FINSBURY

Debevoise & Plimpton

How Secure Is Your Kitchen? Corporate Cyber Risk in the Time of Coronavirus: In Conversation with Debevoise & Plimpton LLP

Luke Dembosky
Partner
Debevoise & Plimpton

Jeremy Feigelson
Partner
Debevoise & Plimpton

Paul Holmes
CEO, North America
Finsbury

Honey Debelle
Associate Director
Finsbury

All organizations face cyber risks, and those risks have only increased as more employees work from home as a result of COVID-19. With these added challenges, a cyber incident can even more easily damage a company's reputation, limit its ability to operate and expose it to significant legal liability.

In the latest Finsbury conversation with global cybersecurity experts, Paul Holmes, CEO, North America and Honey Debelle, an Associate Director on the firm's Cyber Task Force, spoke with Luke Dembosky and Jeremy Feigelson, Partners and Co-Chairs of the Data Strategy and Security Practice at the international law firm Debevoise & Plimpton LLP.

Paul: For many employers, the pandemic has changed the cybersecurity landscape. What is top of mind for companies at the moment when it comes to cybersecurity?

Jeremy: Remote working raises a whole slew of issues about how to secure the workplace when the workplace may be your kitchen table, with your family or your roommates wandering through while you're discussing confidential issues or handling confidential materials on your screen. There's a need to raise consciousness and train the workforce about maintaining security in a world where everybody's working at home, in an environment where you're not used to maintaining the same level of security consciousness that you do at the office.

There's also the uptick in attacks that our clients are seeing specifically because of the pandemic; for example, in ransomware, and in phishing attacks aimed at business email compromise. These are the types of attacks where a good defense in ordinary times might be to wander down the hall and ask a colleague, say, "Hey, is this payment instruction legitimate?" But now, there's no hallway to walk down, and the security risk has increased.

Paul: How are companies responding to these changing threats? Are companies having to require different things of their employees or take different defensive measures?

Luke: It's been a scramble to catch up. At first, a lot of the information security teams were moonlighting as IT professionals to help companies move to remote working, and that onslaught of "help desk" requests pulled a lot of the limited resources on the information security side into the IT space. And now, things that were challenging even before have been exacerbated by the remote situation. We've had clients hit with cyber-attacks that, because their systems are down, had to get special permission for somebody to enter the building to retrieve something in hard copy that's not otherwise available — for example, their incident response plan. In these cases, the ability even to access your playbook has caught some off guard.

Paul: And how are companies policing this with their employees? How can they ensure that there are appropriate security measures in place at home?

Jeremy: You know, the old real estate joke is only three things matter: location, location and location. When it comes to your employees, it's training, training and training. And it's overwhelmingly about getting the message out, and then getting it out again, to be sure that people have upped their game on these issues in a way that simply was never necessary before. A close second behind training is making sure your people have the right equipment, and that "bring your own device" policies are updated to reflect the new realities of so many people working primarily on a home computer or personal laptop.

Paul: Do you see specific types of companies that are especially at risk in this new environment? Is there a sector or geographic emphasis or scale that comes into play?

Luke: I think the challenges are across sectors, but some companies have been harder hit by the pandemic, and that presents distinct risks. We've had some clients that have had to lay off a substantial portion of their workforce, including many people with privileged access credentials that need to be turned off. You've also got people that may be upset with you as a result of being laid off, and so there's an insider threat risk to manage. And then, you're left to do more work, and with fewer people, while trying to preserve the network.

The other area that's been a real challenge, and that the regulators are intensely focused on, is vendor vulnerability. We could be buttoned up, but if a key vendor-managed services provider can't do their job securely, and we depend on them, that's a risk that we inherit. That risk really cuts across sectors.

Paul: And has there been a different approach to due diligence and compliance as a result of having to take on new vendors remotely?

Jeremy: I think the main effect is that companies engaging vendors have had to simply swallow hard and accept that you're going to have to go on trust to a greater extent. If you can't do a site inspection of the vendor, you can't do a site inspection of the vendor, but you still need their services. You can try to compensate by asking more questions in the remote due diligence than you would have before. But I would echo what Luke said, that there's probably no more intensifying area of scrutiny from the regulatory community right now than for third-party vendor relationships. The New York State Department of Financial Services, for example, is all over this, and I don't think there's going to be any sort of pandemic discount in terms of the regulatory intensity.

Honey: As we think about eventually returning to the office, what are the biggest challenges for corporations when it comes to maintaining cybersecurity and data privacy?

Jeremy: On the cyber side, I think it seems likely that a much larger degree of remote working is here to stay. That means that all the issues we have been talking about, providing employees with the right technology and a constant need for vigilance — these are going to be permanent considerations.

On the privacy side, employees are going to have to be constantly answering personal questions that we all would have thought were very weird and intrusive six months ago. So how do you deal with that data? You get policies and procedures in place so that it's regularized, so that there's a framework for it, people are educated to expect this new normal, and so that it's not being done in a random way. You train people and you have off-ramps for particularly knotty cases, and you find sensitive ways to deal with the fair concerns that people are going to be raising.

Honey: Looking further out, what's the next evolution of cyber threats that companies need to start anticipating and preparing for now?

Luke: We're seeing a growing trend in destructive threats like ransomware and other extortion-type schemes, and we're seeing a spike in targeted schemes against executives. These could be business email compromises where they have studied your LinkedIn profile and developed a very targeted scheme. They've gleaned who reports to you and can craft the perfect message and be very tailored about how it's used.

Honey: How effectively do you think the legal and regulatory landscape is keeping up with these evolving threats? And how do you expect it to evolve in the future?

Jeremy: Well, the basic legal rule is that security has to be "reasonable." It's a deliberately flexible standard so that regulators don't need to go back and write new laws in order to hold companies accountable as threats and best practices change. They see a change in circumstances, they expect companies to respond properly, and if they don't see a prompt and effective response to change — for example, if you see a company not engaging reasonably with all the security and privacy challenges of the pandemic — then they won't hesitate to hold companies to account.

Luke: A regulation trend in cyber, certainly in the U.S., is that leading regulators have added tremendous technical capability to their staff and can be much more in the weeds on cyber issues. Regulators have the ability now to roll up their sleeves and ask very detailed questions right up front. It means that you'd better be prepared to explain why you made certain choices one way or the other. And ideally you would have documented that, so it doesn't appear that you're simply rationalizing a decision after the fact.

Paul: Before we go, any parting thoughts?

Jeremy: All of the risks we're talking about, and all of the response strategies, are global. The pandemic doesn't respect borders. Cyber threats don't. Privacy threats don't. And in our practice, we see companies, and the agencies that regulate them, literally all over the world — dealing with this whole set of issues. The legal standards are also converging globally to an extent, which makes it somewhat easier for a global company to manage compliance.

Luke: If there was ever any doubt before regarding the need for a cross-functional response across not only technical functions but also legal, communications, compliance and others, it's very evident now that modern cyber threats require a whole-of-company response and capability, and the companies that take that approach will be best positioned for the future.

All of the risks we're talking about, and all of the response strategies, are global. The pandemic doesn't respect borders. Cyber threats don't. Privacy threats don't.

For more information, please contact:

Paul Holmes
Paul.Holmes@finsbury.com

Honey Debelle
Honey.Debelle@finsbury.com

FINSBURY

FINSBURY US
3 Columbus Circle, 9th Floor
New York, NY 10019
+1 646 805 2000

www.finsbury.com
enquiries-us@finsbury.com