LTIMindtree

POV

The Role of Board Oversight in Cyber Risk Governance

Why It Matters and How to Get It Right

Cybersecurity is no longer just an IT concern. It has become a boardroom priority.

The realization that strong board oversight is crucial became clear to us during a discussion with a board member from a large enterprise. They mentioned how fundamental gaps in third-party access controls and identity review cycles had gone unnoticed in a core system.

That lapse almost triggered a wider disruption across their network. We agreed that the issue could have been avoided entirely if the board had been involved in the risk review from the start.

A strong reason why Gartner's 2025 cybersecurity trends indicate that board directors and C-suite leaders now view cyber risk as a core business risk, and security and risk management (SRM) leaders are shifting their focus from prevention to resilience. This "when, not if" mindset accepts that incidents will occur, and the real test is how fast the organization can contain the impact and recover.[1]

Additionally, with the Securities and Exchange Commission (SEC)'s 2023 disclosure rules now in force, the stakes have never been higher.[2] We believe boards are expected to move from observers to active guardians of cyber resilience.

One that treats cyber as a purely technical issue is already behind the times. Cyber resilience now defines how well a company can survive disruption, protect its people, and defend its reputation.

In this PoV, We will discuss why it is crucial for boards to actively oversee cybersecurity and what the SEC now expects from them. We will also discuss how cybersecurity professionals like us can step up and address these challenges, especially as cyber risks can significantly impact, or even determine, a business's success today.

What Has Changed
SEC Rules and Impact on the Board's Mandate

The SEC's final rules, adopted in July 2023, introduced two major disclosure-related requirements that directly involved the board:

01

Form 8-K Incident Disclosure

Companies must report material cybersecurity incidents within four business days of determining materiality of the incident. This means boards need to ensure that incident response and escalation procedures are strong enough to support timely and accurate disclosures

02

Regulation S-K Item 106

Annual reports must now incorporate:

- An explanation of the company's processes for identifying and managing cybersecurity risks.
- Role of Management and expertise in handling those risks.
- The board's oversight of cybersecurity threats, including any committees responsible for that oversight

We want to emphasize that this is not just about compliance. It extends into the realm of accountability. High-profile breaches in the past have underscored the consequences of inadequate cyber risk governance by the board, prompting a call for stricter regulatory oversight.

The SEC's enforcement actions send a clear message: Boards must understand cyber risks, ask the right questions to the right people, and ensure that management is prepared to respond effectively.

Why Do Boards Still Struggle with Cyber Oversight?

While discussing with our cybersecurity peers across the industry, we discovered a common thread: despite growing awareness, some boards are facing challenges in fulfilling their role as cybersecurity overseers.

01

Lack of technical expertise

Usually, directors are not updated with cybersecurity concepts, such as identity and access management, zero trust, or threat exposure.

This makes it hard to ask the right questions or challenge assumptions. For example, a board may approve a major cloud program without understanding how access controls or shared responsibility models work.

02

Limited visibility

Without structured metrics such as mean time to detect, mean time to respond, or high-risk vulnerabilities by business unit, boards often lack timely and relevant information.

For example, leadership may only see a quarterly summary that hides growing ransomware attempts or rising phishing success rates

03

Reactive posture

Some boards only engage after an incident, instead of shaping risk strategy early.

For example, leaders may jump into action after a breach hits the news, yet they may have ignored earlier recommendations on backup readiness or incident playbooks.

Strategy and Recommendations
How Boards Can Lead in Cyber Risk Oversight

To meet these expectations, we believe boards must adopt a more proactive approach to cybersecurity oversight. Here are some of the ways to do so:

Figure 1: Foundations of cyber risk governance

01 Establish Clear Oversight Structures

We've been through this entire journey and realized that tackling the challenges mentioned above starts with the board officially appointing a dedicated committee for cybersecurity oversight, usually the audit or risk committee.

This committee can include the Chief Information Security Officer (CISO) or a representative from their team to work closely for regular updates and strategic alignment. At the ground level, this committee provides essential oversight on policies, standards, processes, and stakeholder responsibilities for key cybersecurity roles.

Key actions:

- Define roles and responsibilities for cybersecurity oversight.
- Ensure committee members have access to cybersecurity expertise.
- Schedule regular briefings to be delivered by the CISO and risk officers.

02

Integrate Cyber Risk into Enterprise Risk Management

Cyber risk should not be isolated. Boards should ensure the integration of cybersecurity into the broader enterprise risk management (ERM) framework. This includes:

- Mapping cyber risks to business objectives.
- Evaluating the financial and operational impact of potential incidents.
- Reviewing risk mitigation strategies and risk appetite of the organization.

Boards should ask:

How does Cyber Risk affect our ability to deliver value? What are our most critical assets, and how are they protected?

03

Well-Defined Metrics and Reporting

Boards need visibility into the effectiveness of cybersecurity programs. A CISO must provide clear and actionable metrics that reflect both technical performance and business impact.

Recommended metrics:

- Number and severity of incidents.
- Time to detect and respond.
- Compliance with regulatory standards.
- Results of internal and external audits.

While defining these metrics, some of the key success factors that have emerged include the boards reviewing trends over time. They should also have a clear view of their cybersecurity maturity (NIST maturity score) and develop a well-crafted cybersecurity roadmap that encompasses people, processes, and technology to enhance maturity and growth over time.

04 Ensure Incident Response Readiness

Given the SEC's four-day disclosure rule, boards must ensure that the company's incident response plan is completely disclosure-ready. This means:

- Clear escalation protocols.
- Defined criteria assessing the materiality of incidents.
- Coordination between legal, communications, and technical teams.

We strongly recommend that boards participate in annual simulation exercises to test the company's readiness and understand their role in crisis scenarios.

05 Promote a Culture of Cyber Awareness

Cybersecurity is a shared responsibility, and what has truly worked for our enterprise is fostering a culture where human cyber risks are taken seriously throughout the organization, from the CEO to new hires.

We recall how my team assisted one client in developing their security awareness training strategy, along with recommendations for automating the entire program. This enabled regular monitoring, provided insightful reports on risk and awareness coverage, and included customized training campaigns tailored to individual needs.

Still, our prescriptive approach includes:

- Supporting ongoing awareness and training programs.
- Encouraging transparency in reporting incidents and risks.
- Recognizing cybersecurity as a strategic driver, not just a business expense.

Boards that lead by example set the tone for the entire organization. They must demand real-time visibility. Regulators should anticipate quick disclosures, and resilience has now become a business differentiator.

But technology alone is not enough. To truly lead and excel, organizations must have a partner who can immerse *governance, risk, and compliance (GRC)* into a unified, intelligence-driven framework.

Case on-point

We'd like to highlight a moment when we delivered a cybersecurity governance framework and risk management method for a client struggling with inconsistent controls across business units.

Through our strategy, we helped close basic gaps in access reviews and risk ownership, providing them with a clear approach to managing cyber risk across their lifecycle and ensuring board members' buy-in.

We also utilized Power BI to create a dashboard featuring board-level metrics, including critical risks, NIST maturity score, and security awareness. This was important because leaders needed a simple way to measure progress and address issues early.

Conclusion

Cyber risk will only become increasingly difficult to manage, and boards that remain passive will fall behind. We recommend practicing these:

Ask for the worst-case scenario every quarter

If leadership cannot explain impact, dependencies, and recovery steps in simple terms, the plan is not ready.

Demand proof of control performance, not control existence

Policies and slideware mean nothing unless the board sees how often controls fail in real conditions.

Treat third-party incidents as your own

Require the same reporting, testing, and metrics from critical partners that you expect from internal teams.

References

[1] *Cybersecurity Trends: Resilience Through Transformation, Gartner, 2025*

https://www.gartner.com/en/cybersecurity/topics/cybersecurity-trends

[2] *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Securities and Exchange Commission, 2023*

SEC Final Rule Release No. 33-11216 (PDF)

[3] *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Federal Register, 2023*

https://www.federalregister.gov/documents/2023/08/04/2023-16194/cybersecurity-risk-management-strategy-governance-and-incident-disclosure

[4] *Statement Regarding Administrative Proceedings Against SolarWinds Customers, U.S. Securities and Exchange Commission, October 22, 2024*

https://www.sec.gov/newsroom/speeches-statements/peirce-uyeda-statement-solarwinds-102224

About the Authors

Tejusvi Sharma
Senior Consultant – GRC, CyberSecurity, LTIMindtree

Tejusvi Sharma is a cybersecurity professional at LTIMindtree, specializing in Governance, Risk, and Compliance (GRC). He has contributed to projects enhancing compliance, risk management, and cybersecurity governance frameworks. He is pivotal in designing and delivering tailored GRC solutions that meet regulatory standards, mitigate risks, and boost operational resilience.

Rupa Parekh
Principal Director – GRC, Cybersecurity, LTIMindtree

Rupa Parekh is a Principal Director at LTIMindtree with over twenty years of experience in governance, risk, compliance, and enterprise data security. She leads GRC and Data Security Practice, managing global teams to develop and implement compliance and risk programs across various industries and regions. She promotes innovation and resilience in solution design to help organizations achieve operational excellence and security amid a dynamic cyber landscape.