Privcap/
Context for Private Capital Investment
TRANSCRIPT

Cybersecurity: The Threats Every GP Should Understand
With Daimon Geopfert from RSM

Mike Straka, Privcap:

Welcome to Privcap. I'm Mike Straka. Cybersecurity has become a hot-button issue in private equity, both at the GP level and the portfolio company level. Joining me now to talk a bit more about this is Daimon Geopfert, the national leader of security consultant at RSM. How do you define cybersecurity on the private equity level?

Daimon Geopfert, RSM:

As you would guess, it's a bit nuanced. What we try to coax a lot of our clients into thinking is—there's the security at the fund level itself, at the portfolio level, and then the interaction between the two. So a lot of funds will come back and say, "We, ourselves, 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 entrée into some of the portfolio companies. We've seen a wide array of attacks over the last year or so of organizations that get breached through some related body. An attacker breaches them and then works into that company. So we're starting to see those styles of attacks at the fund level. But it really is understanding their own security, the security of their portfolio companies and then, how do they track that over time? How does it get reported back up and how do they manage their risk?

Straka: What are the specific risk areas? Where do you see the targets happening? Are they after financial information or customer information, insider trading information, things like that?

Geopfert: All of the above. There's obviously the ones that are going to make it into the press and get the most focus. Attackers are pure targets of opportunists, if anything. If they can find something, they'll take it and they'll figure out how to monetize it later. There really are a very small number of groups that actually go out only looking for one type of data. That's abnormal. Most of them are going to breach somebody because they can. Once they get in, they're going to figure out, "What can I get to? What can I have access to?" They'll steal everything and then sell it off later.

In order of preference, though, credit cards are always going to be top of the heap. If you've got anything to do with retailers, because they're simply just easier to sell. After that, there's a whole second tier of customer PII—personal identifiable information. Anything they can get to—financial information. The ones that never make it into the news as part of these breaches are the attackers. While they're in stealing all this sensitive data that you have to notify and it makes it into the news, they get into the corporate bank accounts—ACH and wire transfer money out, stuff like that.

You've seen a huge attack on health records recently, in health insurance. And then we're starting to see (it's been rumored for the last several years but hard to prove) stuff that they can trade off. For example, if someone's going to buy a company and take it private—stuff like that. Or for publically traded companies, that they can get in and see their quarterly and financial statements before they go public so they can sell it to somebody, get on the right side of the trade. It's really its own ecosystem at the moment.

Straka: I'm sure being a programmer, [with] the IT experience you have, it's easy for you to find out how they got into a certain system. But is it easy to find those back doors they create once they're in there?

Geopfert: I would actually push back. It's gotten extremely difficult in some cases to figure out how they've gotten in. They've gotten very sophisticated on some of the initial breaches, where they don't leave as many tell-tales as we normally would look for. They'll put stuff in that's 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 reboot all the systems. Well, that destroys all the evidence.

When they get in, the first thing they do is what we call "move laterally." If they get in, they're usually on one system at a time. If that system gets cleaned up, taken down or whatever, they're back out of the environment. So the first thing they do is try to spread out and get as many channels back in. That is a crap shoot, to put it nicely. 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. The very experienced attack groups—for each system they compromise, they'll put in a slightly different style of back-door, hoping that you might find five out of 10, but they can still get back in.

Straka: Do you and all the private equity firms have to be to the portfolio company's existing IT personnel? Because obviously, people have egos and you don't want to go in there and say, "Dude! You got some major problems in your system." How do you walk that line?

Geopfert: It's difficult because at a certain point you're under the gun to get it done one way or the other. And, as part of that, you have to understand your relationship with those portfolio companies. So when we work at the fund level and start coming down to the portfolio companies, we almost do a scoping and personality check with everybody before we go in: "Who do we talk to? How do we talk to them? How do they respond?" Some people take that type of very direct assessment very well. They want someone to come in and say, "This is exactly the issue. This is what you need 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 is the ones that take it as a personal insult, and now they become an insider threat, let's put it that way. They might have some angst about what you said.

Straka: So, if a PE firm suspects that they're under breach, what should they do first?

Geopfert: If you are there—hands off, stay as pristine as you can. Call in somebody who knows what they're doing. And the next call is probably [to] your lawyer and insurance company.

Straka: Is there a way you can still operate while under attack? Would you recommend redundant systems in other data centers somewhere else, storing stuff on a cloud? How do you continue to operate when your main systems are being attacked?

Geopfert: You're almost always going to have to operate while breached. There are very few organizations—I've only been involved in four or five in my entire career—where it has been so dicey that they simply said, "We're done." And they kill their network connection and are separated from the Internet. It's extremely difficult to do that. What you're normally going to do is, if you're under breach—if you've prepared for it correctly and you've isolated the data, you know where it is, who has access to it—you basically put the screws down. You make sure that data is almost impossible to access, except for exactly what is needed.

Straka: Let's say you're auditing a portfolio company's IT that hasn't been breached yet. Where do you see red flags?

Geopfert: The big one is always—we'll talk about situational awareness. We show up for a group and they say, "Come in and talk to us about security." Okay, let's do so. Before we talk about security—90% of your security risk comes back to your data. What data do you have? Where is it? Who has access to it? When we walk in, 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, but there's copies of it everywhere." Well, who has access to it? "Everybody."

At that point, you've already lost this battle, because what it means is if an attacker gets in, they can find copies of that data essentially everywhere. And we try to guide them to understand what that data is, who needs it and what the value is and lock that down as small as possible.

Straka: What is the safest way to protect your data?

Geopfert: Understand where the data is. That's it. Any technology you're going to throw out there—[like] what if I did this?—there is an attack that will compromise that. Period. When you're asking what are the most common areas of failure? [It's] people, by far.

So never forget it. We keep talking about all the sexy hacking and everything that goes with it. The biggest data breaches of all time are people leaving laptops in the back of taxis, thumb drives, backup tapes—stuff like that. That still happens. Even though that's become more rare, people are still the biggest failure because of the proliferation of social-engineering attacks. One of your employees gets an email [saying], "Here's this UPS tracking number." And they click on the link not realizing it's going to a website that's hosting malware. 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. They hit the website. It takes over their computer. Now, the attack is sitting inside and there's really a human error. The attacker didn't throw an exploit—the employee went out and got the exploit and brought it back.

Straka: What government or regulatory agencies are putting the screws down on PE companies and portfolio companies to really make sure they're secure?

Geopfert: Well, you're going to have two different pieces. The portfolio companies are going to be much more industry-focused, so you're going to see Department of Health and Human Services. If they're

retailers, you're going to see the PCI Council. You're going to see a lot of stuff at the portfolio company that they are facing. Then, at the PE level, you're going to have the SEC and, depending on some of the others, what's going on. But the recent SEC OCIE cybersecurity initiative caught a lot of people by surprise. They've already come out with a first round of announcements. It was very interesting. They publicly said—they came out and it was more of a questionnaire and discussion format. They didn't do technical validation of the answers they were getting. So a lot of the percentages we saw—and there were people saying, "Yes, we have this program, this technology, we do this"—were higher than a lot of us would have guessed it would have been. I'm curious what it's going to look like in the future when the SEC actually starts to validate the data.

There's a lot of money at risk. I mean, when you're buying into those, you are accepting that you are buying right now at a huge premium. We've got industries where we're working with private equity groups that are very heavily invested in anything to do with healthcare, health insurance, health providers, retailers—anything along those lines. They understand they could buy into that, and if that is breached when they buy it or right afterward, they can lose that entire investment. When you're paying huge multiples for these and you're looking at buying a source of fines and lawsuits, adding security into these is now making the valuation process much more valuable to them in that space. As an example, there was one on the West Coast a couple of years ago where they bought a group that was writing a video game. When they acquired it before the video game went out for sale, they didn't know that a group from China had already breached them and stole the source code for the video game. So before they could get the video game to market and start to recoup their investment, the group out of China had basically gone through and just changed the name and were reselling it already at a much lower price. So they basically bought a goose egg. So a lot of people are rolling security in, not just for the protection of the investors or the fund itself. They're trying to identify issues before they bring stuff into the portfolio.