ESG Essentials: What You Need To Know Now

Episode 4 – Cybersecurity

Colvin: Welcome to another episode of "ESG Essentials: What You Need To Know Now," a podcast from your friends at Fox Rothschild. I'm your host, David Colvin, Co-Chair of the firm's Environmental, Social and Governance Practice Group.

I want to welcome back those listeners who tuned into prior episodes and are familiar with our podcast. For any new listeners out there, our series of short and bite-sized podcasts cover core ESG concepts and explore important issues for businesses that are concerned with corporate responsibility, responding to increased scrutiny from regulators, investors and customers over their environmental and social impact, and minimizing the legal and business risks associated with ESG.

For this episode on the topic of cybersecurity, and how cybersecurity fits into any company's ESG profile, we welcome my partner and good friend, Kristen Broz. Kristen is a partner in the firm's Washington, DC office and is a litigator with a national practice focused on class action, data privacy, intellectual property and federal government contracts. Of significance and relevance for today's discussion, Kristen has a particular set of skills in the world of data privacy and data security. She teaches courses in legal and ethical issues around cybersecurity and information assurance as an adjunct professor at UVA and at Capitol Technology University in the capitol of Washington, DC.

With that, I welcome you, Kristen, to this episode of the podcast.

Broz: Thank you very much, David, for that introduction. I'm looking forward to speaking.

Colvin: So, Kristen, let's just jump into it. We've all heard – unless you've been living under a rock – we've all heard cybersecurity discussed as a technology issue because at its core, it is a technology issue and also a privacy issue. But why should companies be looking at cybersecurity as an ESG issue?

Broz: There's a whole host of reasons companies should look at cybersecurity as an ESG issue. I read recently that the average cost of a data breach can be nearly $4 million per company, which is staggering by anyone's assessment.

Cybersecurity and data privacy are a major issue for company management. They're a major issue for investors, and they can be a major issue for employees. Since COVID-19, increased working from home has increased exposure to cyberattacks, as has the onslaught of cyber criminals over the last five years – and particularly over the last two years, increased threats to companies. Companies face a lot of different risks from a cyberattack. This can include harm to their reputation, to their financial performance, to customer and vendor relationships. There's also threats from litigation in the event that sensitive data is compromised. That litigation can come from customers whose data the company houses, or it can come from banks and other financial institutions if there are obligations under financial regulations. It can come in the form of issues with health care data. Really, the sky is the limit.

There are also threats that companies may face in the event of a cyber incident from a regulatory investigation or action. That can come from state regulators, it can come from national regulators, or it can come from an international body, like the European Union.

Some of the more vulnerable companies right now are actually those that have not previously invested in significant cybersecurity infrastructure. A lot of tech companies and financial companies have been all over this for years, and they had breaches five, 10 years ago and they got smart. But now, companies that didn't previously have to care about cybersecurity have to think about it more. There's also growing national and international requirements that increase the cost of compliance with cybersecurity regulations. This is driving corporate spending on cybersecurity higher, and it also increases the financial risk of the breach.

Then finally, what I'll say is that customers and investors want to know that companies are doing what they need to do to protect themselves against a breach and that they have disaster recovery plans to mitigate any financial impact of a breach. Because ultimately, any cyberattack, any cyber risk, is going to affect the company's bottom line.

Colvin: You talk about the various ways that a cyberattack can really impact a company, its operations, ultimately its bottom line, and maybe even most importantly, its reputation, all of which ESG permeates and touches. Can you talk a little bit about the obligations that a company's board of directors has to oversee cybersecurity and data privacy policies and programs?

Broz: What's really interesting, David, is that even the Federal Trade Commission (FTC), as recently as last year, issued an article urging boards of directors to take accountability for cybersecurity. The FTC mentioned that there were actions against major companies for allegedly deceptive or unfair conduct related to companies' data security policies.

Bottom line: Cybersecurity is expensive. It costs a lot to become compliant with applicable regulations, and it costs a lot to invest in the appropriate technological infrastructure to make sure that data and networks are protected. So, for this reason, any company whose board of directors isn't involved in cybersecurity decision-making is missing the point. The board needs to approve those expenditures, and cybersecurity needs the attention of the highest levels of management to make sure that it's getting the right attention and resources that it needs to have an adequately robust framework. I would recommend that if your company's board isn't dealing with cyber already, it should be. I would even suggest that your board might want to create, or consider creating, a cybersecurity committee or subcommittee and at least hold a regular security briefing.

Colvin: Kristen, you mentioned the importance of the board of directors being involved with respect to overseeing a company's cybersecurity policies. As companies are thinking about their ESG profile – and maybe starting one or improving upon what they already have —they should be looking to identify key stakeholders within the enterprise to lend their voices and to make sure that, at all levels of the

company, appropriate voices are contributing to the ESG efforts. I take it you would recommend that one of those key stakeholder groups be the IT department or group or function within the company?

Broz: Yes, David, that's absolutely right. There's one thing I'll add to that. I've been teaching cybersecurity for over 10 years. When I first started teaching this, a lot of the heavy lifting was explaining to students (who were going to be leaders in cybersecurity within their organization) what they needed to do to get buy-in from key stakeholders within the organization to recognize the importance of cybersecurity. When we talk about business management of cybersecurity, we talk a lot about involving key stakeholders from across the organization, including IT, because ultimately everybody within an organization bears some level of responsibility for maintaining cybersecurity. Any user has to make sure that its passwords are protected, that it doesn't lose its devices. It's very important to have all of the areas of the company involved in these decisions. And I would say that reporting obligations to the board, depending on the nature of the data your company manages, might go across business units as well as IT.

Colvin: We talked a little bit about the governance aspect in terms of the board's role in oversight when it comes to cybersecurity, and your recommendation that boards really need to be involved on these issues. But you also touched at the beginning of your comments on cybersecurity also being a "social issue" under the social pillar of ESG, and that's a concern for companies, or at least should be a concern for companies, as well. Can you talk a little bit about how company leadership can address the social components of cybersecurity?

Broz: From where I sit, there are actually two big social issues in cybersecurity that companies face. There's one that is front of mind right now, and it's the risk to a company if there's a big data security breach and all the things that come from that. What are the reporting obligations? Does the company bear some liability for the stolen data? And then, reputational concerns if the data was somehow inadequately protected. That's all one of the big social concerns. The way that it works out as a social concern is, investors and customers will say, "Well, I don't want to invest in a company that isn't protecting its data appropriately, isn't complying with laws, or if it is, isn't engaging in best practices."

The other social concern though – and I want to focus on this because we've talked a lot about cyberattacks recently – and it's if the company itself is somehow misusing personal data. Breaches often get the spotlight, but it's equally important that companies that collect personal, identifying information, protect that information and use it only in keeping with clear consumer disclosures. I think a big issue for companies socially will be if they said, "Hey, we're taking your data and we're only using it for this purpose," and then it's uncovered later that they're selling it to third parties. That they're using it to investigate information about you, that they're using it to market to you. I think that is increasingly frustrating to consumers and frustrating to investors and making them less likely to invest in your company.

I think consumers and investors are becoming much more conscious about their privacy rights and about the ways companies use and sell their information. They want to have confidence that their

information is being used for good. Frameworks like the GDPR that came out of the EU in 2018 include some unique privacy rights, like the right to be forgotten, that don't just require companies to use data consistent with their disclosures but also require companies to have some affirmative obligation to delete any data that they have on a person if that person requests it. I think concepts like that are going to continue to have hold even in the United States. There's a huge social component to cybersecurity.

Colvin: I totally agree. One of the things you mentioned, among others, was the reputational concern if there's a data …event, we'll call it, because we don't want to necessarily call it a data breach, but if there's a data event or an incident and that gets disclosed to the public and reported out according to the applicable law. You mentioned, obviously, the natural reputational harm that can arise if it turns out the data was not adequately protected. I'm just wondering how you counsel companies that are in that situation. Is there a way to restore that reputation once you've been outed as a company that doesn't take appropriate steps to protect the data of its employees, or its customers, or its suppliers, or whatever the case may be? Is there a way to restore their reputation?

Broz: David, that's a great question. The answer is such a lawyerly answer: It depends. I think that any repairing of reputational damage from a breach is going to depend on how the company responds to the breach. It's about informing the public promptly of the scope of the breach and what the company is doing to fix it. Complying with all applicable reporting obligations, reaching out to customers, if the company is customer-facing, who might've been affected by it to try to offer them things to remediate any effects of the breach. And then also how they investigate the breach on their end.

Of course, I think it's always going to be in proportion to the magnitude of the breach. The smaller the breach, the easier it will be for the company to recover reputationally. But there have been major breaches over the last few years that I don't even need to name, that I think all of you are aware of, with significant U.S. companies that remain robust and are doing well in their businesses. Their reputations have recovered, so it's definitely possible, and it's happened many times before.

Colvin: I think the upshot is that companies, from an ESG perspective, need to be thinking not just about the cost of responding to a breach – and all that goes into it with the appropriate reporting and the cost and issues related to resource constraints and what I would call the time suck of having to defend potential legal claims, all of which is important and all of which needs to be considered, but the reputational aspect really needs to be considered and addressed to the extent the company is proactive about implementing cybersecurity policies and programs as part of its ESG profile.

That's not to say that a robust ESG profile is going to protect companies from cybersecurity attacks. We know that there’s no silver bullet to protect companies from that. But certainly, it will put the company in a better position to at least present itself as being sensitive to those issues, sensitive to the data that it maintains on behalf of its employees or customers or suppliers or whoever. That it's trying to “do the right thing.” I think from an ESG perspective, getting out in front of it by making sure that they have the right cybersecurity protocols in place will help mend the reputational harm that could arise in the event of a breach.

Broz: That's absolutely right, David. If you don't mind my saying one more thing to that: The conduct of your company, if one of these incidents results in litigation, in terms of policies and things like you're describing, is going to have impact whether there's liability too. So, not only do good front-end policies improve any of the reputational risks of a cyber incident, but they also improve your chances of succeeding in defending against a lawsuit.

Colvin: That's a really good point.

No podcast would be complete without a reference to COVID. Hopefully going forward, those references will become fewer and fewer, but can you talk a little bit, Kristen, about how the remote working environment that we've all grown accustomed to in the time of COVID has increased cybersecurity-related concerns as it relates to ESG?

Broz: I might've mentioned this a few minutes ago about how employees are part of a good cybersecurity protocol. A common adage in the cyber world is that you're only as strong as your weakest link. For the vast majority of companies, their weakest link is their employee user. Of course, remote work gives employers a lot less control over their employees and, importantly, over the devices those employees are using.

There was a study that came out a year or two ago showing that employees are less aware of things like phishing scams when they use their devices at home. From my perspective, it's a sort of fascinating psychological phenomenon that comes from, I guess, letting one's guard down when you're sitting on your couch working rather than being in a formal office. Also, it's a little harder to train employees in a remote environment than in the office. But all that said, I think that we'd be kidding ourselves if we didn't acknowledge that remote work is here to stay. My thought is that companies really need to double down on best practices like multifactor authentication, encrypted hard drives and supplemental employee training to address potential security weaknesses in a remote environment.

I hear a lot of companies are talking about, “Oh, let's bring people back to work because that'll fix a lot of these problems.” It won't. Even if employees come back to the office full-time, they're still taking their devices home. They're still using them when they're outside of the office. These vulnerabilities exist regardless. It's just that the remote work environment is highlighting them for us, maybe in a helpful way. Maybe it's helping us protect against things that would have happened down the road regardless. I think companies should prepare for a remote workforce that is cyber savvy, with devices that have higher security standards. I think that's really the way to address this problem.

Colvin: Let me ask you one last question, which is for public companies, for anyone out there listening who is affiliated or employed by a public company. Can you talk just a little bit about what cybersecurity reporting obligations those companies have to their shareholders, if any? Because I think that, again, one aspect of the governance prong under ESG are aspects of shareholder rights and the company's commitment and respecting of shareholder rights, and so, could you talk just a little bit about what, if any, obligations the company has to report on cybersecurity to its shareholders?

Broz: As far as I understand, the Securities and Exchange Commission (SEC) has not issued separate rules regarding cybersecurity reporting obligations as such. However, the SEC has issued a statement and interpretive guidance on public companies' cybersecurity disclosures as they fit within the existing reporting frameworks. Companies are always required to report on things that would be material to investors, and they have to comply with things like insider trading obligations. Those things apply equally within a cybersecurity environment such that companies do have affirmative reporting obligations in the event of incidents.

The companies have to report, under materiality framework, risks and incidents. They should be reporting on the importance of policies and procedures, insider trading issues and anything that could cause harm to reputation, financial performance, customer and vendor relationships or could lead to litigation or regulatory investigation, are all things that a public company is required to report regarding cybersecurity. The SEC chairman issued some interesting comments in 2018 when the SEC put up this interpretive guidance that, "In particular, I urge public companies to examine their controls and procedures, not only their securities law disclosure obligations in mind, but also reputational considerations around sales of securities by executives."

So even though the SEC doesn't have a separate framework for cybersecurity, it's obvious that the reporting obligations extend to certain types of cybersecurity issues.

Colvin: I think our time is up. I really appreciate you taking the time, Kristen, to share with us your expertise and experience in cybersecurity issues and to help us to understand why those issues are generally really important. And also, the importance of including them in implementing appropriate cybersecurity policies and protocols as part of a company's ESG profile. I think this was really informative and hopefully very helpful to those who are listening. Thank you so much for being here today.

Broz: Thank you, David.

Colvin: Folks, that concludes this episode of "ESG Essentials: What You Need to Know Now." Please do check back frequently for upcoming episodes. As always, if you have any questions, ESG related or otherwise, please feel free to reach out to me at dcolvin@foxrothschild.com. Thanks so much.