Expert Discussion

# PE Value Creation Through Cybersecurity

## An expert conversation about how GPs can protect and add value via data security

SPONSORED BY RSM

**Eric Feldman**
Chief Information Officer
The Riverside Company

**Kevin Carpenter**
Director, Risk Consulting
RSM US LLP

**Privcap: How do you approach cybersecurity from the perspective of value creation?**

**Eric Feldman, Riverside Company:** We tackle this head on shortly after an acquisition, many years before we're even talking about an exit. We've developed a program internally; since we invest in the lower mid-market, it was initially created to help educate our portfolio companies about some of the threats that impact smaller businesses. What it's evolved into something that's now fully operationalized across a number of our funds. Within that first hundred days, roughly, we work with a few third parties, but we do an entire evaluation and it's based on the NIST framework, the National Institutes of Standards and Technology.

We're looking at risks related to ransomware, data breach, impersonation attacks, and business email compromise. By the time that we're at the table with an investment banker or a buyer, should the topic of cyber come up, we have a pretty nice way to report on some of the work that we've been doing. There have been a number of cases where the actual reports themselves are introduced into the conversation.

**Privcap: Kevin, what are your clients looking for when putting a number on the value of cybersecurity readiness and capabilities?**

**Carpenter:** Eric hit on a number of great points that we're seeing in the space right now in terms of adding value during the hold period, but also starting that off and making sure that you understand what you're inheriting. It's like a home inspection, if you will, but really getting inside and taking a look around and making sure that the reason that you're actually looking to acquire the target is sound and secure.

We've seen time and time again where, at least a due diligence perspective, a lot of that information can potentially change the outcome of the reps and warranties calls, can change even the deal structure from a funding perspective. It's becoming more commonplace.

Something that is definitely showing its value is when looking to exit. Historically, it's really been tough to tie directly to the bottom line. Today, that type of diligence, which was once seen as overhead, is now part of the conversation given its potential to destroy—or create—value.

**Privcap: Does doing this type of analysis, even if it's focused around threats and vulnerabilities, often lead to a more efficient and profitable organization?**

**Feldman:** Absolutely. It's a huge benefit. For example, a lot of times after we make an investment, we have already identified during due diligence that they're running email on a server that's sitting in a closet somewhere. That's just ripe for a whole host of problems. One of the things we work with our companies on is to immediately transition into a cloud service. We don't really need or want them to be in the hosting business. We've killed two birds with one stone, if you will, from a pure efficiency perspective. And we're then able to apply some pretty good security practices around that system, such as multi-factor authentication.



↓ CONTINUES ON NEXT PAGE

**Carpenter:** What we're seeing, too, is that for any company, it's difficult for them to know what they don't know, if you will. Having somebody that you can partner with to come in and take a look at that and provide some of those alternative solutions, to either leverage economies of scale across the portfolio potentially within licensing, or to understand what is some of the options from a managed provider perspective, is extremely valuable.

The point that I want to stress is while we do utilize governing frameworks and standards for this, these aren't audits. These are assessments. The biggest difference to that is that you're able to really get into the recommendations afterwards and craft those in such a way that it does bring value. It is forward looking.

**Privcap: Given the incredible amount of data out there, how much is privacy factoring into your overall analysis?**

**Feldman:** Our European companies really started to evaluate and start thinking about that, probably a good, I don't know, 12 to 10 months before GDPR went live.

**Feldman:** I think it came as a bit of a surprise for a number of our US companies that this also impacted them. Now with the CCPA in California, which I think is set to go live sometime in 2020, we have spent roughly the last 10 months educating our affected companies about its implications. Our operating teams are focused on it. A number of our companies have worked with third parties to help them build privacy programs that are continuing to grow and are supported today.

**Carpenter:** It's not going away, unfortunately. It's only going to continue to ramp up in importance, in scrutiny. We've historically seen the focus on security and putting in place a proactive program as opposed to a reactive one. Privacy is no different. And this is the one area where you are potentially liable for fines and depending on your exposure there, that's a very serious consequence where security and breaches occur. That's something that can't be ignored and has to be addressed and quickly within a lot of the portfolio companies that we're partnering with.

**Privcap: That's a good segue into our Q and A portion, because one of the things you mentioned Eric was readiness varying by industry. I guess, Kevin, are there particular industries that are more vulnerable or typically targeted more by bad actors?**

**Carpenter:** Sure. I think the misconception overall is that the only industries and companies that have to worry about cyber security or worry about it the most are the ones with what we consider to be the most valuable information be it credit cards or social security numbers, things of that nature. While that's true, I think that over time there's definitely been a response in a good way towards protecting a lot of that data. Consequently it's the fraud alerts and all of those things that make it a lot more difficult for the credit cards to be more valuable on the black market. We've seen a shift in business models in terms of, the two biggest things that are our moneymakers for the attackers is going to be the wire transfer fraud and the spear fishing to get that information that Eric alluded to earlier, and ransomware, where you'll use more broadcast fishing techniques across an organization to see if people will get to click a link and infect their systems.

**Carpenter:** With that being the case, it really has become a bit agnostic as to industry in terms of where they get infected. That said, it can be very impactful depending on the type of attack where there ransomware knocks off some manufacturing shop floor systems and they're not able to actually be under production for days or a week at a time. That's incredibly impactful where nothing not have been stolen necessarily, but they're definitely not able to operate as intended. We're seeing obviously in very impactful breaches in regulated industries. Again, going back to the fines and liabilities there. I think more than anything, it's been very impactful around privacy recently with healthcare and financial services in terms of breached, regulatory concerns from a breach perspective and notifying individuals. There's a huge reputation concern there as well. It's not just the financial impact but the reputation of actually being impacted by that breach.

**Feldman:** Yeah, I can just add that very briefly.
Feldman: 10 seconds here. My experience, I gave two examples earlier in the conversation about what we've seen here across the Riverside portfolio. Kevin is spot on, these attacks, they seem fairly agnostic, at least from my perspective. The businesses that we've seen affected are across multiple industries. It's not as if, let's say we make investments in healthcare companies as well as manufacturing. We're seeing an equal distribution of who the bad actors are going after. If you can get one accounts payable clerk to fall for a phony wire transfer, then there's no reason why most of our companies aren't vulnerable.

**Privcap: Beyond fines, there's also the reputational hit that a firm can take. What are the steps post remediation that address both those issues?**

**Carpenter:** An incident response plan is critical. Understanding what are the elements, how can we potentially be breached? What are our biggest risks and threats? Where are we vulnerable? And if there is a breach, what do we do about it? How do we practice some of that? Who's responsible? That's where we see the majority of the companies that do a good job with reacting quickly, triaging an incident, having the proper backups in place.

**Feldman:** We coined it internally as incident preparedness, but it's really the same thing as response. What we've tried to do is to create a very simple playbook for our portfolio company. If there's a perceived or actual incident, we have worked with our operating teams to make sure that there is a communications protocol.

One of the things that we saw very early on, particularly when we were first building out this program is, there would be a problem, and our portfolio companies would start firing off dozens and



↓ CONTINUES ON NEXT PAGE

dozens of emails. We have educated them and continue to work with them to make sure that that communication is a little bit more refined and not broadcast to the universe.

**Privcap: What role does insurance have to play in protecting value?**

**Feldman:** The biggest bang for the buck with these policies to date has been on the forensic side. We don't want our portfolio companies to be in a position where there's an incident and they're sitting down and negotiating terms when it's really important to get that forensics group involved as soon as possible. Although I'm not an insurance expert, I can tell you from maybe like a thousand foot view that, at least to date, the insurance programs that we put into place for our companies have been pretty effective. ■



## About the Experts

**Eric Feldman**
Chief Information Officer
The Riverside Company

Eric Feldman joined global private equity firm The Riverside Company in 2011. He is responsible for all aspects of the firm's global technology strategies, including application development, project management, information security and an IT infrastructure supporting 17 global offices. Mr. Feldman was instrumental in creating Riverside's Information Security Program, which provides a risk-based approach for managing information security for Riverside's 80+ companies. He previously served as the Director of MIS for the Office of the Mayor, City of New York, where he worked on a number of citywide initiatives focused on improving service delivery and reducing cross-agency inefficiencies. Mr. Feldman received a B.A. from Eastern Illinois University.

**Kevin Carpenter**
Director, Risk Consulting
RSM US LLP

Kevin is focused on security and privacy risk with over 15 years of consulting and auditing experience, including with a Big Four firm. He has experience in the design and implementation of information technology (IT) systems and infrastructure, as well as IT audit from both an external and internal perspective. He has served a wide array of client markets in various industries for both public and private companies of varying sizes as well as the public sector. Kevin has managed and executed numerous IT environment assessments, ranging from internal controls work and application audits to government regulatory audits.