The strategic CISO: Aligning cyber risk with growth and governance

A CISO's Boardroom strategy

Chief information security officers (CISOs) need to innovate, be business and mission aligned, communicate clearly to lead cybersecurity, and must manage up to the Board to be effective. Param Vig, CISO of Solventum Corporation, discusses her 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

Param Vig

Hello and welcome to the series on CISO's Boardroom strategy. My guest today is Param Vig. Param is the CISO at Solventum Corporation. Welcome Param. Let's begin with a little bit of background about your organization. As a global organization, what's unique in your threat landscape compared to other industries such as banking or technology?

We are a healthcare and medtech company and what is unique about our environment is that cybersecurity risk cannot be separated from customer service, i.e., patient safety, and from continuity of care. To give you some context, our products reach 90 countries through more than a hundred thousand customers. To enable all this, we operate across clinical workflows, medical devices, and complex global supply chain—all of which are supported by the backbone of an IT function. So, the company operates a highly interconnected technology-based ecosystem where any cybersecurity incident can have a direct impact on patient health.

So back to your question, compared to financial and technology industries we not only need to focus on protecting sensitive data but also focus on operational resilience, integrity of our devices, and the trust placed in us by hospitals, healthcare systems, and most importantly our patients. Because of the sensitive and critical nature of services, any healthcare company must have the ability to run 24-7, even under adverse cyber conditions. This differential reality shapes our daily approach to managing cyber risk—where we work on the resilience of our business, the safety of our patients, and on trust in our markets.

Sai Gadia

Param Vig

How has the role of CISO evolved as it pertains to Board reporting?

The Board sees the CISO as its independent risk adviser for cyber. The CISO's role is to help the Board fulfill its fiduciary responsibilities and to help it govern the area. So CISO's role requires that they provide a transparent view into what risks impact the company's goals or it's market presence, they inform how cyber risk fits in the overall portfolio of enterprise risk management (ERM), and they gain alignment on the appetite for residual risks.

Today, the CISO is not engaged in educating the Board on the technicalities of cyber or to merely provide reports on incidents. Instead, the CISO is engaged to provide an understanding of the cyber risks inherent in the business—in digital systems, supply chains, connected medical devices, use of AI, etc. They are engaged to present the company's capabilities to address those risks, to inform the Board of independent verification in how the company compares with its peers, to update adequacy of funding, and to gain alignment on a roadmap that shows how the risk will continue to stay managed. The Board also looks at the CISO in how they are helping the company win new markets through published certifications or where fast-changing regulations can potentially impact revenue continuity.

In summary, the Board dialogue in recent years has shifted from updates on technical metrics and architectures to enabling governance oversight, risk management, and strategic growth.

For Board meeting preparation, how do you go about collaborating with the corporate technology and business units…. from preparation to presentation?

In most healthcare companies, cyber risk touches product, supply chain, business operations, corporate systems, and sensitive data. So, any preparation for the Board is literally an exercise in gaining broad executive alignment.

When a CISO presents a comprehensive view of enterprise-wide cyber risks to the Board, they are also indirectly representing the relevant functions and business line leaders. So, the Board preparation must be jointly developed with their collaboration because it will reflect to the Board how those functional and business line leaders are aligned with the enterprise cyber strategy, how they are allocating resources for cybersecurity, and progressing on executing commitments. It is also important for the CISO to have a regular review with the senior officers of the company so there is a feedback loop between bottom-up communication of aggregate risk and top-down guidance on risk appetite. Similarly, it is important for the CISO to conduct ongoing conversations with external financial auditors because they usually have a good perspective of company's

Sai Gadia

Param Vig

overall risks, and this review can support auditors with new insights or conversely support the CISO with calibration of severity of impact. From my experience in serving multiple Boards, I believe about 60 percent of a CISO's time must be spent in gaining alignment from across the business, and this alignment should not be done as a discreet activity. This should be part of a continuous partnership through regular operating reviews that builds common ground among executive stakeholders. If done right, this joint preparation for the Board ceases to be a one-sided hustle of CISO galvanizing across multiple company executives. With continuous partnership in place, the need for preparation becomes mutual. Likewise, when the business and functional leaders are preparing their strategy and long-range plan updates for the Board, they also proactively seek input from the CISO. This symbiotic work enriches the message to the Board and helps in earning their confidence and trust.

The SEC in the last couple of years issued guidance about Board monitoring for cybersecurity. How has that changed the level of due diligence by Board members?

Certainly, the regulation has converted this area into a topic of shareholder value preservation. The SEC has mandated intentional structures for Board oversight where there is a dedicated Board member aligned to this area, where the Board focuses on the company's processes to assess materiality of any cyber incident.

So why was this needed? Simply because for years media was reporting material cyber incidents that were causing damage to financial performance, shutdown of operations, litigation, negative impact to stock prices—all of which were impacting shareholder value. Over time, when enough analysis was performed on the root cause for several incidents, it highlighted inadequate capital allocation toward cyber, inadequate skill sets supporting the function, or weak controls enterprise wide. To address this on a proactive basis, SEC regulation now asks public companies to report within four business days if any cyber incident is deemed material. The SEC also requires public companies to provide a narrative in their annual report that explains the company's cyber risk management practices. In doing so, the SEC has made cyber threat a topic of shareholder interest. If you look closely at the voting guidelines issued by some proxy advisers such as Institutional Shareholder Services, you will notice they are calling out many SEC regulatory requirements for incident reporting and cyber risk management in their advisement for proxy voting.

Sai Gadia

Param Vig

That's some great advice for collaboration. What topics are Board members usually interested in hearing about? How has that changed over the years?

Boards are asking questions about what framework is in place to assess materiality, who runs it, how they will promptly report, to which stakeholders, and most importantly how the Board will be informed during the lifecycle of an active incident that is assessed as material.

So back to your question, this regulation has helped the Board shift their lens from the traditional question of "Do we have a CISO who knows how to do their job?" to a more evolved perspective of "Does our company have robust practices to assess the impact of potential cyber incidents and promptly disclose any material incident that could raise shareholder scrutiny?"

Board members want to learn cyber risks manifesting within the company because of its model and ways of working. They want to align with the risk profile of the industry in which the company sits. They want to be informed about top cyber risk priorities. They want to see if timebound well-funded plans exist to address those priorities and if progress is occurring per plan.

As for the topics, there are some common themes. Board members are interested in understanding the maturity of the company in managing these internal and external risks. They want to see the maturity scores of the company compared to peers and competitors in the market.

Board members want to assess if sufficient financial allocation is being provided. They want to understand how their operational cyber budget compares against peers in the industry.

Board members want to have oversight into the effectiveness of most critical cyber controls that minimize the potential to disrupt the care delivery, so they want to see an operational scorecard.

Board members also want to understand the trajectory of cyber risk over the next three to five years and how it might impact the strategic growth outlook. So, you want to see an investment road map that commits that the cyber risk will stay managed.

All these are different topics from the ones I have seen about five years back where the content used to be technical with architectural diagrams and a lot of translation of cyber jargon. Today's Board wants to understand the relevant cyber risks, how these are being managed, and what the residual cyber risk is.

Sai Gadia

Param Vig

AI remains a hot topic. What are you getting asked by your Board members about the impact of AI on security threats? Any other emerging technologies or attack vectors?

Board members understand the duality of AI. AI presents significant opportunities for value creation, but at the same time, AI-powered cyberattacks have achieved unprecedented scale and speed.

Boards are interested in how the company is performing the balancing act between speed and diligence. They are asking management to demonstrate how AI is being used responsibly through policy guidance, governance structures, and training of the global workforce. Boards are seeking to gain comfort on diligence in selection and use of AI technologies, in confirming integrity of data and the functionality of models, and in protecting IP and privacy.

Boards understand that threat actors are developing new ways to attack through use of AI. Also, new weaknesses and control gaps are emerging in use of AI due to the incredibly evolutionary nature of this technology. They want the management team to help them understand where these risks manifest most critically within the company and in face of fast-changing technology, how the exposure of the company is changing.

Boards also understand that the potential of AI cannot be achieved without a workforce that has been upskilled in responsible AI use. They want the management team and CISO to share status and progress in workforce development on leveraging AI responsibly.

Several medtech companies are learning to embed AI in medical devices and software to enable productivity with the physicians, the hospitals, or the patient performing self-service. The Board likes to understand how the use of AI does not negatively impact functionality of the products and safety of the patients. In essence, Boards want to ensure that innovation and value generation do not outpace safety, security, and risk management controls.

How can AI help address both new and legacy cybersecurity challenges?

AI serves as a powerful force in tackling long-standing cybersecurity issues while also enabling effective defenses against emerging threats. For legacy challenges, one of the most persistent issues is the overwhelming volume of alerts and resulting false positives. AI can significantly reduce this noise by identifying complex patterns with greater accuracy, enriching signals with context, and operating at scale. Vulnerability management is another critical area. Traditional enterprise patching cycles often take weeks or months, leaving organizations exposed. AI can drive more effective prioritization by focusing on vulnerabilities with the highest likelihood of exploitation,

Sai Gadia

Param Vig

helping reduce backlog and accelerate remediation. Legacy IT environments remain highly susceptible to attacks. AI can automate routine and repetitive tasks, freeing up skilled engineers and architects to focus on higher-value activities. Identity sprawl has further complicated traditional security controls. AI can dynamically adjust authentication and access decisions based on contextual signals, improving both security and user experience.

For emerging threats, AI enables faster, more adaptive defenses. AI-powered attacks can occur in seconds, far outpacing human response times. However, AI-driven detection and response systems can act in near real time to contain threats and prevent lateral movement.

Additionally, the adoption of large language models (LLMs) within enterprises introduces new risks of data leakage. AI-based controls can monitor and analyze data flows to detect and prevent sensitive information from being exposed to public LLMs, helping enforce policy and protect critical data.

What are a couple of essential attributes for CISOs for managing up to the Board particularly when seeking their attention for large strategic cybersecurity investments

The starting point is to understand the perspective that the Board members have in fulfilling their roles. To gain that perspective, there are two avenues that CISOs can pursue. One avenue is to assume a Board seat within a nonprofit, or a private or public entity, and bring the external perspective back into their operating role. The other avenue is to get formal education in corporate governance.

CISOs should work with the intention of earning the trust and credibility of their Board, which requires the CISO to elevate themselves from being a technical leader to being a business leader. They must demonstrate business acumen and a financial mindset that translates funding requests in terms of business enablement. They must balance their narrative between cyber as a threat prevention to cyber as an enabler of growth, revenue generation, and customer retention. They must bring a pragmatic mindset in their requests, where they are not overly indexed on narrow control needs but articulate to the Board how investment in cyber results in optimization of enterprise-wide risks.

CISOs should invest sufficient time in framing the cyber investments in terms of business outcomes such as coverage of assets under protection, regulatory approval cycle time for

Sai Gadia

Param Vig

medical devices, cost of products shipped through a secure factory, impact to customer trust with industry aligned SLAs, retention of revenue through approved certifications, and so on. A seasoned CISO should be able to provide the Board with clear choices and recommendations for investment ask and how those choices bring the cyber risk to a level acceptable by the Board.

While on the topic of investments, have you been asked how much investment in cybersecurity is enough?

It's not uncommon for a CISO to be challenged to justify cybersecurity investments. In my experience, business stakeholders—often competing for the same pool of funding—frequently ask how a specific investment level is determined. The reality is that no amount of spending can guarantee complete security.

In these discussions, it's helpful to reframe the conversation around aligning investment to the organization's risk appetite. This includes demonstrating how spend:

- Advances cybersecurity maturity
- Positions the company closer to industry peers
- Strengthens brand trust with customers
- Helps avoid the costs associated with potential breaches
- Drives measurable progress (e.g., reducing legacy risk, expanding protection coverage, and increasing business adoption).

In my experience, Boards generally recognize that cybersecurity is an evolving risk area that requires sustained and adaptive investment.

Sai Gadia

Param Vig

I really like how you suggested reframing the conversation around aligning investment to the organization's risk appetite. Switching to another classic topic of metrics/KPIs: Have you seen a shift from tactical and compliance – driven metrics (such as number of vulnerabilities, or number of audit findings) toward a smaller set of fundamental metrics (such as % of EOL and EOS infra, % of infra that is automated via scripts)? What do you find useful for Board reporting?

Boards want to understand how the CISO and management team are overseeing the effectiveness of controls on a regular basis, so they typically request an operational score card. They are not looking for hygiene data on a long list of metrics. They are looking for an index of structural cyber controls.

The CISO should focus on the most fundamental metrics. For those metrics, the CISO should be able to explain why these rank at the top for Board reporting. For each fundamental metric, Boards are not just looking for current value, they want to understand the target that company wants to achieve, how the company determined that target, what the timeline is over which metric target will be achieved, and finally how company is progressing towards that target.

Boards like to see that metrics are not biased toward certain domains and are balanced. A popular scorecard will show key metrics and their targets against an established cyber framework. The conversation centers on a few metrics that are most foundational and leading indicators.

Wow, that's some seriously impactful work your organization is doing. How different is management of OT security from IT security?

Resilience, recovery, restoration matters a lot more in operational technology (OT) security because if there is disruption from a cyber incident, the organization still needs to deliver to its customers and meet commitments. OT security needs to help with availability, safety, and reliability of physical systems because these elements have a direct implication on patient care and safety. Boards view this area against the backdrop of numerous events reported in the press where cyber incidents at manufacturing plants have caused impact to all of the elements mentioned previously.

As you mature your OT security program, what has been the top learning or two about OT security as you update your Board?

Reporting to the Board should begin with helping them understand the unique aspects, the fundamentals of OT security—visibility into the assets at manufacturing plants, how OT security is heavily reliant on partnerships with engineering, product teams, and operations teams. OT security cannot be run as a central enforcement function. Accordingly, the CISO should align messaging with the head of supply chain on roles and responsibilities, and accountability for OT cyber operations. CISOs should be ready to explain the company's

Sai Gadia

Param Vig

comprehensive crisis management process that enables it to continue plant operations, even if they are in a minimal viable state.

CISOs can help their Boards understand the relationship between control maturity and corresponding investments. They can achieve this by sharing relationship between system uptime and endpoint protection, and between legacy obsolescence and exploitability of vulnerabilities. CISOs should articulate that physical and digital convergence at the factory floor creates more risk and requires higher investment for mitigation.

Do you leverage cyber maturity assessments? Is that a management tool or Board-level tool or both?

Yes, absolutely we leverage cyber maturity assessments. And it serves both purposes—as a management tool to understand where the company must invest and make defensible choices as well as a Board tool that enables governance on whether the risk is being managed adequately and in alignment with industry peers.

The cyber function and the management teams use maturity assessments for developing tactical execution plans. The Board will use this as a way to bring risk to the appetite and to get confirmation that continued investments are producing that data of the results.

Anecdote:

At one of my previous roles where I was reporting to the Board on the topic of manufacturing security: The discussion focused around how the company was making investments in leading-edge cyber practices at a site that was to serve its top tier customer, and how the security controls at that manufacturing plant were being developed in partnership with customer's expectations. A roadmap showed how the cyber control implementation was tied to the first wave of production output. With that tie-in in place, the Board became increasingly interested in the progress of this initiative because of the importance of meeting expectations of one of the most important customers of the company. This was a great lesson in how CISOs can spend the time and effort to help the Board understand the business outcomes of their work.

This has been a great dialogue and lots of valuable perspective. Some great advice for fellow CISOs. Thanks for your responses. For more information about Boardroom strategies, check out KPMG's 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

Param Vig
Chief Information Security Officer, Solventum

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**