ISTARI

UNIVERSITY OF CAMBRIDGE
Judge Business School

Beyond the Firewall

Leadership and Governance Insights for Cyber Resilient Organisations

Author:
Simon Learmount

Illustration by: Kouzou Sakai

Research and report authored by Dr. Simon Learmount of the University of Cambridge acting through Cambridge University Technical Services Limited.

Contents

Foreword

The transformation of cybersecurity is no longer a matter of debate; there has been an era-defining shift. What was once a technical safeguard buried in the back office has been thrust into the centre of the boardroom.

Today, cybersecurity is a primary engine of enterprise value in the digital age: the bedrock upon which trust, brand reputation, revenue, and operational continuity are built.

Yet, as the digital estate expands, the stakes have shifted from management to survival. In the UK alone, the National Cyber Security Centre (NCSC) manages four nationally significant incidents every week. For household names across retail, manufacturing, and transport, a cyber incident is no longer a remote possibility; it is a high-stakes stress test of their entire governance framework.

Digital reality, however, defies traditional borders. Unlike the physical world, where jurisdictions are clear and order is enforceable, the digital realm is a patchwork of overlapping mandates and conflicting responsibilities. In this borderless landscape, there is no universal rulebook.

This research, conducted by *Dr. Simon Learmount* at *Cambridge Judge Business School*, addresses this vacuum. It reflects a critical reality: as cyber risk evolves from a technical hurdle to a systemic threat, the traditional silos of governance are failing. Boards can no longer afford to be reactive. To govern effectively, they must develop the institutional foresight to anticipate crises before they arrive, as gaps in understanding are not just administrative flaws; they are the primary inhibitors of recovery.

"An area that both interviewees and literature sources converged on is the pressing need for continuous training and education in cybersecurity governance – for CISOs, boards, and indeed all organisational actors with cyber responsibilities."

—

Dr. Simon Learmont

Drawing on anonymised, high-level insights from 23 global leaders across policy, business, and security, this report exposes the friction points in current governance models. It seeks a new path forward where risk does not perpetually outpace opportunity.

We believe the solution lies in a decentralised, ecosystem-led approach. True resilience must be built through constant iteration and a radical collaboration between academia, government, and industry. Effective governance now demands:

- **Business continuity:** Moving beyond fragmented mandates to unified standards.
- **Radical Accountability:** Defining who owns the risk when the borders are blurred.

- **Agile Adaptation:** Ensuring governance evolves at the speed of AI and emerging threats.
- **Deep Public–Private Synergy:** Transforming compliance into a shared mission.

At ISTARI, we view this challenge not as a regulatory burden, but as a competitive mandate. Resilience and trust are the new currencies of the global market. The organisations that will lead the next decade are those that elevate cyber risk from the boiler room to the boardroom, integrating it into the very DNA of their commercial strategy.

We stand at a crossroads. As the lines between technology, risk, and governance dissolve, the future will not belong to the most protected, but to the most connected. Through working with Cambridge and our global network of experts, we invite you to move beyond mere security toward a future of enduring resilience.

ROSSA SHANKS

Chief Executive Officer
ISTARI

Executive summary

This report presents key findings from a novel, in-depth study on the fast evolving world of Cyber Governance. Based on interviews with Chief Information Security Officers (CISOs), board directors, policy makers, regulators and other security professionals, the research goes beyond generic surveys or best-practice checklist, offering rich, granular insights into how the complex and often messy world of cyber governance continues to evolve.

Cybersecurity as a core governance issue

For boards and executives, cybersecurity is no longer just an IT issue – it is a core governance priority. Interviewees stressed that effective governance requires weaving cyber risk considerations into strategic decisions, enterprise risk frameworks and organisational culture. In short, managing cyber risk is inseparable from managing the organisation itself.

Bridging the board–CISO divide

The research highlights that cyber governance works best when boards and CISOs truly "see eye-to-eye" on risk, though many participants noted this relationship is often strained or misaligned. Boards often lack cybersecurity expertise and focus on compliance or financial risk, while CISOs grapple with technical complexities and operational disruptions. The resulting gap in language and expectations leads to frustration on both sides. Interviewees stressed the need to improve communication, trust, and mutual understanding.

Beyond compliance to resilience culture

True cyber resilience requires more than compliance checklists. Cultural integration, business alignment and distributed responsibility are critical. Organisations with robust cyber postures must cultivate a security-first culture that permeates every level of the business. They align cyber risk management with business goals and embed it in daily operations rather than treating security as a siloed IT checkbox. In these organisations, responsibility for cybersecurity is shared across departments, not isolated in one team. This cultural approach shifts the focus from mere compliance to proactive resilience.

Governing third-party and supply chain risk

Third-party and supply chain cyber risks emerged as top governance priorities in the interviews. As organisations rely on vendors and partners, they are exposed to security vulnerabilities outside their direct control. Boards are increasingly seeking assurance that these external risks are managed through formal structures. New oversight mechanisms are emerging to address this challenge – for example, dedicated supply chain risk committees, stricter vendor due diligence, and accountability frameworks. Effective cyber governance now extends beyond the organisation's four walls, requiring collaboration across the entire value chain.

The evolving role of the CISO

The role of the Chief Information Security Officer (CISO) is undergoing a fundamental transformation. Traditionally a technical expert managing defences and incident response, the CISO is now becoming a strategic risk leader and adviser to the business. Interviewees described CISOs stepping into enterprise leadership by translating cyber threats into business terms, shaping risk strategy and informing board decisions. Successful CISOs bridge the gap between technology and business, communicate in the language of risk, and influence company direction.

Cyber governance as a socio-technical system

The research makes clear that cyber governance is not purely a technical issue – it involves understanding a complex socio-technical system. Managing cyber risk involves an interplay of technical measures, human behaviours, organisational processes, and ethical considerations. Good governance balances technical controls with human factors: open communication, clear accountability, and a willingness to share decision-making across the organisation. Cross-disciplinary expertise is vital, and input from IT, risk, legal, HR, and ethics helps address the full spectrum of risk. In essence, governing cyber risk is a human and technical challenge, requiring holistic thinking and collaborative leadership.

Building capabilities and shared language

There is a pressing need for targeted training and development to build cyber governance capability at all levels. Boards often lack a shared language and basic cybersecurity knowledge. Likewise, CISOs and security teams may need help communicating risk in business terms and working across disciplines. Interviewees suggested tailored programmes – from boardroom cyber workshops to cross-functional exercises – to foster shared understanding and bridge the knowledge gap. Investing in people and education builds a common vocabulary and trust, enabling more cohesive digital risk governance.

Conclusion

These findings position cybersecurity and digital governance as an urgent leadership priority. The takeaway is clear: cybersecurity and digital governance require urgent attention, sustained investment, and a long-term commitment from leadership – a journey that must begin now to secure the organisation's digital future.

Cybersecurity: backroom to boardroom

In an era of digitalisation and data-driven business, organisations of all sizes find that cyber risks are now strategic, operational, and reputational concerns at the highest levels of leadership.

High-profile attacks and breaches in recent years have demonstrated that a single cyber incident can halt operations, compromise sensitive data, and erode public trust. The World Economic Forum now ranks cybersecurity among the top five global risks to economies and societies[1], reflecting a consensus that cyber threats pose systemic challenges on par with climate change or geopolitical instability. In this context, boards of directors and C-suite executives are increasingly expected to treat cybersecurity and digital governance not as technical niches, but as core components of corporate governance and enterprise risk management.

Why it matters now

Several converging trends make this topic especially salient today. First, the cyber threat landscape is escalating in both scale and complexity. Ransomware attacks, supply chain compromises, and state-sponsored cyber operations have surged dramatically. Two recent incidents illustrate the magnitude of the threat. A major ransomware incident at the UK retailer Marks & Spencer, which unfolded as this research was undertaken, is estimated to have cost the organisation over £300 million in lost profit, wiped £750 million from its market capitalisation, and continued to impair its online and supply chain operations months after the initial breach. Another cyber attack on Jaguar Land Rover (JLR), still taking place as this report is being written, has already become the most economically damaging cyber incident in UK history, with estimated total costs now approaching £1.9 billion: the attack forced a five-week production shutdown, disrupted operations across 5,000 businesses in JLR's supply chain, and is expected to continue well into 2026 before full recovery. Such events underscore that the consequences of cyber incidents extend well beyond immediate financial losses: they impose long-tail costs through sustained reputational harm, operational disruption, and legal repercussions.At the same time, organisations' dependence on digital infrastructure has never been greater. Cloud computing, data analytics, and AI-driven processes unlock new value, but also create new points of vulnerability that adversaries seek to exploit. The result is that cybersecurity lapses can quickly spiral into enterprise-wide crises, threatening business continuity, market share, and even national security in the case of critical infrastructure attacks[2]. It is no surprise, then, that board members in recent surveys consistently cite cybersecurity and data privacy among their very top priorities[3]. Ensuring digital resilience is now viewed as integral to fulfilling a board's fiduciary duty to safeguard the organisation's assets and stakeholders.

From IT issue to board priority

A decade ago, cybersecurity might have been seen primarily as an IT department's concern; today it is firmly on the

1 World Economic Forum (2025) Global Risks Report 2025: 20th Edition. Geneva: World Economic Forum. Available at: https://www.weforum.org/reports/global-risks-report-2025 (Accessed: 30 May 2025).

2 Hendren, W. (2025) "World Economic Forum: CISOs "Need to Quantify Cyber Risk"", Safe Security Blog, 22 January. Available at: https://safe.security/resources/blog/world-economic-forum-cisosquantify-cyber-risk/ (Accessed: 30 May 2025).

3 Edgerton, B. and Smith, J. (2024) "Americas board priorities 2024", EY. Available at: https://www.ey.com/en_us/board-matters/americas-board-priorities-2024 (Accessed: 30 May 2025).

boardroom agenda. Governments, regulators and investors are ramping up pressure on organisations to elevate their cyber risk management and disclosure practices[4]. For example, in the US new regulations are compelling greater board accountability: importantly the Securities and Exchange Commission's 2023 rules now require public companies to formally disclose their cyber risk oversight and incident response processes at the board and management level[5]. In the UK and Europe, regulatory scrutiny and guidance (from GDPR to new digital operational resilience rules) signal that cyber governance is a director-level responsibility[6]. Investors, too, are vocal — major asset managers and institutional investors increasingly ask to see evidence that companies have robust cybersecurity governance structures and board expertise in place[7]. In short, the time is now for corporate leaders to actively embrace cybersecurity as a matter of good governance[8]. Failing to do so can invite not only attacks, but also regulatory penalties, litigation, and loss of investor confidence.

The evolving role of the CISO

Amid this shift, it is claimed that the role of the CISO has been rapidly evolving from a technical manager to a strategic business leader. Once responsible mainly for IT security operations, many CISOs are now integral members of executive management, tasked with translating cyber risks into the language of business outcomes and strategy[9]. Recent industry data shows that approximately 60% of all CISOs engage with their boards quarterly[10], and that these interactions are not just status updates on patching and firewalls but high-level discussions framing cyber threats as **enterprise risk factors** — touching on business continuity, regulatory compliance, customer trust and competitive position. Notably, according to one global survey, 82% of CISOs now interact directly with the CEO, rather than solely reporting up through IT channels[11]. This trend underscores how deeply cybersecurity has become woven into modern business strategy and risk management.

However, increased "face-time" with the board does not automatically equate to effective communication or influence. Tensions remain in many organisations around the CISOs mandate and voice at the top table. Misalignment in perception is a recurring challenge: the same global study cited previously found that 44% of CISOs believed they were adequately communicating security progress to the board, yet only 29% of board members agreed[12]. This kind of gap suggests that despite sitting in the same meetings, CISOs and directors may not be speaking the same language or measuring success by the same yardsticks. It suggests the need for CISOs to further refine how they convey risk information (e.g. using financial and business impact metrics, rather than technical jargon) – and equally for boards to deepen their cyber literacy so that critical warnings are not lost in translation. The interviews underpinning this present report seek to probe such issues in depth, examining how leading CISOs and organisations are navigating the delicate balancing act of making cybersecurity a business enabler rather than a blocker, and ensuring that security leaders have the authority and resources to meet expanding expectations.

Digital and data governance as a board priority

Cybersecurity does not exist in a vacuum; it is intertwined with broader digital and data governance imperatives that boards are now grappling with. In the past, boards might have delegated data protection or IT strategy far down the organisational chart. Today, topics like customer data privacy, digital transformation risks, and technology ethics (e.g. AI

4 Ibid

5 U.S. Securities and Exchange Commission (2023) SEC adopts rules on cybersecurity risk management, strategy, governance, and incident disclosure by public companies. [Press release] 26 July. Available at: https://www.sec.gov/newsroom/press-releases/2023-139 (Accessed: 30 May 2025).

6 Harvard Law School Forum on Corporate Governance (2022) "Building Effective Cybersecurity Governance". Available at: https://corpgov.law.harvard.edu/2022/11/10/building-effectivecybersecurity- governance/ (Accessed: 30 May 2025).

7 BlackRock Investment Stewardship (2022) Data privacy and security: Our approach to engagement. Available at: https://www.blackrock.com/corporate/about-us/investment-stewardship/ insights/data-privacy-security (Accessed: 30 May 2025).

8 Easterly, J. (2025) "Corporate Cyber Governance: Owning Cyber Risk at the Board Level", Cybersecurity and Infrastructure Security Agency, 8 January. Available at: https://www.cisa.gov/news-events/news/corporate-cyber-governance-owning-cyber-risk-boardlevel (Accessed: 30 May 2025).

9 Fanning, M. (2025) "Bridging the Gap Between the CISO & the Board of Directors", Dark Reading, 31 March. Available at: https://www.darkreading.com/cybersecurity-operations/bridging-gapbetween-ciso-board (Accessed: 30 May 2025).

10 IANS Research and Artico Search (2024) State of the CISO 2023–2024 Benchmark Report. Available at: https://www.iansresearch.com/resources/all-blogs/post/security-blog/2024/01/17/state-ofthe-ciso-2023-2024-benchmark-report-is-live (Accessed: 30 May 2025)

11 Splunk (2025) The CISO Report 2025: The Path to Digital Resilience Starts With Your Board. Available at: https://www.splunk.com/en_us/campaigns/ciso-report.html (Accessed: 30 May 2025).

12 Ibid.

governance) are frequently discussed in the boardroom alongside more traditional concerns. There is a growing recognition that good digital governance is good business governance. Protecting data and technology resources is essential to maintaining customer trust, operational resilience, and strategic agility.

One recent board survey notes that directors may be broadening their view of cybersecurity and data privacy beyond mere compliance, instead looking at these areas as potential strategic advantages and sources of competitive differentiation[13]. For instance, a company adept at safeguarding data and ensuring privacy may find it easier to innovate with analytics or AI, because it has the governance structures to do so responsibly. Conversely, boards also acknowledge that their own knowledge in this domain can quickly become outdated – the threat landscape and technological environment evolve continuously, making ongoing education and expert input vital. This has led some organisations to create dedicated board committees for technology or risk, bring in board members with cyber or IT backgrounds, and integrate cybersecurity metrics into enterprise risk dashboards reviewed at every board meeting.

A rapidly changing landscape

The backdrop to all of this is a cyber threat environment that grows more sophisticated and unpredictable by the week. The rise of double-extortion ransomware, supply-chain compromises (as seen in incidents like SolarWinds), and attacks on critical infrastructure (such as energy and healthcare systems) has blurred the line between cyber risk and overall business risk. We are also witnessing threats evolve in tandem with emerging technology: for example, the misuse of artificial intelligence to craft more convincing phishing or to discover vulnerabilities at scale. Organisations report that simply maintaining the status quo is not enough - continuous adaptation and innovation in security practices are needed just to keep up. Complexity itself is a major adversary; large firms must manage sprawling IT environments across cloud, on-premises, and operational technology (OT) systems, while smaller firms often lack resources and skilled personnel to cover all bases. In a recent World Economic Forum study, executives from small, medium, and large organisations alike all flagged the "complex and evolving threat landscape" as a top-three challenge hindering their cyber resilience efforts[14]. When even well-resourced global companies concede how challenged they are by the pace of change, it becomes clear that no organisation can afford to be complacent. This climate of ever-evolving threats reinforces why cybersecurity governance must be dynamic and proactive – a standing item on board agendas, not a one-off project.

Peeking inside the complex, messy world of cyber governance

Given the high stakes and fast-moving context described above, this report adopts a deliberately 'close-to-the action' approach to understanding how organisations are coping and adapting. The analysis presented here is grounded in detailed, in-depth interviews conducted with a cross-section of global experts: cybersecurity professionals on the front lines, board-level executives and risk officers, regulators shaping policy, and thought leaders in cyber governance. By engaging directly (and confidentially) with those who live these challenges day-to-day, the research aims to surface insights that go beyond the platitudes and self-reported statistics of annual surveys. While many of the high-level studies and best-practice frameworks that have been carried out in this domain provide important and useful ideas about trends and trajectories, some important questions are unanswered and richer context is often absent. Generic surveys can tell us, for example, that a certain percentage of CEOs claim to prioritise cyber risk, or that X% of companies have implemented a given framework – but they rarely illuminate how organisations navigate internal trade-offs, why certain well-intentioned initiatives fall short, or what practical barriers leaders encounter as they try to effect change. Surveys are useful for capturing broad trends but benefit greatly from being complemented by qualitative research that provides a more in-depth understanding of the phenomena[15]. In cybersecurity, where much of the hardest work involves organisational culture and human decision-making, qualitative methods are especially powerful: they can reveal the nuances of socio-technical practices and add rigour by uncovering the why behind the metrics[16].

13 Edgerton, B. and Smith, J. (2024) "Americas board priorities 2024", EY. Available at: https://www.ey.com/en_us/board-matters/americas-board-priorities-2024 (Accessed: 30 May 2025).

14 World Economic Forum (2025) Global Cybersecurity Outlook 2025. Geneva: World Economic Forum. Available at: https://www.weforum.org/publications/global-cybersecurity-outlook-2025/ (Accessed: 30 May 2025).

15 Learmount, S. (2002) Corporate Governance: What Can Be Learned from Japan? Oxford: Oxford University Press.

16 Marcu, A.-M. (2022) "Behavioural Insights to Cyber Security: A Qualitative Analysis on European Students", BSc dissertation, University of Suffolk. Available at: https://

Moving beyond frameworks and checklists

Likewise, industry frameworks and standards (from NIST Cybersecurity Framework[17] to ISO 27001 and others) provide valuable benchmarks for cyber governance, but they are not a panacea. Many boards and executives candidly admit that compliance with checklists does not automatically equate to true security or resilience. A company might tick all the boxes of a maturity model and still suffer a major breach if underlying behaviours and assumptions were flawed.

This report will argue that we need to go deeper than a box-ticking approach, and examine the 'lived experience' of organisations – how do real people in varied institutional contexts understand their roles and responsibilities for cybersecurity? Where do they encounter friction or confusion? What strategies have proven effective in aligning cybersecurity objectives with business objectives, and where do gaps remain? By using open-ended interviews, we aim to capture stories and perspectives that shed light on these questions, enriching the empirical base for recommendations. The goal is to marry academic rigour with practical relevance, drawing-out patterns from qualitative evidence while maintaining an independent analytical lens free from commercial or partisan bias. This project is committed to evidence-based insights – the aim is that board members, CISOs, policymakers and business leaders alike can trust the findings as credible and grounded, even as they find them thought-provoking.

www.researchgate.net/publication/335091777_The_power_of_interpretation_Qualitative_methods_in_cybersecurity_research (Accessed: 30 May 2025).

17 https://www.nist.gov/cyberframework

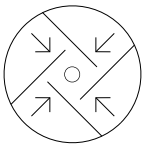
Setting the stage for what follows

In the pages ahead, we will delve into the findings from this research, but it may be worth introducing a few emergent themes in advance that will frame the discussion that follows. One is the tension between compliance and security outcomes – many organisations feel caught between satisfying external frameworks or regulations and developing an internal culture of security that actually prevents incidents. Another theme is the integration of cybersecurity into core business strategy – some organisations have achieved a true marriage of digital innovation and security (seeing them as complementary), while others still treat security as a standalone technical domain, leading to misalignment. We also observe patterns of leadership and communication that make a difference: for instance, organisations where boards and CISOs have a shared understanding of risk appetite and clear lines of communication tend to navigate threats more confidently, whereas those with siloed communication often encounter unpleasant surprises. Additionally, questions of role definition and scope surface repeatedly: as the CISOs remit expands to include areas like data governance or even safety in the context of cyber-physical systems, how should structures adapt to support this broadened responsibility? These are not purely theoretical matters – they manifest in budgeting decisions, reporting lines, crisis management protocols, and strategic planning processes, all of which will be explored in subsequent sections of this report.

In summary, this section has outlined why cybersecurity and digital governance demand urgent and elevated attention from top leadership, and why the fresh research approach adopted here is warranted to understand the evolving landscape. The stakes – financial, strategic, and reputational – are higher than ever, and traditional playbooks are being tested by relentless change. The following sections will build on this foundation, examining in detail how organisations are reimagining the role of the CISO, embedding cybersecurity into broader governance, and striving to stay ahead of a threat environment that refuses to stand still. The tone throughout will remain objective and analytical, befitting an independent study, but always with an eye to practical insights that leaders can apply. The aim is to provide not just analysis, but also a degree of guidance and foresight to help boards, executives, and policymakers make sense of the shifting terrain and make informed decisions that strengthen their organisations' cyber resilience in a digitally empowered world. Together, the evidence and perspectives gathered here will illuminate the path forward in bridging the gap between awareness at the top and effective action on the ground – a bridge that is essential for any organisation that hopes to thrive amid the opportunities and risks of the digital age.

Cyber concerns: in their own words

This section distils 8 key themes that emerged from the deep-dive research interviews. The vignettes and quotations that support these themes have been selected in an attempt to capture how CISOs, policymakers, business leaders and other cyber practitioners we interviewed experience and feel about cybersecurity at the 'sharp-end' inside their organisations. Each theme is presented in a relatively raw form here — more detailed analysis will follow in the next section of the report.



1. The governance gap: boards and cyber leaders are still talking past one another

—

Across sectors, interviewees described a stubborn misalignment between directors' strategic oversight responsibilities and cyber leaders' operational realities. Most boards now seemed to table cybersecurity as a standing agenda item, yet several CISOs reported that the discussion remained a "tick-box" issue rather than a deep-dive topic for directors:

"They nod when I present the heat-map, but the questions stop at 'are we green or red?" [1]

"Board members tell me they're 'all over cyber', then just ask how many patches we installed last month – this is the wrong metric at "The breakthrough came when I framed a ransom demand as 'equivalent to losing our Asia-Pac operation for a quarter'." [2]

1 Interview #12 – CISO, asset-management (UK)

2 Interview #16 – Regional CISO, global logistics

Three specific gaps were frequently mentioned:

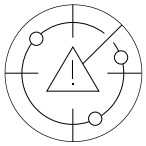
Governance dimension	How CISOs describe current practice	Why it matters
Risk appetite	*"Implicit, never written down"*	Without an explicit cyber-risk tolerance, security teams either default to worst-case assumptions or under-protect business-critical data.
Success metrics	Patch counts, phishing-test click rates	Boards struggle to map technical KPIs & business impact (e.g. days revenue at risk).
Decision-making	CISO invited but *"not a vote"*	Cyber leaders often lack formal authority over the budgets they are expected to safeguard.

Several interviewees noted progress where boards established dedicated technology-risk committees or co-opted non-executive directors with cyber expertise. Yet even in those cases, CISOs emphasised the importance of 'translating' issues into terms the board could understand:

> *"The breakthrough came when I framed a ransom demand as 'equivalent to losing our Asia-Pac operation for a quarter'."* [3]

The implications of this 'governance gap' were clear and consistent across interviews: boards must shift from interrogating operational minutiae to clarifying risk appetite, funding thresholds and acceptable downtime; CISOs, in turn, must present scenarios in business-outcome language – a recurring success factor discussed further under Theme 3 (below).

3 Interview #16 – Regional CISO, global logistics



2. From IT hazard to enterprise risk: cybersecurity's financial & societal stakes

All interviewees uniformly rejected the idea that cyber incidents remain simply a "tech problem". Instead, they portrayed cyber risk as a multidimensional, increasingly critical threat encompassing revenue loss, legal exposure, safety and, in certain cases, human life.

"Our ransomware tabletop showed a two-week outage in pathology could kill patients – that changed the tone overnight." [4]

"If the trading platform stalls for eight hours, that's £30 million gone – audit understands that; the board does too." [5]

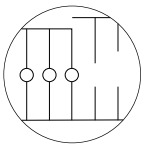
The impact vectors that were reported to resonate most strongly with senior leadership included:

- **Business continuity** – manufacturing CIOs worried less about data exfiltration and more about *"production lines freezing mid-shift"*.[6]
- **Reputational capital** – consumer-facing brands fear the (social and traditional) media fallout of breached customer data: "*Bad press costs more than the ransom*" said a retail CISO.[7]
- **Regulatory and legal exposure** – fines under GDPR-style regimes remain an *"iceberg"* that boards now track as closely as financial audit numbers.[8]
- **Societal harm** – energy and healthcare respondents in particular referenced ransomware as a physical-safety risk, not merely an IT one.[9]

This broadened framing seems to be driving two notable shifts:

- **Cyber quantification** – some CISOs, especially in the financial-sector where such language is more common, are beginning to express risks in terms of Value-at-Risk or Capital-at-Risk, aligning with regulatory capital models.[10]
- **Insurance as a double-edged sword** – executives welcomed the 'discipline' that insurers could bring (*"insurers ask harder questions than our own board"*[12]) and yet warn of how this can breed some complacency within the organisation: "*Cover is shrinking; you can't transfer reputation.*" [11]

The implication of this theme is that boards which view cyber through a purely technical lens tend to underestimate its enterprise-wide ramifications. Linking cyber risk to financial, legal and human-safety outcomes accelerates funding decisions and clarifies priorities.



3. The expanding CISO mandate: from firewall custodian to strategic integrator

Almost every interviewee reported CISO role expansion:

"Security, privacy, data, resilience, AI ethics: they all end up on my desk"[12]

4 Interview #19 – CEO, healthcare trust
5 Interview #4 – Deputy CISO, multinational bank
6 Interview #7 – CIO, automotive manufacturer
7 Interview #15 – CISO, consumer-retail group
8 Interview #10 – Data-privacy officer, EU telecoms provider
9 Interview #6 – CISO, energy utility
10 Interview #4 – Deputy CISO, multinational bank
11 Interview #4 – Deputy CISO, multinational bank
12 Interview #3 – CISO, US tech company

Key drivers of this expansion were reported to be:

Driver	Manifestation	In their own words
Regulatory convergence	GDPR, DORA, SEC rules conflate cyber, data privacy, and operational resilience.	*"The board doesn't care if it's privacy or cyber – they just ask if we're compliant."*[13]
Digital transformation	Cloud migrations and DevOps require security baked in, not bolted on.	*"If I'm not in the sprint review, risk appears in production."*[14]
Supply-chain exposure	Third-party software bill-of-materials now a board concern.	*"SolarWinds made it my problem to vet every vendor's vendor."*[15]
Talent & culture	Security advocates embedded across organistional functions.	*"My KPIs now include 'security champions' per business unit."*[16]

Some key structural patterns observed in the interviews:

- **Evolving reporting lines** – 23 % of the CISOs interviewed now report directly to the CEO or COO, bypassing CIO hierarchies. Those who retained CIO reporting claimed this enabled *"budget leverage" but risked perception as "IT cost centre"*.
- **Board-engagement cadence** – quarterly deep-dives are becoming more common. Several firms had instituted *"cyber incident rehearsal"* sessions with directors: *"Nothing sharpens focus like role-playing the ransom call."*[17]

Yet greater visibility brings new tensions:

- **Performance metrics** – boards are becoming less likely to ask for technical dashboards, but CISOs struggled to agree on suitable business-aligned KPIs. "Mean time to contain is meaningful to me, not to them" noted a utilities CISO.[18]
- **Personal liability** – multiple CISOs cited heightened anxiety after recent US prosecutions of security officers. *"D&O insurance is now part of my package negotiations."*[19]

The implication of this theme is that organisations must clarify the CISO remit, ensure reporting lines match strategic expectations, and establish shared metrics. Without this alignment, role expansion for the CISO risks burnout and strategic drift.

13 Interview #14 – CISO, global insurer

14 Interview #2 – DevSecOps lead, fintech start-up

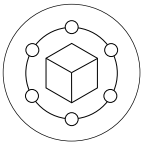
15 Interview #11 – Public-sector security head

16 Interview #1 – CISO, industrial manufacturer

17 Interview #18 – Non-executive chair, FTSE-250 retailer

18 Interview #6 – CISO, energy utilit

19 Interview #9 – CISO, North-American healthcare network



4. Supply-chain & third-party risk: theAchilles' heel of digital ecosystems

Interviewees expressed near-unanimous concern that an organisation can *"do security brilliantly internally, and still fail"*[20] because of vendor compromise.

"Our [******] partner's ransomware outage shut down 40% of hospital services for weeks." [21]

"We have 3,000 suppliers; even 1% poor hygiene is 30 doors open." [22]

The key pain-points for interviewees included:

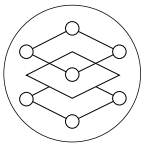
- **Due-diligence fatigue** – standard questionnaires ("tick-box ISO 27001"[23]) no longer reassure boards; one CISO called them *"security theatre"*.[24]
- **Visibility limits** – even with contractual audit rights, firms struggle to see beyond Tier-1 providers. *"The risk now hides in your vendor's vendor's code,"* said a tech CISO.[25]
- **Cloud concentration risk** – several respondents worried about over-reliance on two hyperscale providers: *"We've swapped data-centre lock-in for cloud lock-in."*[26]

Some of the mitigation strategies commonly observed included:

- **Risk-tiering suppliers** – high-impact vendors undergo deeper technical reviews and executive-level attestation.[27]
- **Software bill of materials** (SBOM) – some 'tech-forward' firms now demand SBOM transparency in contracts.[28]
- **Shared assurance pools** – interviewees from the finance sector described sector-wide utilities that conduct vendor audits once then share results, reducing duplication and improving leverage.[29]

Nevertheless, the consensus amongst respondents was that *"no one has cracked third-party cyber risk"*, with one regulator warning that cascading supply-chain incidents may pose *"systemic financial-stability concerns"*.[30]

The implication of this theme seems to be that boards must allocate explicit budget and authority for continuous supplier assurance - not episodic questionnaires. Sector collaboration and contractual innovations (e.g. SBOM clauses) show promise but remain unevenly adopted.



5. Human factors & organisational culture: the hardest layer to patch

Technical controls mattered to every participant, yet many insisted that *"people, not ports"* [31] remain the dominant vulnerability.

"Social-engineering still beats zero-days nine times out of ten."[32]

"We had five tools flag the phish; the finance assistant paid it anyway because 'the CEO sounded urgent'." [33]

20 Interview #19 – CEO, healthcare trust
21 Interview #19 – CEO, healthcare trust
22 Interview #5 – CRO, financial-services group
23 Interview #16 – Regional CISO, global logistics
24 Interview #11 – Public-sector security head
25 Interview #15 – CISO, consumer-retail group
26 Interview #6 – CISO, energy utility
27 Interview #8 – CISO, manufacturing conglomerate
28 Interview #14 – CISO, global insurer
29 Interview #4 – Deputy CISO, multinational bank
30 Interview #20 – Regulator, central-bank cyber unit
31 Interview #5 – CRO, financial-services group
32 Interview #14 – SOC director, global insurer
33 Interview #15 – CISO, consumer-retail group

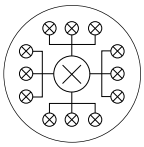
Some of the common cultural pain-points included:

Challenge	In their own words	Observed consequence
Security fatigue	*"If every e-mail is marked 'caution', staff eventually click everything."*[34]	Alert desensitisation; click-throughs rise after three months of a new filter.
Shadow IT habits	*"Traders spin up SaaS in minutes; IT hears about it when the invoice lands."*[35]	Data-exfiltration risk and licensing sprawl that security cannot monitor.
Mixed messages	*"The board preaches resilience, then rewards speed-to-market above all."*[36]	Project teams bypass security gates to hit launch dates.

There were, however, a few counter-measures that were credited with helping to mitigate human risks:

- **Embedded "security champions"** – business-unit liaisons translate policy into local context, *"cutting ticket volume."*[37]
- **'Live-fire' exercises** – organisations that ran ransom-call simulations with executives saw increased board buy-in and budget acceleration for resilience projects.[38]
- **Behavioural metrics** – one energy utility replaced generic phishing rates with *"risk-reduction per user"* tied to bonus schemes.[39]

This theme suggests that boards often assume culture change follows tool deployment; yet the evidence indicates the reverse. Sustained leadership signalling, cross-functional incentives and scenario-based learning are essential to convert awareness into secure behaviour.



6. Post-Covid perimeter collapse: remote work, cloud sprawl and device dilemmas

All interviewees mentioned the pandemic as an irreversible inflection point; remote-access scale-ups executed in weeks left lasting *'architectural debt'*.

"We set up split-tunnel VPN for 25,000 staff in 10 days – nobody reviewed the trust model."[40]

"Pre-Covid I knew every laptop; now I'm fighting personal iPads on home Wi-Fi." [41]

34 Interview #17 – CTO, national health agency

35 Interview #4 – Deputy CISO, multinational bank

36 Interview #2 – DevSecOps lead, fintech start-up

37 Interview #1 – CISO, industrial manufacturer

38 Interview #18 – Non-executive chair, FTSE-250 retailer

39 Interview #6 – CISO, energy utility

40 Interview #19 – CEO, healthcare trust

41 Interview #23 – University IT lead

Key stressors for organisations included:

- **Device proliferation** – endpoint counts doubled or tripled; Bring Your Own Device (BYOD) spiked in academia and smaller enterprises.
- **Cloud rush** – *"lift-and-shift first, secure later"* migrations resulted in mis-configurations during early Office 365 roll-outs.[42]
- **Identity overload** – password-reset social-engineering was the ingress vector for two high-profile breaches.[43]

Interviewees were also concerned about the massively enlarged post-Covid attack surface:

Layer	2019 baseline	2023 reality (median)
Managed endpoints	≈ 1 device / employee	1.8–2.3 devices / employee
SaaS applications	< 20	75–120 (finance/tech)
External identities (contractors)	Marginal	Equal to or greater than employee headcount.

Some of the mitigation measures – not always successful - included:

- **Zero-trust pilot projects** — logistics, banking and higher-ed CISOs are shifting from *"castle and moat"* to identity-centric controls; pilots confined to single business lines to reduce fatigue.[44]
- **Conditional-access and Multi-Factor Authentication (MFA) hard-lines** – several cyber leaders expressly mandated MFA for board members after observing targeted phishing.[45]
- **Endpoint standardisation battles** – one CISO tried enforcing institution-owned devices; the board pushed back.[46]

Some implications of this theme are that Covid-era 'quick fixes' have ossified into long-term exposures. Boards need to recognise that their organisations have to fund architectural refits—zero-trust, identity governance, endpoint management—rather than incremental patching of a dissolved perimeter.

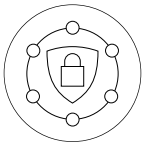
42 Interview #15 – CISO, consumer-retail group

43 Interview #21 – CISO, asset-management firm

44 Interview #16 – Regional CISO, logistics group

45 Interview #14 – CISO, global insurer

46 Interview #23 – University IT lead



7. Regulatory & liability pressures: from "best effort" to legal duty of care

Interviewees in every jurisdiction referenced a crescendo of regulatory scrutiny and potential personal liability.

> *"After the SEC rule, cyber-risk disclosure is no longer voluntary narrative; it's 8-K material."* [47]
>
> *"Directors ask me if they go to jail when the next breach hits – that focuses minds."* [48]

Some of the myriad regulatory drivers cited included:

Regime / rule	Primary impact in their own words
SEC cyber-incident disclosure (2023)	Mandatory reporting within four business days → *"board meeting in 48 hours"* protocols.[49]
EU DORA & NIS2	Extends accountability to ICT supply chain and senior management; cross-border banks scaling playbooks.[50]
GDPR & global privacy twins	Data-breach fines reframed cyber as monetary risk; *"privacy & security budgets merged."*[51]
Criminal-liability cases (e.g. USA v. Sullivan)	CISOs negotiating D&O coverage and clearer indemnification clauses.[52]

Several respondents welcomed regulatory clarity (*"finally a yardstick to justify spend"*[53]), but others feared a compliance-only mindset:

> *"Boards sometimes treat frameworks like a talisman – tick ISO and you're safe. Attackers don't read ISO."* [54]

The general implication here is that external pressures are elevating cyber on board agendas, yet organisations that conflate compliance with resilience risk a false sense of security. Successful firms treat regulation as a baseline, layering scenario testing and culture programmes above checklist conformance.

47 Interview #3 – CISO, US tech company

48 Interview #5 – CRO, financial-services group

49 Interview #3 – CISO, US tech company

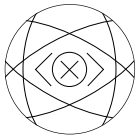
50 Interview #11 – Public-sector security head

51 Interview #10 – Data-privacy officer, EU telecoms provider

52 Interview #9 – CISO, North-American healthcare network

53 Interview #12 – CISO, asset-management (UK)

54 Interview #20 – Regulator, central-bank cyber unit



8. Evolving talent & operating models: multi-disciplinary teams, MSP reliance and role fatigue

This theme, concerning CISO skills and development, had two main tones: the lack of relevant new skills and the overload of existing CISOs.

> *"I'm part shrink, part diplomat, part technologist – which is not sustainable without wider bench strength."* [55]

Some of the key skillset shifts that were observed include:

Traditional need (pre-2015)	Emerging add-on (post-2020)	In their own words
Network & endpoint hardening	Data-governance / privacy-law literacy	*University CIO now chairs joint "Cyber-Data" committee.*[56]
Incident-response playbooks	Crisis-comms & investor-relations fluency	*CISO attends quarterly earnings prep.* [57]
Pen-test & SOC analytics	Supply-chain assurance & contract forensics	*"Reviewing SBOM became 30% of my week."* [58]
Technical leadership	Psychology / behavioural-science insight	*Ops lead (psychology degree) heads anti-phish programme.*[59]

Organisations are experimenting with different ways to address these issues, including:

- **Managed Service Provider (MSP) expansion** – many mid-size firms outsource SOC and vulnerability management. Benefits include 24/7 cover and cost predictability, but downsides are recognised to include *"shift-change drop-offs"* and *"ticket not context"* related failings.[60]
- **Internal capability hubs** – two of the global banks had built in-house "purple teams" blending offensive and defensive skills to reduce 'red-team' vendor spend.[61]
- **Sector talent pools** – healthcare and utilities executives proposed shared cyber-staffing pools to offset wage competition with Big Tech.[62]

The overload on CISOs was said to be increasing burnout & liability anxiety – increased board exposure and legal uncertainty in turn are driving turnover in the profession.

Several leaders spoke of peers taking sabbaticals or demanding contractual protections. One also described *"volatility of tenure"* as a risk in itself: *"The attackers know leadership churn resets priorities."*[63]

The implication of this theme is that boards must invest in sustainable operating models—whether internal centres of excellence or trusted MSPs—and acknowledge the multidisciplinary nature of modern cyber roles. Retention increasingly hinges on clear mandate, resources and liability cover.

55 Interview #9 – CISO, North-American healthcare network
56 Interview #23 – University IT lead
57 Interview #4 – Deputy CISO, multinational bank
58 Interview #14 – CISO, global insurer
59 Interview #14 – SOC director, global insurer
60 Interview #8 – CISO, manufacturing conglomerate
61 Deputy CISO, multinational bank
62 Interview #6 – CISO, energy utility
63 Interview #9 – CISO, North-American healthcare network

Evolving cyber governance

The research for this report supports the picture of the contemporary Chief Information Security Officer (CISO) stepping firmly out of the IT engine room and towards a *bona fide* strategic leadership role.

Many recent surveys have recognised that CISOs are increasingly expected to lean into executive leadership and enterprise risk management, keeping the C-suite apprised of how cyber threats impact organisational objectives, strategy, and business outcomes[1]. There is data suggesting that 60% of CISOs now engage with their board at least quarterly, presenting cyber risks as strategic business risks (not just IT problems)[2]. Our interview participants confirmed this trend, noting they have gained a regular slot in board meetings and are now frequently called on to translate security issues into the business terminology that boards understand.

However, our findings also reveal an uneven, and certainly more nuanced landscape than these surveys. For example, some of the CISOs we interviewed now report directly to the CEO. This shift underscores cybersecurity's integration into core business strategy and helps us understand that when CISOs engage directly at the highest executive level, they are able to champion cyber risk beyond simply reporting to the board. On the other hand, several CISOs we spoke to still report one or two rungs below the CEO and struggle to obtain board buy-in, indicating that the role's elevation is not universal. This nuance challenges any simplistic narrative that the CISOs strategic influence is assured. In fact, while global surveys highlight the CISOs rising profile, they tend to downplay just how many organisations are still catching up.

The World Economic Forum notes that today, effective CISOs frame cyber threats in terms of business continuity, reputation and financial impact – thereby enabling boards and CEOs to view cybersecurity as part of the broader risk landscape rather than a narrow technical silo[3]. Our interviews reinforce this, as CISOs who succeeded in quantifying cyber risk (e.g. impact on market share or brand trust) reported greater executive support. Yet, a few practitioners candidly admitted they lacked the business training to do this confidently, extending current thinking by highlighting a skills gap.

Our research shows how the CISO role is steadily shifting toward that of a **strategic risk adviser and business enabler**, but at the same time illustrates that many CISOs are still on this journey and will continue to face systemic and organisational hurdles before they achieve full strategic and governance integration.

Board–CISO collaboration and communication

Effective cybersecurity governance depends on a strong **bridge** existing between boards of directors and CISOs.

1 SentinelOne (2025) 'Cybersecurity 2025: Preparing for Tomorrow's Threats, Challenges and Strategic Shifts'. SentinelOne Blog. Available at: https://www.sentinelone.com/blog/cybersecurity-2025-preparing-for-tomorrows-threats-challenges-and-strategic-shifts/ (Accessed 3 June 2025).

2 World Economic Forum (2025) Global Cybersecurity Outlook 2025. Geneva: World Economic Forum. Available at: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf (Accessed: 3 June 2025).

3 Ibid

The interviews underscored both progress and ongoing tensions in this crucial relationship. On one hand, nearly all CISOs we interviewed agreed that board engagement has improved compared to a few years ago – boards are asking more informed questions and cybersecurity is now a standing agenda item in many organisations. This aligns with the broader shift in perception at the board level:

> *"88% of boards globally now view cybersecurity as a business risk rather than merely an IT issue."* [4]

Such recognition is a positive development, with some interviewees further noting that their boards actively seek their input on cyber risk during strategic planning or when undertaking major projects.

On the other hand, our findings also highlight a persistent gap between awareness and action in boardrooms – a tension also well documented in recent literature. Notably, some surveys suggest only 12% of corporate boards have a dedicated cybersecurity committee, and a mere 5% of companies include a director with cybersecurity expertise[5]. This structural shortfall was elaborated upon in several interviews: CISOs observed that while boards acknowledge cyber risks, they often lack the deep understanding or mechanisms to govern those risks effectively. One CISO interviewee wryly commented that *"boards nod gravely at cyber presentations, but then pivot to the financials,"* underscoring the challenge of sustaining meaningful engagement.

The UK's National Cyber Security Centre (NCSC) has flagged a related misunderstanding - over 80% of boards do not realise that accountability for cyber risk rests with them.[6] Our interviews confirmed this misconception persists in practice: some CISOs felt their board still views cybersecurity as the IT department's problem, rather than a shared responsibility in governance. This mismatch between board responsibility and board expertise can strain Board–CISO communication. As one interview participant put it, *"it's hard to get traction when my point of contact on the board doesn't know a firewall from a fire drill."*

Encouragingly, both the interviews and external guidance converge on solutions. Several CISOs described success by speaking the board's language – using risk metrics, business impact stories, and avoiding technical jargon – which echoes the NCSC's advice for cybersecurity leaders to couch issues in terms business leaders understand[7]. Building informal relationships with directors, rather than relying only on formal board meetings, was another practical tip from interviewees. Overall, our research findings reinforce current thinking that while Board–CISO collaboration is improving, it needs continued (interpersonal) investment. The tension between high board-level awareness and low cybersecurity governance maturity (e.g. lack of committees or expertise) suggests that organisations must move from simply talking about cyber risk to truly governing it. Our interviews make clear that closing this gap will require education, better communication, and perhaps bringing in outside experts or new directors to provide the cyber-savvy oversight that many boards currently lack.

Cybersecurity as a socio-technical system

A strong theme from the interviews is that cybersecurity is fundamentally a socio-technical challenge involving people, processes, and technology together. Practitioners repeatedly stressed that organisational and human factors often determine security outcomes as much as, if not more than, the technical controls in place. This perspective directly reinforces the modern view in cybersecurity governance literature that the systems we protect are complex socio-technical systems. The NCSC, for example, describes today's enterprise technologies as *"complex 'socio-technical' systems with interaction between technology, people and organisations."* [8] This complexity means there are times when security risks can be well understood and managed with standard controls, and times when they cannot due to unpredictable human elements or system interactions[9]. Our qualitative findings underscore this reality. CISOs in multiple interviews noted that even the best

4 Pandey, A. (2024) 'Beyond Oversight: The Board's Active Role in Cybersecurity'. LinkedIn Pulse 6 August. Available at: https://www.linkedin.com/

5 Ibid

6 The Stack Technology (2024) 'How CISOs Can Get Security Buy-In From the Board, According to the NCSC'. Available at: https://www.thestack.technology/security-buy-in-from-the-board/ (Accessed 3 June 2025).

7 National Cyber Security Centre (NCSC). (2025) How to talk to board members about cyber. Available at: https://www.ncsc.gov.uk/blog-post/how-to-talk-to-board-members-about-cyber (Accessed: 3 June 2025).

8 National Cyber Security Centre (NCSC). (2020) The Socio-technical Security Group Problem Book (v4.0). London: NCSC. Available at: https://www.ncsc.gov.uk/files/StSG-Problem-Book-v4-0.pdf (Accessed: 3 June 2025).

9 Bento Security (2024) 'Complex Socio-Technical Systems'. Bento Security Docs. Available at: https://docs.bentosecurity.com (Accessed 3 June 2025).

technical solution can be undermined by user error or poor process (e.g. an employee clicking a phishing link, or a critical patch not being applied because of organisational silos).

The interviews also extend current thinking by illustrating how viewing cybersecurity through a purely technical lens can lead to blind spots. One participant shared a case where an expensive new security software was rolled out, but little attention was paid to training staff or adapting workflows – resulting in minimal security improvement. Such anecdotes echo the adage that *"culture eats strategy for breakfast"* even in cyber. Indeed, frameworks like the WEF's Global Cybersecurity Outlook 2025[10] emphasise governance and process alongside technical measures precisely because of this socio-technical complexity. Our research findings reinforce that effective governance must account for the messy human realities: security policies must be usable, staff must be motivated and aware, and cross-functional collaboration is essential. As one CISO interviewee put it, *"our firewall never fails an audit – it's the people and processes around it that cause incidents."* This holistic appreciation of cybersecurity as a socio-technical system – one that encompasses human behaviour, organisational structure, and ethical decision-making – is a critical lens that our findings endorse and elaborate. Far from challenging current thinking, the interviews strongly support the consensus that:

"Cybersecurity governance must deal with systems, not just software, and manage an interplay of technical and social factors."

Organisational culture and distributed responsibility

Interviews with practitioners consistently highlighted organisational culture as a make-or-break factor in cybersecurity governance. A key finding is that:

"Cybersecurity can no longer be the sole responsibility of an IT or security department – it must be an organisation-wide, distributed responsibility."

Many CISOs reported that they are trying to cultivate a culture where *"security is everyone's job,"* but they acknowledged varying degrees of success. This aligns closely with practitioner insights from other recent publications which suggest that technical controls will ultimately **fail without an organisational culture that makes cyber risks everyone's responsibility**[11]. Our interviewees echo and add detail to this observation, describing efforts to engage other departments, appoint security champions in business units, and reward proactive security behaviour outside the IT team. In those organisations with more mature security cultures, CISOs observed fewer incidents caused by human error and more willingness by staff to report problems – concrete benefits of a culture of shared responsibility.

However, the interviews also revealed tensions and challenges in achieving such a culture. In some organisations, the refrain that "everyone is responsible" had paradoxical effects – a few CISOs noted that:

"When accountability is diffuse, some employees assumed someone else (usually IT) would handle security."

This resonates with the age-old cultural hurdle of translating slogans into practice: as one interviewee quipped, *"We plastered 'security is everyone's responsibility' on posters, but initially no one knew what actions were expected of them."* Our research therefore suggests that establishing clear roles and empowering people at all levels is key. In fact, governance experts advise delegating decision-making to

10 World Economic Forum (2025) Global Cybersecurity Outlook 2025. Geneva: World Economic Forum. Available at: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf (Accessed: 3 June 2025).

11 CyberOne (2024) 'Creating a Healthy Cybersecurity Culture in Your Organisation'. CyberOne Advisory. Available at: https://cyberonesecurity.com/advisory/creating-a-healthy-cybersecurity-culture-in-your-organization (Accessed 3 June 2025).

those best placed to understand the risks, as long as they have the right security knowledge and clear authority. Our findings reinforce this: organisations where department heads took ownership of cyber risks in their domain (with support from the CISO) tended to fare better than those with a top-down, centralised approach.

The interviews also support the idea that leadership and tone from the top are pivotal. Several participants pointed out that if the board and CEO visibly prioritise cybersecurity – for example, by following policies themselves and investing in awareness programmes – it cascades through the ranks. This is consistent with broader practitioner views. A recent industry report bluntly stated, *"It takes an entire ecosystem and culture of an organisation, united and aligned, with clear focus and priorities, to achieve cybersecurity maturity."* [12] In practice, our interviewees saw this play out as improved incident response and compliance when all business functions engaged in cyber resilience efforts. Conversely, in organisations where security culture was described as *"unhealthy"* or *"siloed"*, CISOs reported frustration with shadow IT, poor compliance with policies, and higher risk exposure. In summary, our findings strongly reinforce current thinking: building an effective cybersecurity culture that embeds good security habits and shared responsibility across the organisation is essential. They also extend the discussion by illustrating how hard this is to implement, yet also how impactful it can be when done right in terms of resilience and risk reduction.

Supply chain risk and ecosystem-wide resilience

Both the interview findings and various international surveys concur that cyber risk increasingly extends beyond the four walls of the organisation. Many CISOs we interviewed voiced growing concern over supply chain and third-party risks, often citing recent high-profile incidents where breaches in a supplier or partner cascaded into the primary organisation. This awareness reflects a broader trend: surveys indicate that *" between 39% and 62% of organisations have been affected by a cybersecurity incident at a third-party vendor or supplier"* [13]

As one interviewee in the critical infrastructure sector bluntly stated, *"We're only as secure as the weakest link in our supply chain,"* which encapsulates the collective sentiment. The literature also reinforces this. The European Union Agency for Cybersecurity (ENISA) reported that nearly:*"40% of cyber leaders and CEOs admitted being negatively affected by a supplier's security incident, and fully 58% of CEOs feel that their partners and suppliers are less cyber-resilient than their own organisation."*[14] Our qualitative findings align with this data: CISOs described investing more effort in vendor security assessments, contract clauses for cybersecurity and joint incident response planning with key suppliers.

However, the interviews also reveal challenges that extend current thinking on ecosystem resilience. Several CISOs noted the difficulty of enforcing or even assessing security standards across a diverse web of suppliers, especially for smaller partners who may lack resources. Some interviewees expressed frustration that their organisations have limited leverage over essential third parties (for example, a dominant software vendor), highlighting a tension: the ecosystem is only as strong as its most vulnerable node, yet individual firms may struggle to influence those external vulnerabilities. This practical insight adds nuance to the widespread call for better supply chain security. Think-tank and industry reports are indeed urging a more collective approach – WEF's outlook emphasises strengthening supply chain security as critical to resilience.[15] The concept of ecosystem-wide resilience is gaining traction, recognising that small businesses and service providers need uplift alongside large enterprises. Our findings reinforce this by illustrating the real risk of *"resilience gaps"*: one CISO from a global company observed that some of their smaller regional suppliers had very basic security, and adversaries could exploit those weaker links. This corresponds with warnings that the disparity in cyber defences between large and small entities threatens overall ecosystem security, as attackers use smaller entities as stepping stones into bigger targets.

In summary, our research strongly supports current thinking that cybersecurity is a shared concern across interconnected supply chains. If anything, our interviews amplify the urgency of addressing this weakness. They show boards and CISOs grappling with how to extend governance practices beyond organisational boundaries. Many practitioners now

12 Security Magazine (2024) 'Orchestrating Cybersecurity Across the Business Ecosystem'. Available at: https://www.securitymagazine.com/articles/91230-orchestrating-cybersecurity-across-the-business-ecosystem (Accessed 3 June 2025).

13 ENISA (2023) Good Practices for Supply-Chain Cybersecurity. Luxembourg: European Union Agency for Cybersecurity. Available at: https://www.enisa.europa.eu/sites/default/files/publications/Good%20Practices%20for%20Supply%20Chain%20Cybersecurity.pdf (Accessed 3 June 2025).

14 Ibid

15 World Economic Forum (2025) Global Cybersecurity Outlook 2025. Geneva: World Economic Forum. Available at: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf (Accessed: 3 June 2025).

view supplier risk assessments and third-party incident exercises as core parts of their governance program, not optional extras. As one interview participant noted, *"Our security team has turned into supply chain auditors and advisers as much as operators."* This perspective reinforces the idea that resilience must be built collectively. It also resonates with the notion of cybersecurity as a systemic risk: a single breach can now rapidly escalate into a widespread crisis, underscoring that cybersecurity is a *"shared, systemic challenge rather than a solitary corporate concern"*.[16] The findings here both reinforce and add concrete examples to the literature's calls for ecosystem-wide risk management, highlighting successes, such as cross-industry information sharing, and pain points, like the resource burden of vetting third parties – as organisations strive for holistic resilience.

Digital ethics and stakeholder accountability

A more nuanced theme that emerged from the interviews is the increasing importance of **digital ethics and accountability to stakeholders** in cybersecurity governance. While technical risk management remains central, many CISOs reported growing expectations from customers, regulators, and the public about how organisations manage cyber risks and incidents. For instance, multiple interviewees discussed the ethical dilemmas around breach disclosure such as the pressure to be transparent with those affected versus the instinct to limit reputational damage. The consensus was clear – transparency and honesty are not just moral choices but are now aligned with strategic decisions to maintain trust. This practitioner view dovetails with evolving global norms. Regulators are signalling that boards and executives must treat cybersecurity as part of their fiduciary duty to the company, its stakeholders and shareholders. In financial services, guidance now states plainly that ultimate accountability for cyber risk management rests with the board, to the extent that board members could be held personally liable for major lapses.[17] This reflects a wider trend to view cybersecurity not only as an operational issue but as a governance and ethics issue tied to corporate responsibility. Indeed, cybersecurity and data privacy are increasingly seen as elements of ESG (Environmental, Social, and Governance) performance that boards must oversee for sustainable business.

Our findings reinforce this integration of ethics and accountability. One interviewee from a consumer-facing industry mentioned that their board now discusses cyber risks in the context of customer trust and brand promise, not just compliance – a clear extension of accountability to broader stakeholder interests. Current thinking supports this: organisations are being encouraged to consider the stakeholder impacts of cybersecurity decisions, whether it's ensuring products are secure by design to protect users or weighing the ethical implications of cybersecurity measures (for example, surveillance vs. privacy of employees). The interviews also surfaced the human side of cybersecurity leadership. Several CISOs spoke of the personal ethical responsibility they feel – to do the right thing for customers, employees and partners when a cyber incident happens. This closely echoes thought leadership on the CISOs role in ethical decision-making. A recent report argues that CISOs must lead with integrity, ensuring prompt action, clear communication, and a focus on minimising harm to all stakeholders during incidents.[18] Our practitioners wholeheartedly agree: those who had experienced major incidents recounted how prioritising transparent communication, timely notification and strong support for affected parties ultimately preserved their company's reputation more than a cover-up would have.

In challenging or extending current thinking, our findings suggest that digital ethics in cybersecurity is not an abstract concept but an important emerging practice. This includes questions of fairness, transparency, and accountability that boards and CISOs are increasingly grappling with. For example, the ethics of paying ransoms, or decisions about collecting customer data for security purposes, were raised by some interviewees as areas where clear policies guided by values are needed. We observe that high-quality governance frameworks (e.g. those from the WEF or OECD) are beginning to incorporate principles of responsible cyber governance, emphasising duties to inform stakeholders and uphold trust. The interviews reinforce that trend: they show that leading organisations treat cyber incidents as not just a technical crisis, but a moment of accountability to stakeholders. In conclusion, our findings support the notion that robust cybersecurity governance now demands a strong ethical compass and a stakeholder-centric approach, aligning with regulators' and society's expectations for accountability when it comes to protecting data and digital systems.

16 Safe Security (2025) 'World Economic Forum: CISOs "Need to Quantify Cyber Risk"'. Safe Security Insights. Available at: https://safe.security/resources/blog/world-economic-forum-cisos-quantify-cyber-risk/ (Accessed 3 June 2025).

17 FS-ISAC (2024) Navigating Cyber 2024 Report. Reston, VA: Financial Services ISAC. Available at: https://www.fsisac.com/navigatingcyber2024 (Accessed 3 June 2025).

18 Cyber Security Tribe (2023) 'The CISO Ethical Dilemma: Why It Matters'. Available at: https://www.cybersecuritytribe.com/articles/the-ciso-ethical-dilemma (Accessed 3 June 2025).

Regulatory pressure across sectors and jurisdictions

The interplay between regulation and cybersecurity governance was a prominent theme in both the literature and our interviews. A critical insight from our interview conversations is that regulatory pressure on cybersecurity varies greatly by sector and geography, creating a patchwork of expectations for CISOs and boards. For instance, CISOs in highly regulated sectors like finance or healthcare spoke of frequent audits, mandatory board reporting on cyber risk, and detailed compliance requirements, whereas those in less-regulated industries voiced frustration about the lack of clear guidelines or external impetus to invest in security. Recent international developments reflect this divergence. In the European Union, the new NIS2 Directive explicitly introduces accountability of each entity's management for cybersecurity risk management compliance[19], effectively tightening the screws on board-level responsibility for cyber across many sectors. Financial services worldwide also continue to lead in cyber governance expectations – one study found that one-third of companies with *"advanced"* cybersecurity performance are in the financial sector[20], likely due to regulators driving stricter oversight in that industry. Meanwhile, the United States has recently implemented (in 2023) SEC rules requiring public companies to disclose their cybersecurity risk management, board oversight processes, and whether they have cyber expertise on the board. These moves support what one interviewee from a global company observed: *"The regulatory trend is only in one direction – toward more mandatory governance of cyber, not less."*

The interviews reinforce that regulatory context is a major factor shaping organisational behaviour. In sectors under intense scrutiny (e.g. banking, utilities, telecoms), CISOs described well-established governance routines such as board committees focused on cyber risk, regular reporting of metrics, and even regulatory inspections of cyber programs. By contrast, some interviewees in sectors without specific cyber regulation noted that executive attention on security was driven largely by internal risk appetite or high-profile incidents rather than by law. This finding aligns with global survey data: 76% of CISOs report that navigating fragmented or complex compliance requirements is a significant challenge.[21] Many organisations operate across jurisdictions and industries, so CISOs must reconcile a patchwork of standards – from EU's GDPR and NIS2, to US state data breach laws, to sectoral rules like healthcare's HIPAA or finance's PCI-DSS – which was a sentiment voiced in several interviews. Notably, one CISO of a multinational firm shared that they maintain a *"compliance map"* to brief their board on various cyber obligations country by country, highlighting the practical burden of regulatory complexity.

While our findings largely reinforce the notion that regulatory pressure is a key driver of cyber governance (and that this pressure is escalating), they also extend the discussion by showing some unintended effects. A few interviewees cautioned that a checkbox compliance mentality can creep in – boards might fixate on meeting regulatory minima rather than addressing the spirit of security. For example, a CISO mentioned, "Our board is very keen to tick all the compliance boxes for the new regulations, but I worry we might be missing the bigger picture of actual risk reduction." This suggests that governance maturity involves going beyond compliance. Think tanks like the World Economic Forum advocate for treating regulation as a baseline and encouraging proactive, risk-based governance above those baselines.[22] The interview insights support this view: they reveal that the most cyber-resilient organisations often voluntarily exceed regulatory requirements, using them as a springboard rather than a ceiling.

In sum, our findings underscore that regulatory forces are powerful in shaping cyber governance – varying across sectors/jurisdictions – and that organisations must navigate this landscape carefully. They must strive to meet diverse compliance obligations while also developing a unified, enterprise-wide governance approach that doesn't get lost through fragmentation. The challenge of regulatory variation is thus firmly on the agenda, and our interviews confirm it is front-of-mind for practitioners, reinforcing the ongoing push for harmonisation and higher standards globally.

19 ENISA (2023) Good Practices for Supply-Chain Cybersecurity. Luxembourg: European Union Agency for Cybersecurity. Available at: https://www.enisa.europa.eu/sites/default/files/publications/Good%20Practices%20for%20Supply%20Chain%20Cybersecurity.pdf (Accessed 3 June 2025).

20 Security Magazine (2024) 'Orchestrating Cybersecurity Across the Business Ecosystem'. Available at: https://www.securitymagazine.com/articles/91230-orchestrating-cybersecurity-across-the-business-ecosystem (Accessed 3 June 2025).

21 Guerin, T. (2025) 'Beyond IT: Cybersecurity as a Core Governance Responsibility', LinkedIn, 11 March. Available at: https://www.linkedin.com/pulse/beyond-cybersecurity-core-governance-responsibility-turlough-guerin-obvuc/ (Accessed: 3 June 2025).

22 Harvard Law School Forum on Corporate Governance (2022) 'Building Effective Cybersecurity Governance'. Available at: https://corpgov.law.harvard.edu/2022/11/10/building-effective-cybersecurity-governance/ (Accessed 3 June 2025).

Training, education, and professional development needs

Finally, an area that both interviewees and literature sources converged on – and is a fitting theme to conclude on - is the pressing need for continuous training and education in cybersecurity governance – for CISOs, boards, and indeed all organisational actors with cyber responsibilities.

The qualitative interviews revealed a stark skills and knowledge gap at the governance level. Many CISOs recounted how they spend significant time educating their board and senior executives about cyber risks, sometimes starting with basic concepts or, in one case, exposing directors' passwords. But CISOs also acknowledged their own shortcomings, and were aware how important it was to constantly develop new competencies – from understanding business strategy and finance to mastering soft skills in communication and influence. These observations resonate strongly with practitioner-oriented guidance internationally. In fact, a U.S. Cybersecurity Advisory Committee in 2023 recommended delivering cyber education *"at scale and continuously"* for corporate directors **and** CISOs, urging the creation of platforms for ongoing cyber literacy training.[23] It went as far as to suggest promoting formal cybersecurity certification for board members, and encouraging companies to seek such qualifications in their director recruitment. The logic is straightforward:

"Boards with even a baseline of cyber competence can govern more effectively, and CISOs with training in risk communication can better bridge the gap."

Our interviews strongly reinforced this view. Several CISOs said that after their board attended external cyber governance workshops (in one case, a session run by the national cyber agency), the quality of board questions and support improved markedly. Likewise, CISOs who had invested in executive education or business leadership courses felt better equipped to translate technical issues into strategic discussions.

Our research, in addition, also highlights some innovative practices as well as areas needing development. A few organisations represented in the interviews have begun incorporating cybersecurity into wider management training and even onboarding for new managers, signalling that cyber awareness is becoming part of general management competence. This reflects a growing view that cybersecurity is analogous to financial literacy – a fundamental part of a leader's toolkit. High-profile institutes and associations (e.g. NACD, ISC2) have rolled out cyber-risk oversight training programs for directors, which were mentioned by some participants as useful resources.

At the same time, the findings challenge organisations to do more. One recurrent theme was that annual training or a one-time seminar is not sufficient.Both directors and technical leaders benefit from continuous learning and upskilling, given how fast the threat and regulatory environment evolves. CISA's guidance for boards emphasizes a continuous education mindset, not a one-off, which our interviewees certainly echoed. Importantly, training is not just for boards: CISOs in our study noted the value of mentorship and peer networks to develop their own strategic acumen. There is also a recognised need to educate other actors like risk officers, legal counsel, auditors, and business unit leaders on cybersecurity to create a common understanding across the organisation. This comprehensive approach to capacity-building is increasingly seen in leading practice.

In reinforcing current thinking, our interviews strongly support the idea that investing in people's cyber governance skills is as critical as investing in technology. They provide real-world validation that educated boards engage more, and well-rounded CISOs (with business and leadership skills) perform better in governance roles. The discussion also shows that this is not purely an in-house effort: many called for industry bodies and governments to facilitate more accessible training, information-sharing forums, and certification pathways. We also saw encouraging trends such as boards voluntarily bringing in outside experts or appointing directors with cyber backgrounds (though this seems to still be rare).

23 CISA (2023) Cybersecurity Advisory Committee Recommendations (December 2023). Washington, DC: Cybersecurity and Infrastructure Security Agency. Available at: https://www.cisa.gov/resources-tools/resources/cybersecurity-advisory-committee-csac-reports-and-recommendations (Accessed 3 June 2025).

Conclusion

The findings underscore a clear message: continuous professional development for both security and business leaders is vital to keep cybersecurity governance effective. Building cyber literacy in the boardroom and business literacy in the security team will help bridge the remaining gaps identified in all the themes above – from strategic alignment and communication to ethical decision-making and resilience. The commitment to education and training emerges as a foundational enabler of progress in cybersecurity governance, reinforcing every other insight from this research and the wider literature.

Approach: carrying out the research

We adopted a rigorous qualitative approach centred on in-depth expert interviews with a global, cross-sector group of cyber-governance practitioners – including CISOs, board directors, regulators, risk officers and cyber-policy professionals.

23 participants were selected to ensure diversity in sector (e.g. finance, healthcare, government, critical infrastructure), geography (representation from multiple regions), gender and professional background. Notably, we included experts who entered cybersecurity via non-traditional routes such as law, criminology and risk management, not only those from IT or engineering. This breadth of perspectives was deliberate, allowing the research to capture a wide range of real-world governance experiences and challenges. All interviews were conducted one-to-one via secure video-conferencing (Microsoft Teams or Zoom), providing a consistent and confidential environment for discussion.

Critical Incident Technique (CIT)[1]

To move beyond generic commentary and get to the heart of cyber governance in practice, we used CIT. Interviewees were asked questions relating to specific events, decisions or 'critical incidents' they had encountered during their career and in their current role. Instead of answering abstract questions, they recounted concrete situations – for example, a particular cybersecurity crisis, a boardroom decision on cyber risk, or a significant policy implementation – and described what happened in detail. This technique elicited context-rich narratives rather than high-level generalisations. By focusing on real incidents, we captured the often messy reality of cyber governance: how policies play out on the ground, how decisions are made under pressure, and how various stakeholders interact in actual scenarios. CIT also encouraged interviewees to reflect and elaborate on internal reasoning and motivations for actions and decisions, adding further richness and opportunities to learn from the analysis[2].

Data capture and transcription

Each interview (lasting roughly 60–90 minutes) was conducted either in-person or via Zoom or Teams, and audio-recorded with the participant's consent. To preserve insights accurately, we transcribed all interviews using AI-powered transcription tools (DeepSeek, ChatGPT or in-built tools). The AI provided a fast initial draft, which was then manually reviewed and corrected by the research team to ensure accuracy. This two-step process combined efficiency with rigour: the AI captured a detailed record of each conversation, and human checking preserved nuances (such as industry-specific terminology or tone) that automated methods might miss. The result was a rich qualitative dataset of expert testimonies.

Qualitative analysis with AI support[3]

1 Flanagan, J. C. The Critical Incident Technique. Psychological Bulletin, 1954, 51 (4), 327-358.

2 Ahmad, A., Hadgkiss, J., & Ruighaver, A. B. (2012). Incident response teams–challenges in supporting the organizational security function. Computers & Security, 31(5), 643-652.

3 Amani, S., White, L., Balart, T., Watson, K., & Shryock, K. Applying Generative AI for Thematic Analysis: A Model for Researchers Exploring Qualitative Methods. SSRN Working Paper, 2025.

We imported the validated transcripts into qualitative-analysis software equipped with AI-assisted coding features. Using this platform, we conducted an iterative thematic analysis to identify and organise key themes, patterns and insights across the interviews. Our coding process began with an initial framework based on our research questions, and evolved as new insights emerged. The software's AI capabilities helped cross-reference themes and quickly surface patterns (e.g. highlighting when multiple experts independently cited similar challenges), enhancing our ability to compare experiences across different organisations and sectors. All AI-generated suggestions were reviewed to ensure they accurately reflected the interview content. This blend of AI efficiency and human judgement aligns with emerging innovations in qualitative research[2]. Throughout the analysis, we kept a clear evidence trail: every theme in the white paper can be traced back to multiple, concrete examples from the interviews.

The voice of participants

To preserve the authentic voice of participants and give readers direct insight into the data, we rely heavily on verbatim quotations. When presenting findings, we include carefully selected, anonymised quotes that illustrate key points. Using participants' own words adds credibility and richness, ensuring tone and individual meaning are retained rather than diluted into purely analytical summaries.

Anonymity and ethical safeguards

Given the sensitive nature of cyber governance and our use of the Critical Incident Technique, it was essential to ensure confidentiality for all participants. All interviewees were guaranteed anonymity; no quotes or examples are attributed to specific individuals or organisations. Participants consented on the basis that neither they nor their companies would be identified. This encouraged candour – experts could speak openly about challenges, including potentially controversial incidents, without fear of sensitive information being made public or repercussions. We also adhered to standard research-ethics procedures: participants were informed about the purpose of the research, how the data would be used and their right to withdraw at any time.

Strengths and limitations

The research draws its strength from the use of the Critical Incident Technique (CIT), which generated rich, experience-based insights grounded in real-world events rather than abstract opinion. A deliberately diverse sample—spanning regions, sectors, genders, and career paths—ensured a multifaceted view of cyber governance. The analysis was further strengthened by the integration of AI-enhanced transcription and coding tools, which improved efficiency and consistency, while manual oversight preserved contextual nuance. However, the approach was also time-intensive, with the identification, briefing, interviewing, and validation of participants requiring considerable effort. As with most qualitative research, the findings are not meant to be statistically generalisable, but are instead intended to illuminate patterns and lived realities of this dynamic, fast-evolving area. Additionally, while the focus on critical incidents enhances authenticity, the reliance on participants' memory introduces potential recall bias (although this was partially mitigated through document cross-checking). Overall, this methodology ensures that the report's insights are both credible and grounded, offering a textured understanding of the current state of cyber governance at the leadership level. In summary, this methodology ensures that our insights are evidence-based, reliable and grounded in real-world experience.

About the author & acknowledgements

Simon Learmount

Associate Professor Corporate Governance,
Cambridge Judge Business School, University of Cambridge

Simon Learmount is Professor of Corporate Governance at Cambridge Judge Business School and Fellow of Pembroke College, University of Cambridge. He has served as Director of both the MBA and Executive MBA Programmes at Cambridge Judge Business School, and is recipient of the Pilkington Prize, awarded by the University of Cambridge to honour outstanding teaching across the university. His research focus is on international corporate governance (notably in the US, UK, Japan and China) with a concentration on digital (including cyber-security and AI) and sustainability (including climate and nature) governance and ethics. He serves as co-chair of the World Economic Forum Climate Governance Expert Committee, is a member of the Global Futures Council on Climate and Nature, advises multiple organisations on digital and cyber governance, sustainability and green transition, risk management and director development.

Acknowledgements

We are grateful to the business and industry leaders who supported this important study, taking time to share candid perspectives and valuable personal insights.

ISTARI

ISTARI is a global cybersecurity firm, established by Temasek in 2020, with a unique model for helping clients build cyber resilience.

Our mission is to help organisations achieve lasting cyber resilience with a whole-of-company approach, by leveraging peerless talent, expertise, and innovation through an unparalleled network - with ISTARI at the centre. Our vision is to curate the defining cyber resilience ecosystem of our time - uniting academia, enterprise, practitioners, policymakers, and innovators to outpace cyber risk and build collective resilience.

Cambridge Judge Business School,
University of Cambridge

Cambridge Judge Business School is a world leader in business research and education, embedded within one of the world's most prestigious research universities. Established in 1990, the School pursues innovation through inter-disciplinary insight, entrepreneurial spirit and collaboration. Located at the heart of the Cambridge Cluster (Silicon Fen) - Europe's most successful technology cluster - the School has unrivalled access to entrepreneurial networks and innovation opportunities. Cambridge Judge was ranked #1 in the UK's Research Excellence Framework for business and management studies, with 94% of research submissions rated as 'world leading' or 'internationally excellent'.
The School offers transformative programmes that attract innovators, creative thinkers, and future leaders from diverse backgrounds globally, all committed to solving real-world problems with lasting societal impact.

ISTARI