# BALANCING BETWEEN SENIOR MANAGEMENT & BOARD'S EXPECTATIONS AND CISOS' BURNOUT

On 2 July 2024, ISACA SG Chapter (ISACA SG) and Chartered Management Institute (CMI) Singapore organised an inaugural round table discussion addressing the key concerns about balancing Chief Information Security Officers (CISOs) state of wellness and discharging Senior Management & Board's expectations. The round table was well represented by ISACA SG and CMI invitees comprising CISOs, Technology Auditors, CEOs, Board members, Government Agencies, Risk Professionals and Associations' Key Representatives to provide a holistic view of this discussion topic. The conclusion is that "**Building a Resilient Cybersecurity Culture is A Whole of Company Approach".**

In today's fast-evolving digital landscape, cybersecurity is not merely the responsibility of the CISO or the technology team; it is a collective responsibility that must be driven from the top by the board. The Tone-at-the-Top principle is crucial to drive the right behaviour of any organisation building a resilient cybersecurity culture.

The role of the CISO is critical, but it is part of a broader strategy that requires the entire organisation to be involved. This article explores the dynamics between boards and technology risk professionals, emphasising the need for a cohesive approach to managing technology risks, fostering resilience, and achieving business objectives.

*"A recent survey report[1] released by ThreatReady from HackTheBox indicated that 90% of the CISOs surveyed are concerned about stress, fatigue, or burnout affecting their team's well-being. Yet only 8% of them are considering quitting their jobs due to overtime, stress, burnout, or mental health challenges within their role in cybersecurity."*

## Unrealistic Expectations and Misplaced Blame and Hidden Risks

One common issue is the expectation that technology professionals can solve all cyber security problems leading to misplaced blame when cyber-attacks arise. Boards must understand that technology belongs to everyone in the organisation, not just the technology (and risk) team. Accepting that there will be lapses in people, processes, and technology is essential, especially in a constantly changing environment. A recent findings of the World Economic Forum indicate that human error accounts for 95% of cybersecurity incidents. Therefore, Board has

[1] Reference: https://resources.hackthebox.com/building-a-firewall-against-cybersecurity-burnout?utm_source=linkedin_newsletter&utm_medium=social&utm_campaign=building_a_firewall_against_cybersecurity_burnout_report&trk=article-ssr-frontend-pulse_little-text-block

to take the whole of company approach to build cyber resilience and mitigate the business disruptions caused by cyber-attacks and threats.

If the attitude of the Board is not changed, it can result in the hidden risk of burnout of CISO and technology professionals.

**Cybersecurity and Business Alignment**

The Board and the C Suites face an uncertain and challenging operating environment caused by geopolitical tension, wars, intense competition, supply chain disruptions, capacity and talent constraints; and new and changing laws and regulations. These issues occupy the priority list of most Board Agendas. It is telling that cyber security risks are relegated to the Chief Technology Officer (CTO) and CISO and most Board do not have members who are familiar with managing cyber security risks.

The rise in cyberattacks, has disrupted business services, breached confidential and privacy data, caused harm to critical systems, and resulted in reputational damages and monetary losses. The Board and C Suites need to reprioritise resources to manage cyberattacks and build a culture of cyber resilience. Cybersecurity is not just about technology; it involves people and processes. Attackers often target employees, making them soft targets. Therefore, it requires the Board and C Suites to change mindset and make it a personal responsibility of everybody to be vigilant on cyber threats.

The Board has to include cyber threats as a key risk in the organisation enterprise risk management system. In setting the risk appetite and risk tolerance, the Board has to recognise it is not realistic to put a zero risk tolerance for cyber threats. It is proven that no matter how robust is your cyber defence orientation, clever hackers can still breach the defence. Therefore, the Board must work with Management to put in place a business continuity framework that ensures the protection of critical information infrastructure and the recovery of these infrastructures from cyber-attacks.

**Effective Communications and Building Trust**

CISOs and technology professionals need to build trust with Management and Board Members through effective communications. A common observation is that they do not consider business objectives and budgetary constraints when requesting capital investment in cyber security infrastructure. Some inject fear and go into technical details that befuddle the decision-makers. These are not helpful in building trust and obtaining buy-in from Management and the Board.

**Accountability and Ownership**

When a breach occurs, determining liability can be complex, especially if it stems from user errors. Building resilience means not relying solely on external support or government funding. Instead, organisations should focus on identifying and protecting critical information assets and preparing for recovery. Balancing cyber protection with investment cost is vital, and Board must be aware of the trade-offs involved.

*"A Harvard Business Review article[2] wrote that Boards focus on protection when they need to focus on resilience, and Boards believe cybersecurity is a technical topic. Hence, Boards are having wrong conversations in their board rooms!"*

**Building a Culture of Resilience**

A resilient organisation is one where the senior management, board and CISO work together to address and learn from incidents. Instead of seeking quick fixes, the focus should be on continuous learning and improvement. Security should be integrated into the business culture, with investments justified by their contribution to business benefits. Sudden budget increases are not the solution; a consistent and strategic approach is needed to make security an integral part of the business.

Building a culture of resilience starts with the board, which must shift from a compliance mindset to a growth and performance mindset. The board needs to provide:

- **Purpose and Direction:** Clearly defining the organisation's cybersecurity goals and objectives, including clear risk appetite of cyber risks. It is not realistic to take a zero tolerance approach to cyber threats.
- **Developing People and Capability:** Investing in training and development to so that every staff is vigilant on cyber threats.
- **Building Relationships and Networks:** Fostering collaboration across departments and with external partners through effective communication.
- **Leading Change and Innovation:** Encouraging innovation in cyber resilience and stay ahead of evolving cyber threats.
- **Managing Resources and Risks:** Allocating resources effectively to manage and mitigate cyber risks. Promote proactive risk management where risk professionals are consulted early to mitigate any cyber risks that lead to reputational damages and financial loss.
- **Achieving Results with Defined Outcomes:** Setting and measuring clear outcomes to ensure the effectiveness of cybersecurity initiatives. Cybersecurity key performance indicators (KPIs) should avoid external factors that are not within the control of the CISO team e.g. number of breaches attempted from attackers, etc.

**Communication and Education**

*"CISOs will not have a seat at the Board table. They are just too technical. Their reporting officer such as Chief Information Officer or Chief Digital Officer may be considered. Board's role is to provide strategic directions and risk oversight of an organisation." – commented by several experienced Board members in & outside of the discussion*

Effective communication is key to aligning board expectations with technology realities. Boards, often composed of individuals with backgrounds in accounting, law, or business, may lack technical cybersecurity expertise. In addition, Board members with decades of experiences

[2] Reference: https://hbr.org/2023/05/boards-are-having-the-wrong-conversations-about-cybersecurity

may likely come from the non-digital era where certain habits, knowledge and skills require time to (re-) develop.

Educating them on the importance of technology risks and using a risk-based approach is crucial. Simplifying technical jargon and focusing on the business impact can help bridge the understanding gap.

The role of the CISO is multifaceted, requiring both technical expertise and business acumen. It involves not just managing technology risks but also influencing organisational culture to foster resilience. CISOs must communicate effectively with the board, using storytelling to convey complex issues and justify investments. They should work closely with risk, audit and compliance departments to align risk strategies. The story is not for CISO to tell alone. It is a combined effort to showcase the value that risk investments are worth it.

**The Role of Management**

Technological landscapes are continuously evolving, and organisations must adopt a risk-based approach to manage these changes effectively. No matter how many controls are in place, there is always a risk of attacks. At the board level, discussions often focus on frameworks without integrating the people, processes, and technology components. Managing tech risk involves creating a resilient system that can detect, respond to, and recover from incidents. Boards must recognise that cybersecurity is not just about managing technology risks but ensuring business resilience.

At the management level, the right support provided to drive the right direction is very important. Management is often the cushion in between the Board and the CISO team. If the Management team leaves the technology risk effort to the CISO team alone, then everyone will get disappointed. Management can help to create adequate opportunities for the CISO team to engage with both Senior Management and Board to share technology risk insights. It should preferably not be the last agenda item on the Board agenda where 5-minute session was allocated to discuss cyber security risk. And it should not be a box ticking agenda either.

Currently, the position of CISO is not yet a core team member of the C Suites. Most CISO reports to a Chief Information Officer (CIO) or the Head of Technology, or the CFO. Therefore, cyber security issues continue to be relegated as an operational issue, not a strategic issue. It is necessary for the Board to consider elevating CISO to be a regular invitee to the board room before considering making CISO a core member of the C Suites. Regular attendance of Board room activities help to develop CISOs' strategic thinking skills and may be one of the talent development opportunities to prepare CISOs for higher role and responsibilities.

**Conclusion**

A CISO's role includes developing a robust risk management framework and coordinating with risk owners to mitigate cyber risks. They need strong interpersonal communication skills to effectively engage with risk owners responsible for managing cyber risks. Cyber risks must be a mandatory checkpoint for every business process design, incorporating technologies from the start. Many organisations make the mistake of adding cybersecurity as an afterthought, making the CISO's job arduous and the expectations of the board difficult to meet.

Cybersecurity is not just the responsibility of the CISO; it is a collective effort that requires the involvement and commitment of the entire organisation, driven from the top down by the board. Realistic KPIs and the cyber vigilance of the entire organisation is necessary to mitigate the risk of cyber-attack.

Building a strong, collaborative relationship between boards and technology teams is essential for navigating the complexities of today's digital world. By fostering a culture of resilience, aligning cybersecurity efforts with business goals, and improving communication and education, organisations can better manage technology risks and achieve sustainable success. A simple test of commitment from the Management and Board for a cyber/ business crisis management simulation can indicate the maturity of the organisation resilience commitment.

Lastly, committing to organisational risk resiliency is a journey. Businesses need to appreciate that good risk performance leads to good business performance.

*Co-authors: Jenny Tan (ISACA SG), Hoi Wai Khin (CMI) and Tay Woon Teck (CMI)*

---

*Organisers:*

- *CMI – Tay Woon Teck, Chairman and Hoi Wai Khin, Education Director, CMI*

  **About CMI** (https://www.managers.org.uk/about-cmi/)
  Turning accidental managers into conscious leaders

- *ISACA SG – Jenny Tan, President and Yap Lip Keong, Vice-President*

  **About ISACA** (https://www.isaca.org/about-us)
  A community of IS/IT professionals in pursuit of digital trust | We are working to build a better digital world

*CMI and ISACA SG would like to thank the following persons for contributing their views at the round table leading to this article formulation:*

- *Andreas Dannert, Principal Enterprise Security Architect, Standard Chartered Bank*
- *Anthony Ong, Vice Chairman, CMI, Senior Advisor, Adera Global*
- *Chan Meng Fai, Senior Manager IT IA, Singapore Airlines*
- *Chua Chay, Head MCISO, Mindef*
- *Hardik Thaker, Executive Director, Tech & Cyber Risk & Cybersecurity, GXS Bank*
- *Murari Kalyanaramani, SID Digital Chapter Committee Member, UOB CISO*
- *Patrick Tay, COO & GM, Data Connect Technologies (Co Konica Minolta)*
- *Phoram Mehta, Senior Director and CISO International Markets, PayPal Pte Ltd*
- *Saw Ken Wye, Honorary Chairman, CMI, Director En-Vivo Pte Ltd*
- *Siew Yim Cheng, Senior Vice President, Digital Value Chain Solutions, Yara Asia Pte Ltd, Council Member, CMIStephen Ching, President, IIA*
- *Tan Boon Yen, Senior Director Risk Advisory, RSM Singapore*
- *Veronica Tan, Director, Cybersecurity Agency of Singapore*