Ep. 13: Cybersecurity and the Boardroom

February 20, 2019

Jose Garriga: Hello, and welcome to *OnAir with Akin Gump.* I'm your host, Jose Garriga.

Cybersecurity issues and concerns are inescapable, from Main Street to the White House, social media sites to your local voting booth. And the news is rarely good. This is the final episode in a mini-series of podcasts that delve into the topics covered in the 2019 edition of Akin Gump's annual *Top 10 Topics for Directors* report.

And we have with us today Akin Gump cybersecurity, privacy and data protection practice co-leader Michelle Reed. Her practice focuses on advising companies and boards on cybersecurity and privacy governance and risk management, as well as breach preparedness.

We'll be reviewing cybersecurity issues in 2018, discussing cybersecurity as a concern for companies and their boards, and looking at 2019 and best practices for companies facing cybersecurity threats.

Welcome to the podcast.

So, this is a big topic, so let's start by setting the stage. In 2018, to what extent did cybersecurity grow as a matter of concern, both for national and for enterprise security?

Michelle Reed: 2018 had a lot of surprises for companies across the country. There was the standard garden-variety e-commerce breaches that we saw. But we saw the cyberattackers become more clever and innovative in their attacks.

And you saw more attacks that were focused on industries that previously hadn't been targeted, seeing more in the energy industry, more in the national security space. And more clever attacks in the way that they approach it.

And, so, the attacks, as opposed to just stealing your personal information, were attacks that were actually business disrupting, where companies went down for days, sometimes weeks or more, in terms of being able to restore their data. And the damage that they faced from that was pretty significant and potentially devastating.

What we also saw, in addition to that, is a focus and more awareness of the American people on what data companies have related to them, and how it is protected, and how it is used. And I think we'll talk about this a little bit later.

But some of those concerns that were highlighted through various breaches across the country ultimately resulted in pretty significant legislation that will impact companies going forward.

Jose Garriga: So, a busy year. And people, as you said, are becoming more and more aware of things. Who are the principal players in cybersecurity? And we're talking now about boards of directors and from the corporate world. Who are the principal players in cybersecurity that boards should know about?

Michelle Reed: An excellent question, because it varies based on whatever industry you're in. The Federal Trade Commission, the FTC, has exercised its power, and it has pretty broad power, to enforce privacy and cybersecurity. And that has been sort of the principal player in laying the regulatory enforcement framework. However, it has not been a hammer that it has wielded, but, instead, has sort of guided things and ultimately resulted in more oversight and more auditing.

And what we saw in 2018 was some significant players getting involved. Obviously, for our boards, the Securities and Exchange Commission had some pretty significant enforcement and guidance activity in 2018.

For example, they came out with Commission-level guidance on cybersecurity disclosures and controls. And they also issued a 21(a) report, where they warned that it may consider certain cybersecurity vulnerables as actionable violations of the federal securities laws, which require robust internal controls.

In that case, it was particularly with respect to the business email compromise that resulted in pretty significant wire transfer fraud. We saw enforcement actions coming from the SEC based on insider trading, where they targeted and alleged insider trading issues. Failure to disclose cybersecurity incidents.

And then also, we finally saw an enforcement action related to the identity theft Red Flags Rule, which is across all industries, these red flags rules, but we hadn't seen a lot of SEC enforcement related to that.

And so, essentially, finding them in this particular case, they alleged that there was a failure to pay attention to red flag warning signs that hackers were attempting to steal information.

And so, across all of these different enforcements by the SEC, public companies and even private companies regulated by the SEC face some pretty significant issues. But on the federal level, that's not the only regulator. You also see, for example, here in the health care industry, HHS is also regulating. If you're in the communications industry, the FCC; and, obviously, for anyone in the [*defense industry*], the new DFARS [*Defense Federal Acquisition Regulation Supplement*] rules are very significant and have some very detailed requirements now.

At the federal level, that is some of the very significant regulatory activity associated with cybersecurity.

Jose Garriga: Now, I know that you were talking about federal level. How about the state level? Who should boards be looking at as being either regulatory or other authorities that might be playing a role in how they run their businesses?

Michelle Reed: The state level is an interesting and ever-evolving area. And some of the most significant cybersecurity regulations and data privacy regulations that we have now are coming out of the state level.

So, in 2018, at least 35 states introduced more than 265 bills or resolutions related to cybersecurity. And that creates this very big mass of regulatory guidance and frameworks that companies are having to follow.

Specifically, you see California come out with its California Consumer Privacy Act, and the California attorney general will enforce that. And it also provides a narrow private right of action against companies for failing to implement reasonable security controls; that goes into effect in 2020.

However, it has a look-back provision, where you have to understand how data, data practices are being used. And that look-back is one year. Therefore, as of January 1st, 2019, companies subject to the CCPA need to have an understanding of what their data practices are.

But we also saw state actions and regulatory changes out of Colorado, Ohio, South Carolina, Connecticut and New York. Specifically, New York's Department of Financial Services' cybersecurity regulation, went into effect—well, it's been in effect for a little while...there was a rolling implementation date—and some of the most onerous requirements are related to third-party due diligence, have compliance by March of 2019.

And, so, companies are facing this ever-evolving threat, not just from regulatory threat, not just from federal enforcers, but also from state enforcers. One incident that recently happened in the last month was an ability for states to enforce HIPAA [*Health Insurance Portability and Accountability Act*], which normally—HIPAA, the health care privacy enforcement mechanism—is at a federal level. However, it enabled the states' attorneys general to band together and to enforce HIPAA.

And, so, we saw one of the first actions where the state attorney general actually sued a company in connection with a health care-related breach. And, so, the state enforcement is actually a significant player in resulting in multimillion-dollar settlements with companies across the country.

Jose Garriga: Well, stepping back then, and looking at ... well, not even necessarily at the federal level, but you're a litigator. Were there any big court decisions in 2018 that boards should note vis-à-vis cybersecurity and privacy concerns?

Michelle Reed: There were some interesting decisions that you saw with respect to boards in derivative actions. There were some major breaches where the plaintiff's lawyer decided not just to sue on the breach itself, so as representing the consumer, but there was some where you saw stock drop, and the consumer sued under Section 10b of the 1934 Securities Exchange Act. And they also then took another step and sued the directors themselves for breach of fiduciary duty in connection with their cybersecurity oversight.

And there were some decisions that came out ultimately. Some of them formed special litigation committees to evaluate it. And, ultimately, some were able to get them dismissed. Not for free, because the cost obviously of creating an SLC is significant.

And the courts went through many different factors that you can evaluate and look at to see the sufficiency of the review by boards of directors. And, so, when you look at some of the decisions, you see reports that go into great detail about the number of times the board met, the financial expenditures associated with their cybersecurity, their insurance coverage. It evaluated overall cost of the breach and evaluated their policies and procedures that were designed to implement a reasonable information security program, evaluated their compliant policies, looking at the board's audit and corporate responsibility committees. All of these things, and more, were included in that special litigation committee analysis.

And that ultimately resulted in dismissal of the action. And I think it serves as a great road map for directors to evaluate whether they're fulfilling their fiduciary duty on oversight of cybersecurity risk.

Jose Garriga: Thank you, Michelle. A reminder, listeners, that we're here today with Akin Gump partner Michelle Reed in the third of our Top 10 Topics for Directors podcast. We're discussing cybersecurity, privacy and their unignorable relevance and importance to companies and their boards.

So, having set out what seems to be a fairly daunting landscape, what are some best practices that boards and directors can adopt to improve their cybersecurity posture and reduce their compliance risk profile?

Michelle Reed: The most important thing is that the boards know who's responsible for that risk and that they're actually evaluating that risk. Boards need to decide which subcommittee—and frankly, a lot of boards that I've worked with have established the audit committee as the risk oversight committee, and the audit committee is the one looking at this.

But whatever subcommittee you establish, or whether it's the full board itself, the directors should have an idea of what their information security policies look like, and making sure that they have them and that they're effective.

I've certainly worked with lots of different companies who had information security policies, who had crisis management policies, who had incident response policies—none of which coordinated together, and none of which worked very well in the sense of the crisis. So, making sure that there's a really strong existence of policies and procedures, and that these policies and procedures have been tested.

So, encouraging from the top down, things like tabletop exercises, where companies will meet together, and oftentimes we have board members there as well. And they go through a mock breach, and they practice how their incident response will be, so that they can see how the policies work together, how the communication practices work and whether they're effective or ineffective, so having some oversight into that. I'll add, I think, making sure there is some oversight into internal accounting controls. The SEC's reports on the business email compromise and the wire transfer frauds that are occurring was significant, because it's pretty rare that the SEC issues a 21(a) report.

They very specifically warned that it would be considered an internal accounting control failure if they didn't take certain steps to protect from these fraudulent wire transfers that were happening through cybersecurity breaches. So, making sure that we've reviewed those policies, and we make sure that we at least thought through and trained appropriately.

And then thinking through what those public company reporting disclosures look like. With the SEC's guidance on cybersecurity disclosure, there's certainly a trend towards increased disclosure and thoughtful disclosure related to cybersecurity. And it varies, based on what your industry is and what your risk is. And, so, you have to have an understanding of where your data is, and how it flows in order to create those public disclosures that really reflect the cybersecurity risks that your firm may have or that your company may have.

And then also making sure that there's insider trading policies in existence to protect against insider trading in the event that there's a breach and also to prevent against insider trading by the criminals themselves. And, so, making sure that you have some protections of pretty significant data. As you saw from the SEC's own recent breach of its EDGAR system, and the DOJ running an enforcement action in connection with that, that provides some very specific examples of what companies need to do to make sure that they're protecting themselves.

And then, doing things like evaluating what the budget is, and making sure that you're properly funding and that you're adequately thinking through things.

Evaluating risk and learning from mistakes. Every company experiences some sort of privacy or cybersecurity incident response issue. It's very rare to not have some issue throughout the year. And, so, making sure that whoever is presenting the cybersecurity issues to the board, is presenting a complete picture. And that your governance is set up in a way where the people who are charge of cybersecurity aren't trying to hide the ball of what the cybersecurity picture looks like because they're trying to protect their own job or their own department from looking bad.

So, making sure you have an independent eye towards what that cybersecurity risk governance looks like is important. That probably means that you're doing risk analyses, gap testing, and that you're doing penetration testing by third parties who can give you an eye of where the holes are and the gaps are to protect against it.

Going through all these different procedures is going to enable companies to be better prepared. And then I guess last, but not least, is making sure that there is cybersecurity training at your company. And not just training for people in HR or people in finance. But making sure that cybersecurity training exists across the company, because as we've seen in lots of different breaches, it only takes one person falling for the phishing email for the criminals to move laterally through your system and take a lot of your crown jewels.

So, having sufficient training that analyzes and encourages employees to be responsible can protect you better than almost any other recommendation I've given.

Jose Garriga: So, we've looked back a bit at 2018. You're talking about some good practices looking forward. Looking forward, then, again, in a different perspective, what does 2019 hold, do you think, in terms of national data protection initiatives?

Michelle Reed: So, for years, on a federal level, they have tried to get legislation to protect cybersecurity and to primarily provide notice requirements in the event of a breach to some uniformity. And it's never passed. It's never made it through.

And the reason why is because no one necessarily had a dog in that hunt. There were lots of different standards. In fact, now there's 50, plus three territories, of different standards of notification. And there was nothing driving towards a federal resolution.

This year is different. And the reason it's different is because of the California Consumer Privacy Act. The California Consumer Privacy Act is a ticking clock that goes into effect on January 1st, 2020. Because of that, on a federal level, the House of Representatives and the Senate are incentivized to come up with some sort of federal regulation to create uniformity across the states. Because if they don't do it, in effect, California's will become the default law of the land, because most companies who do business ultimately with California are going to have to comply with that CCPA.

And, so, this year's a little bit different, because there's actually an incentive and a time pressure to get it done. Now, whether they're able to do that or not will remain to be seen. Obviously, in 2019, Democrats will control the House of Representatives, and Republicans continue to have a majority in the Senate. And this shift in the House allows privacy advocates to demand greater protection, should a preemptive privacy bill move through Congress.

But it's clear that there's an interest in legislating around privacy and data security issues, even in the Republican-controlled Congress. So, because of this shift in control, combined with the pressures from the California privacy law, I anticipate that you're going to see some federal legislation. What that looks like? I don't think anyone knows at this point.

There are certainly pretty significant alliances of companies that have proposed legislation because they recognize that this ever-changing different state requirement, and sometimes conflicting requirements from various states, is just not a workable solution to companies that operate cross-state, which is most companies.

And, so, I think you're going to see some federal legislation. Hopefully they'll be able to also add some data breach notification standardization, so that companies ultimately are able to move forward with a clear standard and have some streamlining to their cybersecurity practices and their data privacy and protection practices.

Jose Garriga: To what extent would you say that state-sponsored cyberterrorism is also going to be a motivator, or a reaction to that, in terms of getting Congress to come up with a national data protection standard?

Michelle Reed: I think that cyberterrorism is the top of mind for many people in the House and the Senate. Many of our leaders are seeing pretty clearly. And you see some of the recent indictments, some related to the Securities and Exchange Commission breach, and others related to other pretty significant national security breaches.

And the game has changed. The cyberterrorism threat is very real. And although we were sort of at a détente, I think there's some change to that that we've seen. And because of that, I think you're going to see some different actions and behavior and preventative strategy.

Obviously, the key focus on the cyberterrorism front is going to be looking at issues of national security and issues of business continuity throughout the United States. And, so, making sure that we have proper guidelines that help and assistance for the grid, making sure that we have proper help and assistance and standards for our defense contractors.

There's going to be a continued push at probably more detailed standards associated with that, because the high-level approach of generally using a standard that's scalable and that's optional, I think they've found has not necessarily, in certain critical areas, gotten to the result that they want.

So, I think you're going to see an increased amount of enforcement associated with it. So, the Department of Justice will be pursuing criminal actions against the cyberterrorists. But you're also going to probably not see the back-door efforts that are being made with companies to improve our cybersecurity posture.

Jose Garriga: So, to wrap up, we've covered a lot of ground. What are some of the key takeaways for listeners regarding corporate cybersecurity and privacy concerns and countermeasures?

Michelle Reed: I think there needs to be an expectation that your company will suffer a breach. And if they suffer a breach, what does that mean for your responsibility? And what do you have to do?

I think it's incumbent upon directors to understand the company's use and sharing of data so you can understand how potential legislative proposals may impact your ability to do business and then have a monitoring system of what's being discussed.

It's also critical that the directors receive regular cybersecurity briefing. So, it's not a once-a-year report from the chief information security officer, but something that is regular just as you would do with any of your other risks.

Because, frankly, the cybersecurity risk is one that can be so business disruptive, whether it be on your internal basis of employees or on your external basis of your

customers, or some combination of the two. It can make or break your company, your ability to respond.

And, so, having a regular cybersecurity briefing, where you're asking tough questions about preparedness. And you're doing third-party checks with vendors to make sure that the story you're getting on your security status, it aligns with what your security looks like.

And then thinking through the hard questions of "What's my worst-case scenario? What is it that keeps me up at night? If this were to be stolen, or if this were to be breached, what would I do, or how would I respond?" Those are the hard questions that need to be asked because it may impact the way you use and collect data.

The simplest way to decrease your cybersecurity risk, at some level, is to have a stronger hold on the data that you use. Because if you notice from some of the breaches, some of the information that ultimately gets leaked through these breaches has absolutely nothing to do with a social security number or a financial account number, but just have damaging information through overheld emails or through documents that didn't even need to be retained.

And, so, thinking through what that footprint is. How do I use data? Am I sure that's how we're using data? And are we making right promises to our customers, to our employees and to others whose data we are using? Those are the hard questions that need to be asked. And then continually followed up on, so that you learn from your mistakes going forward.

Jose Garriga: Thank you. Listeners, you've been listening to Akin Gump partner Michelle Reed. Thank you, Michelle; that was terrific. Thank you for walking us through this vital and evolving topic, and I think offering folks a really good idea of what the landscape looks like, and what to look for in the year upcoming.

And thank you, listeners, for your time and attention. Please make sure to subscribe to *OnAir with Akin Gump* at your favorite podcast provider to ensure you do not miss an episode. We're on among others, iTunes, YouTube and Spotify.

To read the *Top 10 Topics for Directors* report, please visit akingump.com and search for it by name. And to learn more about Akin Gump and the firm's work in and thinking on cybersecurity, look for “cybersecurity” on the Experience or Insights & News sections on akingump.com.

Until next time.