Deloitte.

Cyber considerations for C-suite while addressing the board

The importance of the C-suite to report to the board on cyber

In this post-pandemic world, cyber risk frontiers have increased multifold. Business leaders now consider cyber more as an enterprise-wide risk management issue, rather than just an IT issue. 72% of survey respondents indicated their organisations experienced between one and 10 cyber incidents and breaches in the last year alone, according to our 2021 Future of Cyber Survey. The 2021 Gartner Board of Directors Survey echoes the same thoughts as directors across the board rated cybersecurity as the second-highest source of risk, after regulatory compliance.

These statistics make it imperative for senior leadership and the C-suite to have a regular cadence with the board on the organisation's cyber readiness and allay any fears they may have on an organisation's cyber posture.

The C-suite refers to, but is not limited to, the Chief Information Officer (CIO), Chief Information Security Officer (CISO), Chief Technology Officer (CTO), Chief Risk Officer (CRO), Chief Executive Officer (CEO), Chief Financial Officer (CFO), and Chief Operating Officer (COO).

Our recent point of view, 'The changing role of the board on cybersecurity', shares insights on the evolving role of the board in cybersecurity conversations, and enumerates a few ways to create a strong ecosystem to enable cybersecurity decisions at the board level.

While presenting to the board, the C-suite must highlight issues that can potentially become a hinderance for the organisation to meet its business objectives. It is also an opportunity for them to put forth their investment needs and get a buy-in from the board on key strategic initiatives.

The C-suite presentations to the board often end up being technical, and full of jargon and domain-specific terms. The board may not be able to relate to or comprehend them. Hence, the key message gets lost in translation, and leads to unnecessary panic and fear when it comes to cybersecurity.

General pitfalls the C-Suite face while presenting to the board

There is no one-size-fits-all approach to present to your organisation's board, because board compositions differ from one organisation to another. Each board has differing awareness levels of the wide impact of cybersecurity. A few challenges that the C-suite faces while presenting to the board are given below:

Ability to link technical presentation to business issues is a critical parameter to get buy-in from the board.

A presentation of cybersecurity from a lens of fear rather than as an enabler for business objectives and innovation

A presentation focused only on the past rather than the future, and fails to highlight the organisation's resilience

Information overload without a proper storyline and key action items highlighted

Less clarity on the board members' background, members, interest and personalities can lead to miscommunication to the board from the senior leadership

Customising conversations with the board

To successfully articulate and present to the board, the senior leadership team should understand the board's duties, needs, and expectations and be ready to answer any questions related to exercising board level duties. It also includes, but is not limited to, duty of care and loyalty, which forms part of the board's fiduciary duties.

Under the Companies Act 2013, directors, as part of their duty of loyalty, are required to act in good faith to promote the company's objectives. They need to act in the best interests of their members, the company, its employees, shareholders, and community as well as to protect the environment. The C-suite needs to understand these duties and tailor their presentation to the board catering to the above-mentioned duties and responsibilities.

> Duty of care requires directors to inform themselves of "all material information reasonably available to them," before making a business decision. Board members will look up to the C-suite to provide the required information on time.

The C-suite needs to have the right mix of business acumen and information security expertise to share key business insights to the board. Every single leader must find a way to present performance indicators to the board with a business flavour. Mentioned below are a few key pointers that security leaders can use to effectively project and showcase their business perspectives to the board:

- Number of intrusion attempts i.e., the number of times attackers tried to gain unauthorised access to the system or network
- Mean Time to Detect (MTTD) i.e., the average time taken by an organisation to detect a cyber threat
- Mean Time to Resolve (MTTR) i.e., the average time taken by an organisation to respond to threat after it has been identified
- Mean Time to Contain (MTC) i.e., the time taken for an organisation to re-secure the breached location
- Patching cadence i.e., the frequency of installation of security patches
- Cyber benchmarking i.e., the comparison of an organisation's security posture with that of their industry peers
- Third-party risk management
- Insider risk
- Cybersecurity awareness
- Succession planning
- Investment IT and security IT project burn rate

For more details, please refer to our ready reckoner.

The all-pervasiveness of cybersecurity in an organisation

It is now a common practice to have a cyber expert/risk or audit committee that periodically reports to the board on key cyber issues.

A recent World Economic Forum report detailed that the percentage of S&P 500 companies that reported having a cybersecurity expert as a member of the board increased from just **7%** in 2013 to **28%** in 2020. It is, in fact, expected to move upwards from here. According to leading research reports, 40% board of directors will have a dedicated cybersecurity committee overseen by a qualified board member by 2025, up from less than 10% today. The C-suite must understand where board oversight responsibility of information security resides before making any presentation to them.

There is no absolute assurance or fool-proof security measure to prevent a cyberattack, and the success of any organisation lies in its resilience, i.e., how fast it can get back up when targeted by cyber threat actors. Sharing a uniform message will allow leaders to balance the famous trade-off between the need to operate and secure the business.

As cybersecurity pervades every aspect of an organisation, it needs to be embedded in business and decision-making conversations. The phrases 'cyber everywhere' and 'secure by design' become meaningful as they bring trust and security to decisions.

For example, if there is a merger and acquisition, the cyber aspect of the M&A should be considered. It could also be relevant for key business decision making in areas such as Initial Public Offering (IPO) readiness assessments, and digital transformation initiatives.

The bottom line

The presentation meant for the board should be informative and have clear action points. The C-suite needs to highlight the broader business perspectives in the metrices being presented, either through slides, dashboards, or table-top exercises to drive their point home in the shortest possible time.

As the board's role in an organisation evolves, the need to demonstrate the organisation's resilience to key stakeholders, such as investors and regulators, becomes prominent. It is up to business leaders to provide adequate context and information for the board to make informed decisions.

Security leaders must have ownership created at the board level, as cyber hygiene is more effective as a top-down approach in an organisation.

Connect with us

Rohit Mahajan
President, Risk Advisory
Deloitte India
rmahajan@deloitte.com

Gaurav Shukla
Partner and Leader, Cyber, Risk Advisory
shuklagaurav@deloitte.com

Deepa Seshadri
Partner, Risk Advisory
deseshadri@deloitte.com

Contributors

David George

Priyanka Subburaman

Deloitte.