From Tech Talk to Business Impact

A CISO's Boardroom Strategy

Chief Information Security Officers (CISOs) need to innovate, be business-and mission-aligned, and communicate clearly to lead cybersecurity. They must manage up to the Board to be effective. Scott Moser, CISO of Sabre Corporation, discusses his role with KPMG Cybersecurity Services Partner Sailesh ("Sai") Gadia. This interview is part of a KPMG series of interviews with CISOs on Boardroom strategy.

This Q&A has been edited for clarity and length.

Sai Gadia

Scott Moser

Hello and welcome to the series on CISO's Boardroom strategy. My guest today is Scott Moser. Scott is the CISO at Sabre Corporation. Welcome Scott, let's begin with the role of the CISO. How has the role of CISO evolved as it pertains to Board reporting?

First of all, I think CISO has the responsibility to ensure that they understand the purpose of Boards, whether those are private or public company Boards. The Board members are representatives of the owners of the business and have due care requirements that they're fulfilling. The CISO side should understand that the Board members are concerned with business risk. They're there to manage the business risk and so the CISO needs to be aligned to that. It's not nearly as technical an interaction as it historically was—say, 10 years ago when CISOs came in and talked about very technical operations and projects. Now it's more about risk, decision-making and governance. The CISO needs to align to that much better. The second big difference is Boards are engaging much more directly with cyber experts. Ten years ago, my interaction with Board members was with people in suits and ties who had limited knowledge of technology, much less cybersecurity. Nowadays I have three "cybersecurity experts" on my Board who I interact with frequently. The Board's level of knowledge, expertise, and how they think about risk is very different and much more mature than it was 10 years ago. Therefore, the CISO needs to not only understand the technologies and security but needs to be able to translate that into business risk and have business level discussions with the Board members about why we do certain things the way that we do.

Sai Gadia

Scott Moser

That's a nice summary. I've seen and heard similar things. The awareness of Board members has gone up from not being very technologically aware to being tech savvy and adding cybersecurity expertise. This brings me to my next question about SEC requirements. You're a public company and SEC in the last couple of years has issued guidance about monitoring cybersecurity. Have you observed a change in the level of due diligence by Board members?

Yeah, certainly a couple years ago as the SEC's draft guidance came out, there was a lot of concern on part of the Board members about how they should react. I don't think in my case that there was greater diligence into cybersecurity, but more of trying to understand responsibilities and ensure that the business was fulfilling the requirements of the SEC. That sort of subsided though over the past year as people better understood what the SEC was expecting. There were a couple court cases that also got resolved and it got back to normal where the SEC guidance wasn't necessarily driving behavior or actions, rather it was informing things. I have not seen a significant change other than awareness on part of the Board members. After the initial 12 months of reactionary behavior, it has come back to: Let's do governance the way we've done it.

Some good points and in relation to that, have you seen situations where the lines get blurred? Have you seen situations where Board can sometimes veer into the management realm?

I certainly know that it's the case for some businesses, but both my previous CEO and my current CEO did a very effective job at maintaining a boundary and made it very clear to the management team, what that boundary is and how to manage that. It's really that the Board members are seeking answers, but not attempting to provide us with direct guidance or tell us how to fix a problem. They are just trying to understand what our approach is to do it.

In summary, I am hearing that the CEO has an important role in establishing the delineation. We'll switch over to talking about Board meeting preparation. When you go present to the Board, CISOs typically collaborate with corporate technology and business units. So how do you go about doing that?

Fortunately, my CIO and my CEO allow me to determine what it is that I want to talk to the Board about. And we've got into a cadence of topics. I do have quarterly interactions with our Chief Product Officer. I meet with our commercial leaders so there's good alignment and feedback on the risks that we need to deal with. As I prepare the materials, they're reviewed by my CIO, by our Chief Financial Officer, Chief Product Officer, and our CEO. We align with the talking points in advance to make sure that we're all comfortable with what's being said. Cyber is one of those topics where the wrong words said the wrong way can create unintended consequences. We're careful about the material that we present, how it's discussed and how we engage. But I think because I've been at this for six years and have almost 10 years of experience, I have a lot of leeway and trust from my leadership to do that.

Sai Gadia

Scott Moser

Trust seems to be an important factor. The conversation becomes a lot richer when there is trust between the CISO and the executive team as well as the Board. I remember speaking with another CISO and they mentioned about the unintended consequences of using words the wrong way is akin to saying 'Fire' in a movie theater.

In this job, having trust of the Board members is extremely important. Also, when you're working through a new CISO position and you get interviewed by multiple Board members, it's a pretty good indicator of their level of interest: How you engage with them and good communication are extremely important, not only to the senior management, but also to the Board members.

Absolutely. We'll shift to our next question: What topics are Board members interested in hearing about and how have you seen that change over the years? I feel AI is such a hot topic. Is AI coming into those conversations and what are you getting asked about AI if you are being asked?

I'll start with AI. AI is important because we're a software technology company investing heavily in AI. The Board wants to understand what our strategy is to protect AI and how we are convincing our customers to trust us with the use of AI. This has gone on for at least the past year or so.

In general, one of the biggest growth areas in discussion with the Board has been the threat landscape over the years. In the early years there weren't as many, and I think the landscape was a lot simpler. For example, in my Board meeting today, I'm going to talk about Chinese nation-state attacks, how that relates to us, and how we think about that risk and what actions we're taking to do to manage that risk. A second normal topic is investment level: I always get asked whether I believe we have the appropriate investment level. As you can imagine that question creates interest with the CFO and CEO every time that is asked. But because we do preparation, we're aligned, we're transparent and we always answer the question very well. Coming back to due care, I think the Board members want to make sure that we have reasonable investments in cybersecurity that create reasonable results. They want us to get an external security maturity assessment every year, and they look at those results on the CMMI scale and That's sort of like our "grade card": investment versus results and maturity. This is a topic that we typically talk about and there are other results that I typically show. I don't show a lot of metrics, but I do show a few consistently. One that we've got aligned around obviously is the number of security incidents we have and then more importantly the time it takes us to contain those security incidents. When I first got here, we weren't tracking that at all. So, I started tracking that and we were able to show very good decrease over the years with increased investment, much shorter time to contain security incidents.

Sai Gadia

Scott Moser

Excellent, it seems like there is a fair bit of education there. Apart from talking about the company initiative, it seems like you educate the Board on threat landscape, and you mentioned some of the nation-state attack vectors.

Obviously, that's helping the Board understand: Yes, the money we're putting into the program is delivering a desired business outcome of less risk because of security attacks. The other thing we look at is we talk a lot about customer and commercial impacts. How do our Business-to-business (B2B) customers (because we're a B2B business) look at us in terms of our ability to protect their information? Is that helping us win deals or are we losing deals because of it? We always talk a little bit about how our customers look at our program. And then finally, if we ever have incidents, we talk to the Board about what happened here, here's why there was a gap, and here's what the threat actors did. Fortunately for us, those incidents haven't happened for quite a while, but should it happen again, I'm sure that that will be on. Every year I always talk about what I'm trying to accomplish in the next year. You're understanding here's the results that we achieved this year, but what am I doing to manage the risk that's coming in the next year based on new external threat actors or things like that. And how is it that we're evolving through that and then how's that aligned to investment changes.

I think this is probably one of the most important skills for a CISO: You take what is typically a very technical, complicated topic and you simplify it because typically the Board members are not technologists themselves, they're business leaders but you want every one of the Board members to understand very complicated technical topics in a simple way. So, there's lots of analogies, there's lots of definitions and simplifications. It's very important because the CISO's role is to help these Board members understand what you're telling them. If you're up there trying to impress them with your technical knowledge, you're completely ineffective in my opinion. So yes, education is a big part of the responsibility.

Sai Gadia

Scott Moser

Excellent. Which brings me to my next question and a related one, which is what would be some essential attributes for CISOs for managing a Board? Seems like you just articulated one. What else would you consider as important attributes?

Good oral communication skills are essential. You know, public speaking skills and good decision-making skills are important. To be able to go in and say, here's what I'm doing, here's why I'm doing it. Negotiation is always important, as well as being able to work with various parties, like the Chief Product Officer. There are times where we must have discussions about gaps as well as why that isn't. The last thing you want to do is get into arguments in front of the Board where they see management is not aligned. On a particular issue, that's just not what the CEO would want to have happened. So, negotiation skills are particularly important and obviously you should have somewhat of a technical background. The stronger technical background you have, the better suited you are to be able to deal with, you know, very high-tech enterprises. Understanding AI and all the security issues is not a simple thing. We're all learning, so you must have good skills to be able to take very technical things and sort of wrap them up in much simpler ways.

Since you mentioned earlier that AI is a topic of interest given your industry and how technology is core to what you do. I am curious about the impact of AI on security. How has the landscape shifted in the last year or two?

Just about every one of our major security partners are all-in on adoption of AI to improve the quality of their product. AI is becoming a feature to make the use of security products and tools simpler, to make them more effective, and to make them faster. I'm very aligned to that. I don't think there are too many security teams that can afford to build security tools themselves. We have some developers who do cool stuff: develop security solutions that we either cannot buy or are expensive to purchase. AI has become a very big part of the security tool portfolio, and I think that that will only grow because we've seen the first wave of attacks where threat actors were using generative AI tools to launch attacks. If we're not using AI to defend ourselves, we're going to be at a major disadvantage over time.

Sai Gadia

Good to hear that perspective both from the product side (vendors embedding AI in their cybersecurity products) as well as your organization trying to do some hands-on AI security. As we move towards the latter part of this conversation, I would like to discuss a couple more topics. First is around metrics. Obviously, we've seen shifts: you mentioned your own journey from the early days of not having metrics to creating some useful metrics such as mean time to remediate. In your experience, how has the landscape shifted since its early days? Are there opportunities to come up with better metrics?

Scott Moser

I've worked closely over the past few years with a consultant who came up with the concept of outcome-based business metrics and I really like that. The purpose of metrics for my team and I is to understand: Is our security program working effectively? Are we accomplishing what we're trying to do? Then choose metrics that appropriately align with the goal and accomplish the outcomes that you want. We have 50 to 60 management metrics that we look at once a quarter. The entire team gets together to discuss any gaps and figure out how to get better. However, there's only 13 metrics that I bring up to my senior leadership team, the CEO and the CFO. We talk about these metrics once a quarter and it's this idea of outcome-based metrics, which we call the Security Profile. It's a weighted average of those metrics on a scale of 0 to 100. We aim to be at 80 or above on all these metrics, however there could be gaps around software development for e.g., time to remediate software vulnerabilities, or time to remediate infrastructure vulnerabilities. Going to the Board, the only ones again I really talk about: Number of security incidents and time to contain security incidents. If there's another challenging area where I see a gap, I want them to know that we have a gap and what we're doing about it such as remediation of vulnerabilities in our software before an attacker does, because we don't want to be the next software company in the news. If there is a gap, it's better that I tell them before they end up reading about it in the newspaper one day. That would not be good!

No conversation around data and metrics in cybersecurity is complete without a discussion on cyber risk quantification. Is that something you think of as a management tool or is it something you use to go in front of Boards?

I have used FAIR model for quantification in the past and it's very complex and resource intensive. The question in my mind is: Is it helping me make better decisions? And I have not been able to justify that because I believe one can use a good qualitative risk program and come up with the same decision. That begs the question: Why do we use quantification? I think FAIR model came out of the insurance industry: what's our expected loss and things like that. I don't think that level of resource-intensive detail is necessary for my business to make better decisions. I think we make good decisions, understanding our top 10 risks and communicating that risk qualitatively. I don't get to the level of: I expect that we're going to have this amount of loss from this particular risk in 2026. There are more important things that I can do with limited resources than quantify risk. That's sort of where I'm at on that.

Sai Gadia

Thanks for sharing your perspective. That brings me to the end of the prepared set of questions. Scott, is there anything we didn't cover that would be useful for readers to know? Maybe a message for newer CISOs aspiring to have the opportunity to present before their board.

That brings me to the end of my questions. Thanks for your thorough responses. For more information about Boardroom strategies, check out KPMG's Board Leadership Center and our thought leadership on cybersecurity.

Scott Moser

I've talked with a lot of CISOs and in their roles they probably have one of the greatest influences on Boards such that they could create great concern for Board members. Board members read the cybersecurity headlines, and they probably sit there and think: Gee, can this happen to us? And what if it does, how is the company going to handle it? The message that ultimately needs to get across to the Board is: We're making good decisions based on the nature of the risks and how much risk we're willing to take; we're not going to be able to eliminate every risk. I think that is the single most important thing, in my opinion, that a CISO can bring when they engage with a Board.

> **It's important that you don't send the Board into a frenzy over cyber risk.**

Contact us

Michael Isensee
Partner, Cybersecurity and Technology Risk US Leader
KPMG LLP
E: misensee@kpmg.com

Sailesh Gadia
Partner, Cybersecurity and Technology Risk
KPMG LLP
E: sgadia@kpmg.com

Scott Moser
CISO
Sabre Corporation

Some of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us: **kpmg.com**