# Top 10 questions about CISO's boardroom strategy

Chief information Security officers (CISOs) need to innovate, be business/mission aligned, and communicate clearly to lead cybersecurity. They must manage up to the Board to be effective. Matt Posid, Principal and Chief Security Officer, KPMG LLP, 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**

**Matthew Posid**

## 1

Hello and welcome to the series on CISO's Boardroom strategy. My guest today is Matt Posid. Matt is KPMG US firm's Chief Security Officer. Welcome Matt, let's begin with the role of the CISO. How has the role of CISO evolved as it pertains to Board reporting?

I think it's evolving in a couple of ways. I'd say Boards are a lot more interested in this topic than they ever have been before. That interest has led to an evolution in how a CISO needs to engage with the Board. I think the CISO of 10 years ago was putting a lot of data and metrics in front of a Board, and providing jargon-filled updates, and the Board's eyes were probably glazing over. Today, a CISO should be having business conversations about how cyber is integral to trust, to client expectations, to regulatory expectations, and to the brand. I was in front of our Board 3–4 hours ago, and these were the conversations we were having.

**Sai Gadia**

**Matthew Posid**

# 2

A couple of follow-up questions. First is around topics. What topics have Board members been interested in hearing about? And then related to that, I think you touched briefly about metrics. What has your observation been in terms of shift from tactical and more compliance-driven metrics towards fundamental metrics?

Let's talk about topics first. Our security briefings generally follow a repeatable pattern. The first section is typically about the dynamic operating environment and how it's changed since our last update. How are threats evolving? How are regulations changing? What are the technology or business needs of the Firm and where do those needs put increased pressures on a security program? So, we spend the first part of our Board conversation talking about the shifts in the environment, because that creates important business context for the rest of the discussion. If we have a static security program and the world changes, we're going to find ourselves in trouble. Next, we shift to a discussion about how we're handling the changes, how we are responding to it, and where we might have taken new or different risks to enable business to happen. We also discuss where we have felt a need to tighten controls and why.

Then we shift into discussing what we see coming over the next six months, discussing the risks that keep us up at night, and how we're attempting to manage those concerns. And lastly, we shift to discussing what the Board can do to help us. That's the general format we are always sure to cover, but we certainly add in current events or topics they may have heard about. For example, during our recent discussion we discussed ransomware cases where the total economic impact crossed the $1 billion threshold. It was important to help the Board understand the magnitude of the impact, since many historical cases had been in the low 10s of millions of dollars. When the number goes from 10s of millions to billions of dollars, that's a data point we want to get on their radar.

Switching to metrics, I think metrics can get dangerous with the Board, because context is so critical to interpreting numbers properly. Let's say I put the number 40,000 vulnerabilities in front of them. Is that one vulnerability on every one of the 40,000 laptops at the Firm, and with one patch we're updated? Or is that 40,000 discrete vulnerabilities that we must patch in 40,000 different ways? What it takes to address those two things is radically different, and with just a number, the Board can't tell whether 40,000 is good or bad. Further, just talking about the metric doesn't let the Board know whether those 40,000 vulnerabilities are critical issues that are exploitable, or if they're low risk vulnerabilities. Data without context can inadvertently cause the Board to focus on the wrong problems.

**Sai Gadia**

**Matthew Posid**

# 3

That makes sense to me as a practitioner. I recognize that metrics without context can be difficult to absorb. I would like to get your perspective on where you think CISOs need to focus their energy on: Adding context to the metrics, or a different fundamental set of metrics that are so straightforward that we don't need to explain.

I think it's more the former with a little bit of the latter and I'll explain why. Yes, I think we need to bring context, and this goes back to how CISOs and Boards are having different conversations today than they used to have. CISOs must bring the business context and put metrics in perspective or else they're not doing their job. The reason I think it's more the former than the latter is that the core and fundamental metrics may change over time, and they may even change based on industry.

We had, maybe three years ago, what we called our key cyber metrics. And what we did was define a set of five key metrics that were so egregious, the only acceptable number was 0. For example, it wasn't how many vulnerabilities we had, it was a combination of how many critical vulnerabilities we had, that were on CISA's known exploitable list and were outside of our patching policy for remediation. If it's critical and out of patching policy and we know it's being exploited somewhere in the industry, the number we want is 0. For this set of five metrics, what we did was continuously brief them to the Board until the number was 0. Once they got down to zero, we retired the metric and found new things to pursue. This is why I don't think we can have a prescribed list of metrics—if I were still briefing on the same metrics, I would have very uninteresting charts that just show zeros for a really long time. Metrics have to change to match what we're currently focused on.

When I talk with the Board about metrics, I try to focus on three key things. One is the direction of change. Is the number getting bigger or smaller? Two is the rate of change. Back to my example, last month there were 40,000 open vulnerabilities and this month there's 39,980. It's moving the right direction, but That rate is too slow. Three, am I content with the direction and the rate. Generally, the Board doesn't have enough security expertise to know if the rate is OK. They're looking for the CISO's opinion. In my briefing today, we talked about some vulnerabilities, the direction of change, the rate, and why we're actually very comfortable with these numbers.

**Sai Gadia**

**Matthew Posid**

# 4

Yes. It's interesting to know that the Board leans into your perspective as well. That got me thinking about our discussion about the manufacturing company and the healthcare company, versus us as a professional services firm. How would you describe the challenge of running security here versus at a company that manufactures vehicles, or a company that offers healthcare solutions.

I think we have to run security in multiple different ways here, and I suspect this challenge is true in most organizations. We are not one homogeneous company. At a minimum, we have three core functions: Audit and Assurance, Tax, and Advisory, and each of them have different needs for velocity, technological evolution, rate of change, and speed to market. Each of them has different risk tolerances too.. But, even if one of those businesses is comfortable with a particular risk, we can't let that expose another part of our business who may not be comfortable with it. A security leader must be able to lead a program that can adapt and be agile enough to meet the needs of those different constituents, while not allowing them to expose each other to risk. I talked about our three core functions, but we're now also a law firm with KPMG Law. We're also a financial services organization with KPMG Corporate Finance. And all of these organizations introduce unique requirements for our program that must co-exist, even when the business needs or risk tolerances are different. Before I came to the firm, I was the CISO of the Central Intelligence Agency, and their needs were different than KPMG's needs. As a CISO, you must build a program that recognizes and responds to the unique business needs and risk tolerances of the organization you're supporting—there isn't a one-size fits all answer.

**Sai Gadia**

**Matthew Posid**

# 5

Which brings me to my next follow up question about essential attributes for CISOs for managing up to the Board, particularly when they're seeking Board's attention for large strategic cybersecurity investments in your experience.

Why do you think that occurs?

> Fast forward to two years, and we will be defending against cyber threats that have not been invented yet, with technologies that have not been invented yet.

I think there's probably at least three. The **first** is the CISO must show up as a business leader, not just a cyber leader. The Board is focused on business risks. CISOs must be able to talk about cyber risk in business context. They must understand that in some cases we minimize business risk by accepting some cyber risk, because things like speed to market also matter. If a CISO thinks cyber risk is all that matters, they're in the wrong room.

The **second** thing I'd say is they need to avoid speaking in jargon There are many cyber leaders that will try to use complex language during their time in front of the Board, and it doesn't help with a dialog.

I think sometimes it because security leaders are attempting to teach the Board how to run cyber security. That's not what you're there to do. You're there to explain what you are doing and give them confidence that you've got it under control, but you don't need to teach them how to do your job.

The **third** area, and we talked about this a little bit earlier, is to talk about the dynamic nature of the job and the operating environment. If we fast forward two years, we will be defending against cyber threats that have not been invented yet, with technologies that have not been invented yet. And when boards think about programs, they often think about what does done look like? What is enough? When have we reached our goal? And the answer is never. We are operating in an environment that is continuing to change, so we must constantly change too. The bad actors are evolving, and I've got to move faster than the bad guys. And so, talking about that dynamic nature, the constant evolution, the constant need to keep pace in that environment is critical.

Overall, The Board has a critically important role in making sure the cyber program is effective, and that starts with good, strong governance. They need to make sure they're hearing about this topic on a periodic basis. The very last question I got from our own Board earlier today is whether our cadence is frequent enough in today's world, or if we need to change it. That's the exact kind of thinking a Board should be having.

**Sai Gadia**

**Matthew Posid**

# 6

Excellent. Speaking of Board meeting preparation, how do you go about collaborating? Because when you go to a Board meeting, you have representatives typically from corporate technology group, and you have the business units. How do you ensure you have a good outcome at these Board meetings?

My answer may not be what you expect. I never share my Board briefing with any of those people in advance. The Board briefing should not be a surprise. It should be a summary of what has transpired since the last Board discussion on cybersecurity. And since the last Board discussion, I will have had significant engagements with all the stakeholders you mentioned. We have routine engagements with our Chief Digital Officers. We have routine discussions with risk management in second line, and with internal audit in third line. We are frequently talking with the business. We continuously seek to understand their perspectives, and we have a highly effective collaborative relationship. Because of that, when it comes time to write my Board update, I have their perspectives already. I know where we're going too slow or where we're too conservative. I know where we've helped them solve a critical business problem. And as a business leader, I share the good and not-so-good aspects of my program with leadership. If you've got the right relationship with your business partners on an ongoing basis, you don't have to get them to review slides–you're telling a shared story.

**Sai Gadia**

**Matthew Posid**

# 7

That's some interesting perspective and turned this question on its head! In terms of Board meetings, we discussed a fair bit of interest on part of the Board, the Board leaning in on. The CISO, the Board trying to respect its role versus management. Do you run awareness sessions for your boards on the topic of cybersecurity? Have they asked you to do Board awareness sessions and I'm curious what some of those topics have been?

> Going with the old axiom, fight like you train, train like you fight, we want to make sure our exercises simulate an actual response.

I view any engagement with the Board as an opportunity to create awareness. Whether that's the overt purpose of the engagement or not, there is always some aspect of awareness that I want them to come away with.

More broadly, we have our Board members, including our external ones, take our general security awareness training. We want them to be cognizant of the top-of-mind security issues that we think are important for every KPMG professional. And that training evolves every year to focus on changes in the threat environment, changes in the regulatory environment, and changes in what our clients are focused on. Although this training is not unique to Board members, it gives them a perspective of what is relevant this year.

Another thing we do, and it's the thing we do that is most tailored to this question, is we do Tabletop exercises. We walk them through exercises, and we do it in one of two ways. Either we will exercise the management committee and provide a readout to the Board, or we will exercise with the Board as well. We generally do more of the former, and the reason for that is in a major event, it's normally a management decision on what we're going to do, and the Board is kept aware and apprised of the situation.

Lastly, and this is more of a pull from the Board rather than a push from me, is event-driven or ad-hoc awareness. I mentioned earlier, we often get questions about current events such as about things members may see in the press, and they ask what we can tell them about it and if it impacts the firm or our clients. And anytime we have a conversation about those types of topics, it's another opportunity for education. I don't let any engagement go by without using it for awareness in some way.

**Sai Gadia**

**Matthew Posid**

# 8

In the few minutes we have left, I want to ask you about Artificial Intelligence (AI). Obviously, that remains a hot topic. What are you getting asked by Board members about AI and other emerging technologies?

The biggest thing we're getting asked about with respect to AI is concerns related to deep fakes, impersonation, employment fraud, and things of that nature. As I'm sure you know, these threats are not new. Employment fraud is something employers have been dealing with since the dawn of time. Impersonation happens all day long, especially on social media platforms. Somebody sets up a fake profile pretending to be from the Firm and we have to work with a social media provider to clean that up. These are not new risks to the Firm. But, deepfakes are a new tool in the toolbox of the perpetrators. This tool is advanced, and it's got capabilities we haven't seen before. The good news is that some of the controls we put in place to address the longstanding risks also help address the deepfake risks. For example, we see news reports about threat actors impersonating CFOs, calling the accounts payable department, and seeing if can trick them into sending money. We've been worried about payment fraud in general and we have robust controls to help address that. Some include things such as change controls over vendors' registered bank accounts, or requiring them to tie a payment request to a specific purchase order number. These controls, if enforced, help protect us from emerging risks such as deep fakes because the impersonator won't be able to satisfy those criteria.

Got it. We are down to our last couple of questions.

**Sai Gadia**

**Matthew Posid**

# 9

Have you ever been asked about how much investment in cybersecurity is enough? I've been asked that question by a CEO of a very large company: Sai, where do I draw the line on cybersecurity? How much is enough? That CEO potentially thought that his company was spending too much on cybersecurity. I am curious if you've run into those questions and how much investment in cybersecurity is enough for our organization?

Yeah, I have been asked that here and I was asked that at my prior employer. There's a whole lot of literature on this topic, and there is no right answer. If you look at some of the industry literature, you'll see trends anywhere from 6% to 12% of IT spend.

That's a pretty big range with variances per industry, with outliers on both sides of that. And the numbers lack context. Are we starting from a mature program or not? What contractual requirements did the organization sign up for? I think it's hard to pin down a precise number. I think it's much more important to look at what your risk tolerances are around certain areas of security, how your organization's control environment lines up against those risk tolerances, and if we are taking on risk we're not comfortable with. If we are, we need to look at what it costs to put in place controls to buy down that risk. The other reason I don't like discussing a percentage is there are ambiguous definitions about "what is cyber" The identity mechanism that we use to run enterprise IT, but that also absolutely provides security capabilities—Is that Cyber spend or IT spend? The firewalls we use as network routing devices and security appliances—is that IT spend or Cyber spend?

The attorneys that help us evaluate an incident, is that cyber spend? I don't know if there is an industry consensus on what belongs in the definition. And if you don't know what belongs in the definition, you can't possibly name a percentage that is appropriate because we're talking different things. Unless we agree on precise definitions and control for context, it's hard to give a percentage.

What my leadership now asks me is do you have the money you need to help us stay within our risk tolerances? Not: Is 6% enough? I think that's a good way to think about it.

**Sai Gadia**

**Matthew Posid**

# 10

I like that. Last question: Is cybersecurity intertwined with resiliency and particularly in the context of couple of other companies we discussed earlier. Do Boards view these topics as intertwined?

At KPMG, absolutely. In fact, in my role as Chief Security Officer, I have our cyber program. But I also have our physical security program, insider risk, safety, resilience, and compliance. All of them were brought together about 2 1/2 years ago. We made an intentional decision to bring together what used to be several different siloed programs. There's absolutely an interconnection between cyber and resilience, and the briefing I gave the Board earlier today included both those topics and how they work together to protect our firm. I don't think you can have a rich conversation about cyber without talking about resilience.

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

# 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



**Matt Posid**
Principal and Chief Security Officer
KPMG LLP
**E:** mposid@kpmg.com


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**