the clarity factory

Cyber security is no longer just a necessary hygiene factor – it is a key differentiator for the increasingly digital organisation. Doing it well starts at the top, but the majority of Boards still don't get it.

Boards are increasingly concerned about cyber security, ranking it as one of their top priorities, and for good reason. The cyber security risk is growing, ever more companies are being targeted, and while multi-million dollar ransoms attract the headlines, the impacts of a cyber incident are felt right across the business: higher insurance premiums, business disruption, lower production, delays, reputational damage, intellectual property theft, litigation, and regulatory actions, to name a few. Board interest is also being piqued as a result of growing media reporting of cyber incidents, a heightened board focus on operational resilience post-pandemic, investor pressure and a tightening regulatory environment.

While there has undoubtedly been progress in recent years on board governance of cyber security, many boards struggle to dispense their responsibilities. Many don't understand their unique role on cyber security, lack the right level of cyber awareness and can't turn to CISOs or other executives to bridge this gap, and as a result fail to challenge what they hear in the boardroom.

This vacuum in cyber security board governance leads to three common problematic postures: passive, in the weeds, and deferential. Directors on these boards, respectively, have a tendency to disengage from the conversation, get distracted by the technical details at the expense of a risk-based approach, or wave through the recommendations of a trusted and well-presented CISO.

Cyber-engaged boards operate differently. Exactly what cyber-engaged looks like will differ according to a company's cyber risk profile, but these boards have a clear understanding of the unique role of the board, recruit directors with specialist knowledge of technology, digital, data or cyber, invest in education to raise their individual and collective knowledge of cyber security, make cyber security a regular topic of discussion in board meetings, ensure cyber security has a home within a designated board committee, and seek out advice from the CISO and independent cyber advisors.

Getting cyber security governance right is not just a win for the security of individual companies; evidence shows that large enterprises with digitally savvy executive teams have significantly higher revenue growth, valuations and net margins. Effective cyber security also brings many top line benefits, including greater success rates when tendering for new clients, improved data insights, investor confidence and maintenance of shareholder value during mergers and acquisitions.

What's more, effective cyber security contributes to the trust and integrity our societies and economies rely on to survive. There is a growing urgency to act, and it requires companies, regulators, investors and public bodies to play their respective roles.

We set out a **5-point plan for effective cyber security board governance** which includes recommendations for all these bodies:

Boards should:

1. Understand their unique role as a board, in setting the company's risk appetite, focusing on resilience and recovery, ensuring they remain informed and up-to-date, and being prepared to respond as a board in the event of a cyber incident

2. Be appropriately informed about technology, data and cyber security:

- Boards should have at least one NED with experience in, and capable of speaking at board level to, technology, digital, data, cyber security or other forms of security, such as physical or supply chain.
- Chairs should encourage directors to educate themselves, invite experts in to brief the board, allow and encourage NEDs to be in contact with CISOs between board meetings, and ensure directors have access to independent board advisors.

Cyber security should feature at least quarterly and more frequently when there is something critical ongoing.

3. Put cyber security on the board's agenda

- Cyber security should feature at least quarterly and more frequently when there is something critical ongoing.
- The board report should be delivered by the CISO.
- Companies with elevated technology, data and cyber risks should consider establishing a technology committee of the board.

4. Ensure they have access to independent cyber security advisors

- CEO and CFO: to help them challenge and arbitrate between the CISO, CIO and CTO in prioritising between security, reliability and uptime. Often security needs to be prioritised against features and functions of business systems or customer facing apps, for example. They can also help them to interpret reports from the CISO before or after board meetings, helping them to understand what questions to ask and which lines of enquiry to probe.
- Non-executive directors: to offer 1-2-1 coaching and mentoring for NEDs, help them to prepare for board meetings, understand cyber strategy, formulate the right questions to ask, and help them to identify red flags.
- CISO: to coach CISOs on how to communicate and engage appropriately at board level.

5. Actions for regulators, investors and public bodies

- Regulators: While regulation should be the last resort in many situations, it is time to act on cyber security with smart and focused regulation. This means requirements for boards to: report on relevant expertise at board and senior management level on cyber security; report on risk management arrangements for cyber security; and disclose breaches to the relevant public authority to build a more comprehensive shared picture of the emerging threat. We welcome the July 2023 SEC ruling on cyber security disclosure.
- Investors: investors should continue to ask questions of their portfolio companies to help drive action on cyber security and more effective governance.
- Public-private partnerships on cyber security:
- They can deliver three vital outcomes for cyber security: a) shared and improved knowledge about incidents and trends, b) shared best practice on cyber security management and governance, and c) joint activities to strengthen the cyber security capability of organisations and the general public.
- The National Cybersecurity Centre does sterling work in the UK and should be further resourced and supported to extend this work to ensure all organisations have somewhere to turn for information, mentorship, best practice, and joint working.

WE HAVE AN OPPORTUNITY – BOARD GOVERNANCE OF CYBER SECURITY IS A SOURCE OF COMPETITIVE ADVANTAGE

This is an extract from Effective Board Governance of Cyber Security: A source of competitive advantage, by Richard Brinson and Rachel Briggs OBE, published by Savanti. To read the full insight paper, visit the Savanti website.

Rachel Briggs OBE
rachel.briggs@clarityfactory.com

The Clarity Factory is an engine room for knowledge, insights and problem solving, helping companies, governments and non-profits.

clarityfactory.com