"I think preparing for what one will do during that crisis and after that crisis is one of the best ways that a general council can help her company. No one makes the best decisions when they're under pressure, and so if we as GCs can help ensure that how our organization has some sort of muscle memory for how to react during a crisis, particularly one involving a breach, that's a huge value add."

MARCH 23, 2020

Plan and Recover

Presenter: Alexa King

Summary

It's tough to know if your organization is really prepared for the aftermath of a cyber-attack, but who can offer you sound advice and planning for a strong recovery? That's where the general counsel comes in – in-house lawyers, trusted advisors, and cybersecurity experts rolled into one. Alexa King, FireEye's EVP, General Counsel, goes into detail about the roles she plays, how to plan effectively, and advising boards.

Transcript

Brian Contos:

Welcome to the Cybersecurity effectiveness podcast, sponsored by Verodin. The Verodin security instrumentation platform is the only business platform for security that helps you manage, measure, improve and communicate security effectiveness. I'm your host, Brian Contos and we've got a really special guest today. Joining me is Alexa King. Welcome to the podcast, Alexa.

Alexa King:

Thanks for having me.

Brian Contos:

So, Alexa, I've got a lot of things I want to talk to you about today. But before we get started, could you give our listeners a little bit of background about you and kind of the path that you took in your career that ended up here at FireEye?

Alexa King:

Sure. Well, I was born and raised in New York city. My parents were Hungarian immigrants. I'm the first in my family to go to college. And after college I was really eager to go to law school and become an attorney. I thought of law as a way to change the system as needed from within, sort of in contrast to what my parents had to escape from their own homeland because there was no hope for change from within in Hungary, particularly not in the fifties and sixties.

Alexa King:

After law school I started as a litigator in a law firm, but I pretty quickly realized that I would much rather have one client. I would much rather work in house for a company where I could understand the business, kind of inside and out and help the company grow strategically. When you're a litigator in an outside law firm, you're more of a hired gun kind of on the back end trying to do a little bit of cleanup when a problem can't be resolved.

Alexa King:

So, I've been much more interested in problem solving and my career path has been really exciting. I've been able to join disruptive tech companies along the way and try to help scale and expand and grow. Cybersecurity was actually quite new to me when I joined FireEye over seven years ago and I've loved every minute of just being on the front lines of cybersecurity, growing and expanding the company, learning through watching what our customers go through and I think it's made me not only a general counsel, but also hopefully I'm somewhat of an expert in cybersecurity.

Alexa King:

And then on a personal note, I had twin daughters who were born a month before FireEye IPO. So rather than taking maternity – yeah, they're delicious – but instead of taking maternity leave, I did an IPO followed by a billion-dollar acquisition of Mandiant, which was a great, great organization to join FireEye. And we had a secondary offering. And so, to this day I pretty much feel like I had three babies born in 2013: Anya, Katya and FireEye.

Brian Contos:

Oh, my goodness. Well, congratulations on all of those things. I am sure you would have rather have maybe spaced them out a little bit more, but life happens.

Alexa King:

It was all good.

Brian Contos:

That's awesome. Well, tell me a little bit about what exactly does a general council do and sort of what's the main focus of what you do at FireEye.

Alexa King:

Sure. Well, sort of the bread and butter, the day job is to manage all things legal around the world, across the company, whether it's contracts, HR, corporate you name it. I also oversee our privacy function and our stock administration function. But when I think about the role of a general counsel, it's more than just a lawyer. It's really to be a trusted advisor for the executive leadership team and for the board. And hopefully if you've built the right relationships to be the conciliar and to be viewed as a strategic problem solver.

Brian Contos:

Yeah, that makes so much sense. And you had mentioned something earlier on that before FireEye seven years ago you didn't really have that much overlap or you weren't that deep into the world of cybersecurity. But I know that's changed a lot for you. So, going from that sort of most traditional general counsel type role. How has your senior role evolved as it relates to cyber risk and security?

Alexa King:

Yeah, well I think the role of general counsel in general has evolved in the last, I would say five to seven years. When it comes to cybersecurity becoming front and center of all of our jobs, I have sort of a unique situation because I'm the general counsel of a cybersecurity company and I sort of see what other general councils see in their day jobs, but also see what our customers and clients go through. And so, I think my takeaway and the message I would give to any and all general counsel out there, regardless of what type of company they're at, is to be front and center when it comes to cybersecurity. You just need to read the newspaper to see every day the headlines of high visibility breaches, which you and I know are pretty much the tip of a very, very large iceberg when it comes to cyber-attacks these days.

Alexa King:

And the costs and the impacts to organization are astronomical, right? There's damage in time, there's damage in cost, there's reputational damage. And sometimes I think that's the one that is least thought about in advance but can often be the biggest damage of them all. In this country at least in the US high visibility breaches are also almost always followed by high stakes litigation, which is also costly and sort of double whammy for the victim company.

Alexa King:

So, GCs need to be on the front end, right? We need to be developing a cybersecurity plan in advance of the breach instead of coming in at the tail end solely to manage the litigation. I feel very strongly that general counsel need to be very closely partnered with their CISO to prepare for the inevitable breach. We need to be advising our boards regularly on their fiduciary duties related to cybersecurity and we need to work closely with management before, during and after a breach to mitigate risk.

Brian Contos:

Yeah, you said, Alexa, that in the last few years the role of the GC has been evolving in cyber security and cyber risk and privacy and these things have taken more of a front and center role. Are you seeing that pretty broadly when you get together with your GC peers and other organizations or other industries or are you in a very unique position in that year working for a cybersecurity company so it's maybe the volume is turned up a little more or is this trend become quite pervasive?

Alexa King:

I think it's a little bit of both. I would say I'm probably on the front lines just because of my role here at FireEye, but I do see across the board. When I talk to our customers council first of all on the front end of a negotiation, we see more and more that customers are getting their contracts and there SOW in place through their general counsel's office or through their outside counsel's office so that they can attach the privilege at the very front end. That's a step that I hadn't seen before and I think it's a direct result of some painful lessons learned by some of the first companies that were sued as a result of being breached.

Alexa King:

I also see at our company board and in my role as a director on a separate public company board that the board has become more and more involved and more and more interested in cybersecurity. And that's squarely falls on the general counsel to be advisor and counselor on that issue to the board. And in between, certainly during the course of a breach and after a breach, I see general counsel more and more involved. They just have to be in many ways, a good general counsel can be the quarterback or the coordinator of one of the most important teams a company's going to have at a time of crisis.

Brian Contos:

Yeah, well that makes good sense. I've heard you speak before and you mentioned this phrase preparing for the inevitable. When you say that, what exactly do you mean? What is this inevitable item that the organization should be preparing for?

Alexa King:

It's the breach itself, Brian. I mean, I think you and I both know that for most organizations it's not a question of if but when they will be breached. And so, one of the main things I try to do and that I recommend to my fellow GCs is to prepare for the inevitable breach in advance. Of course, prevention is critically important, and I think GCs can work with CISOs on trying to get the best cybersecurity program and technology in place to try to prevent a breach.

Alexa King:

But to the extent that breaches are inevitable, which we here at FireEye think they are, I think preparing for what one will do during that crisis and after that crisis is one of the best ways that a general council can help her company. No one makes the best decisions when they're under pressure, and so if we as GCs can help ensure that how our organization has some sort of muscle memory for how to react during a crisis, particularly one involving a breach, that's a huge value add.

Brian Contos:

I like that. I like that muscle memory about the breach. You're right, because in a reactive situation the last thing you want to be is reactive.

Alexa King:

That's right. Well, and also time is truly of the essence in that crisis. And you want to be making the smartest decisions you can at a time of high emotion and high stress. And so, one of the things that I strongly urge my GC counterparts to do and that I do here at FireEye is regular tabletop exercises around a breach crisis scenario. If you're doing a tabletop exercise and you don't come out with a list of lessons learned and a list of things to work on, you're probably not doing the right tabletop exercise because each and every time we learn something new and to practice for the crisis regularly we at least get used to the idea of who the right people are to have in the room. What's our framework for communication? Now, there are a lot of constituents you need to consider when to communicate with. And so those are the types of things we try to think about during a tabletop exercise.

Brian Contos:

Now that's a question that I've always thought of. I've never been on this side of it. I've never been a GC. But when it comes to communication and sort of going… Making sure we're all on the same page, I'm guessing you're bringing in everybody from IT to HR to Executive Leadership, Invest Relations, Public Relations. I mean there's just so many groups that get involved in this. How hard is that to actually get everybody on that same page and make sure that everybody knows exactly what they're supposed to do. I'm imagining this is probably one of the more complex tasks when dealing with a breach juxtaposed to just the technical bits and bytes.

Alexa King:

Well, yeah, so I mean first look, if your worst problem is you have a lot of really smart people at your company who want to help, you're already in a great situation. But I do think it's going to differ from company to company. Every company has a different culture. But for us we were very clear around who are the people who need to be in the room making decisions, who are the people that we need to communicate out to and who are the people who we view as sort of influencers or kind of having on call but not necessarily in the room. When you think about that communication and particularly these days with social media and other ways in which news can get out rather quickly, you want to think about what's the communication to the board? What's your communication internally to your employees? What are you going to say to your customers, to your investors potentially to law enforcement?

Alexa King:

And so, to really have those ducks in a row, I mean we actually have boilerplate communications already drafted that I can then quickly customize and get to the right people because again, in a time of crisis every single second counts. And you also want to manage the communications so that the company is speaking consistently through one voice externally as well as internally. So, in terms of that, the person I work most closely with is actually our CMO.

Brian Contos:

Wow. I wouldn't expect that actually but thinking about what you've just talked through, it makes complete sense as opposed to 2,500 people hitting Twitter, sharing their perspectives, which nobody wants.

Alexa King:

That's exactly right. And so, as I mentioned earlier, sometimes it's not… In addition to the obvious damages that a breach can cause, how an organization chooses to respond and communicate and how that communication approach is perceived can really impact the reputational and brand impact or damage of a breach. And so, organizations need to be prepared. We don't want to take too long to address questions and concerns. To your point, we don't want 2,500 people tweeting, particularly if they're going to have inconsistent messages. We don't want to spend a lot of time on speculation because that's a distraction that you can't afford when every single second needs to be focused on remediation.

Alexa King:

And so, I feel very strongly that part of the tabletop exercise has to include working with the CMO on messaging both during and post breach, both internally and externally. And obviously as you mentioned, there's investor relations, there's customers, there's other constituent as well. And so, I think GCs can really help focus on the communication messaging across the board.

Brian Contos:

Yeah, that's fantastic advice Alexa. One of the topics that's been coming up more and more and I've certainly seen this over the last year or two, is privilege and the importance of privilege at the front end or even before a breach occurs. Can you talk a little bit about why that's important and what exactly that is?

Alexa King:

Absolutely. And this is an issue near and dear to my heart, probably because of my background as a litigator, but I really can't overemphasize this one enough. Here as general counsel, I've witnessed a lot of our customers deal with post breach lawsuits, post breach government investigations. Oftentimes we, FireEye/Mandiant, are recipients of third party subpoenas during the course of those lawsuits and inquiries and an organization's ability to best protect itself to have the most important conversations, the most candid conversations it can both before and after the breach.

Alexa King:

It's going to depend on whether or not a lot of those communications are privileged. And so, in order for general counsels and organizations to make the best decisions possible to protect their data, to protect their customers and employees, for directors to receive the information that they need it's best to have those communications privilege from the front end. And so here at FireEye we have third party contract, three party contracts already set up ready to go where a breach customer, or to your point even a pre-breach customer, that is concerned and wants to do something like for example, a compromise assessment will retain us through their outside counsel. And that way from the very beginning, all of the communications are privileged.

Alexa King:

And I think it allows organizations some freedom to make the best decisions they can make. We've often seen things taken out of context and used I think inappropriately in lawsuits after the fact and privileges one way to try to prevent that from happening.

Brian Contos:

Yeah. We often talk about the maturation in our space as it relates to incident response, but certainly from a legal aspect and privilege, you bring up an important point as we've evolved in this space and we've had the hard lessons learned and what can happen. That makes good sense.

Alexa King:

Yeah. For example, as third-party subpoena recipients here at FireEye Mandiant there's a huge impact on how our Mandiant work as incident responders will be used by plaintiff's counsel against victim customers depending on whether or not that work was done under the privilege.

Brian Contos:

Absolutely. Well, let's talk a little bit about your work sitting on publicly traded companies boards. The role of somebody like you with your background of course as the GC, but also the cybersecurity bit. How does that come into play when you're on these boards?

Alexa King:

It's been wonderful for me actually to sort of sit on the other side of the board room table. Obviously as general counsel, I have been to many, many board meetings across my career at many companies and so three years ago I was also asked to join a public company board as a director and part of the reason I was appointed, I believe, was because of my cybersecurity expertise. This was a company that felt strongly that they wanted expertise around cybersecurity on their board in addition to some other things that I brought to the table. And my observation both from our own board and from the board on which I sit as a director, is that directors just cannot sit on the sidelines any longer or remain uninformed about a company's cybersecurity program. It's clearly part of their fiduciary duty to oversee cybersecurity just as they do, for example, financial controls or other enterprise risk.

Alexa King:

And so both at the FireEye board and at the board on which I sit as a director, I've recommended that the boards receive regular updates from the CSO, that they be informed as to a company's education practices around cybersecurity, pen test results, cyber insurance those types of issues. Directors I believe now are understanding that it is part of their role and part of their fiduciary duties to oversee cybersecurity. That's different from the day to day management. Certainly, that's squarely in the CSOs hands and in executive management's hands, but boards are becoming much more involved after the fact in lawsuits boards have been sued for breach of fiduciary duty when breaches have resulted. And so, I think that boards now understand that they absolutely need to be involved.

Brian Contos:

Yeah. Maybe not so much because they wanted to, it sounds like but because they have to at some point, right?

Alexa King:

Well that's just a life of a board of Directors.

Brian Contos:

Well, it's great to hear that message has up-leveled to the board and this is being taken seriously. And people like yourself are now being involved with public companies like that.

Alexa King:

Yeah and that's actually one of the many reasons that a strong partnership between the CISO and the GC in the area of cybersecurity can be valuable to your company. A board is going to want to hear a regular update and they're going to want to see that partnership. Boards want to have a sense of comfort that executive management is doing all it can. And I think that seeing a strong partnership between CISOs and GCs can help get them there.

Brian Contos:

Yeah and it certainly sends a great message about top-down to the organization that it's a concern for everybody. So, that's fantastic. Well Alexa, as we wrap up here, there's a question I would like to ask everybody on our show and that's who's your favorite superhero or supervillain and why?

Alexa King:

Well, I'll tell you Brian, when I was little I watched a lot of TV. I joke, but it's not a joke that I learned English and everything I know about American culture from TV, rightly or wrongly. And I was obsessed with Wonder Twins and I think part of it is because they were young and I was young, I was an only child, but my best friend and I would often

sort of do the fist bump type thing and pretend that we were Wonder Twins. And there was something really creative about trying to figure out which role each one would take on so that they could work together to win the day.

Alexa King:

And now that I have twin daughters, I sort of have a renewed obsession with the Wonder Twins. I haven't yet introduced them to the Wonder Twins, but it's on my roadmap. And so, I think I would say the Wonder Twins and form of, shape of and…

Brian Contos:

Eagle and shape of a bucket of water.

Alexa King:

Oh, my goodness. Okay, now you're speaking my language, Brian. So yes, I would say the Wonder Twins.

Brian Contos:

That's awesome. Well, thanks so much, Alexa, and thanks to our listeners for joining and be sure to check out other Cybersecurity Effectiveness Podcasts, sponsored by Verodin.