervisory special agent before founding his security firm, has seemingly seen it all. An

➜ CONTINUES ON NEXT PAGE

immediate red flag includes IT groups that are hostile when questioned about processes.

"There are weaknesses they do not want exposed," Larson explains. "There is something they are hiding."

Larson has discovered completely unmanaged systems without any patches. This would indicate a serious problem for any acquirer, he says.

On the client-facing side, things look good, but Larson says, "On the back end, they are in disarray."

His team typically embeds itself with the IT department of the portfolio company for up to six months to run full diagnostics on systems. He runs a "health checkup" on networks, providing acquiring companies with full risk assessment.

Larson is finding that the savvier the management team at a private equity firm, the sooner they will conduct cyber due diligence when making a new investment. Mehta stresses an even deeper dive than focusing on the portfolio company; instead, he counsels clients to create a map of every third party that has access to the firm's sensitive data, including vendors and suppliers.

"You cannot just protect on your end," says Mehta. "How strong is the cybersecurity with those who have your information?"

Geopfert agrees.

"We've seen a wide array of attacks, over the last year or so, of organizations that get breached through some related body," he says. "So an attacker breaches them and then works into that company. And so we're starting to see those styles of attacks at the fund level. But it really is [about] understanding their own security, the security of their portfolio companies, and then how they track that over time. How does it get reported back up, and how do they manage their risk?

Indeed, the SEC recently reported uneven levels of cybersecurity preparedness. According to a report issued by Akin Gump that reviews the government watchdog's findings, third-party due diligence is key. Cybersecurity insurance is also an important step to be considered.

"There are significant opportunities for improvement," according to Akin Gump's report.

Taking a total, comprehensive approach to information technology is key to maintaining security. It is not just one network or component; it is the system as a whole that needs to be tested consistently.

The number one way for an organization to protect itself from a breach is to guarantee that a data-protection strategy is in place, says Darren Guccione, CEO of Keeper Security, Inc., a provider that helps clients password-protect sensitive data files. The strategy is to ensure that all sensitive data is encrypted and that proper controls are in place to permit access to that data. The policy is consistently tested and audited for effectiveness in preventing data loss from both external and internal threats, Guccione adds.

"Centralized management of enterprise-wide access, threat-detection systems, external and internal security auditing systems, and the ability to securely share sensitive information and credentials are all key components of an effective data-protection strategy for any enterprise," he says.

For private equity, the potential damage a cybersecurity event can have for firms is exponential. For instance, a disgruntled employee could provide sensitive data in order to torpedo a deal, Larson points out. And if a hacker breaks into the firm's network, that person would gain access to LP information.

Mehta takes it even further, suggesting the intruders could force a wire transfer from the firm's pools of capital. Mehta has yet to see a successful dummy transfer, but he has seen them foiled. That means it is currently happening.

Cybersecurity for private equity firms is often a more intense process, typically in a shorter time frame, Larson explains. That means providing the initial screening in the first 30 days and then embedding with the firm's IT department for six months to a year. Working with private equity clients often means the stakes are higher than in other industries, because the goal is to provide a full assessment of the IT security without negatively impacting a deal for a target portfolio company.

And while a full assessment of a company's cybersecurity is quite expensive, the alternative could cost considerably more.

"With the multiples being so high right now, there's a lot of money at risk," says RSM's Geopfert. "When you're buying into those, you are accepting that you are buying right now at a huge premium. We're working with private equity groups that are very heavily invested in industries having to do with healthcare, health insurance, health providers, retailers—anything along those lines. If that is breached when they buy it or right afterwards, they can lose that entire investment."■

Click to watch this video at privcap.com

The Threats Every GP Should Understand

Cybersecurity has become a major area of interest for private equity firms, at both the firm and the portfolio company level. Daimon Geopfert, a principal in RSM's Risk Advisory Services Group, says that firms should act as if a cyber-attack is a matter of "when," not "if."

Daimon Geopfert
Risk Advisory Services,
RSM

➜ BIO

Geopfert is the national leader for RSM's security and privacy consulting practice. He has more than 17 years of experience in a wide array of information security dis-ciplines, including penetration testing, vulnerability and risk management, incident response, digital forensics and investigations, and secure software development. He has managed the development and implementation of security polices for multiple U.S. Department of Defense entities, and has deep technical experience with vulner-ability identification and remediation, secure architectures, and regulatory compliance. Geopfert received a B.S. in computer science from the United States Air Force Acad-emy, and a M.S. in computer science from the University of Michigan.

What are some of the most obvious things every GP should know about cyber security?

Many firms mistakenly think they are not targets for cyberattacks, but what they need to know is that hackers are opportunists. They may not be out look-ing for you or even know who you are when they breach your systems. If there's an opening they will exploit it, and then figure out later what to do with the data they've stolen. There's always a buyer.

What are the specific risk areas? Are they after financial information or customer information, insider trading information?

All of the above. If you put it in order of preference, attackers are looking for credit card information, which is very valuable for obvious reasons. But don't forget, PE firms are also entries into portfolio companies, and if there's an imminent sale or acquisition planned, that information can be used for insider trading schemes. There's so much data that companies don't even realize they have until it's out there.

How difficult is it to try to decipher where an attacker got into the system?

It's gotten extremely difficult. Attack-ers have gotten very, very sophisti-cated on some of the initial breaches,

➜ CONTINUES ON NEXT PAGE

"If there's an opening they will exploit it, and then figure out later what to do with the data they've stolen. There's always a buyer."

–Daimon Geopfert, RSM

where they don't leave as many breadcrumbs as we normally would look for. For instance, evidence can exist in only memory resident, meaning it never gets written to disk on the computer. And the first thing people do when they start thinking there's a problem is to reboot all the systems. Well, that destroys all the evidence. When hackers get in, the first thing they do is move laterally. They try to spread out and get as many channels back in, just in case they're booted out of one system or another. If we're lucky, they'll use the same techniques on each system, so once we figure out the signature for one, we can look on multiple systems and try to get them out of the environment. The really experienced attackers will put in a slightly different style of back door entry, hoping that the security teams won't recognize all of them.

How sensitive do you and also the private equity firm have to be to the portfolio company's existing IT personnel?

It's difficult because at a certain point you're under the gun to get it done one way or the other. And a part of that is understanding your relationship with those portfolio companies, so when we work at the fund level and start coming down to the portfolio companies we almost always scope out and do a personality check. Before we go in we understand who we are talking to. How do we talk to them? How will they respond? Some people take that type of very direct assessment well. They want someone to come in and say, "This is exactly the issue. This is what you need to do to fix it. Go!" Others, when you do that, they interpret it as, "I'm doing a bad job," and they get very sensitive about it. What you're more worried about are the ones who take it as a personal insult, to the point that now they could become an insider threat.

What's the first course of action a firm should take when they suspect that they've been breached?

Stop touching stuff. There's nothing more frustrating for instant responders than when we show up to find out they've trashed all the evidence. Rolling logs, rebooting systems, or reformatting discs will wipe away any trace of the attacker's entry, but that doesn't mean they're not still inside. If you are there, keep it as pristine as you can. Call in somebody who knows what they're doing, and the next call is probably your lawyer and insurance company.

When auditing a portfolio company's IT that hasn't been breached yet, where do you often see red flags?

Ninety percent of your security risk comes back to your data. When we walk in and in the first 10 minutes we're asking questions like, "Where is the sensitive data?" and you start getting answers like, "Kind of here, kind of there. Some over there," you ask who has access to it. Everybody. At that point, you've already lost the battle because if an attacker gets in, they can find copies of data essentially everywhere.

The other issue we're looking for is whether they understand the concept of depth. A lot of groups we talk to say they feel confident in their security because they have all of these preventative controls, firewalls, patching, and other measures to try and keep people out of the environment. But modern attackers thrive on bypassing those and getting in. So what we ask about is their detective and corrective controls. If they're stuck at that preventative layer, and they don't understand the concept of depth, it is a big red flag.

What is the safest way to protect your data?

Understand where the data is. That's it. Any information out there can be compromised. Period. And when you're talking about what the most common areas of failure are—it's people. The biggest data breaches of all times are people leaving laptops in the back of taxis, on thumb drives and backup tapes.

And then there's the proliferation of social engineering attacks. For instance, one of your employees gets an email with a false UPS tracking number, and they click on the link, not realizing that it's going to a website that's hosting malware. If the operating system or the browser they're running is missing patches, or they're missing patches in Java, QuickTime, Adobe, or anything else that's running when they hit the website, the malware can take over the computer. Now the attack is sitting inside and that's really a human error. ■