THALES
Building a future we can all trust

The next outage is preventable:

BOARD ACCOUNTABILITY FOR CYBER RISK

WHITEPAPER

EXECUTIVE SUMMARY

Cybersecurity has evolved from a technical concern to a core component of enterprise business value. It affects market confidence, customer trust, operational continuity, revenue, ESG positioning, and regulatory exposure. Cyber risk is business risk.

Global regulatory changes — including the U.S. SEC Cybersecurity Disclosure Rules (2023–2024), the EU NIS2 Directive (2024), and the Digital Operational Resilience Act (DORA, 2025) — now place in many regions explicit responsibility on Boards of Directors to oversee cyber risk.

Boards now have a fiduciary, regulatory and reputational duty to govern cybersecurity.

However, most Boards lack the structural conditions to do this effectively:

a. 88% of Boards view cybersecurity as a business risk (Gartner: "2022 Gartner Board of Directors" survey)

b. but only 26% of S&P500 companies have a director with cybersecurity experience (Harvard Law School: "Board Practices and Composition: 2024")

This whitepaper proposes a practical governance model that Boards can implement without needing deep technical expertise. It reframes cybersecurity as a business risk that requires:

3. Clear accountability
4. Business-aligned reporting (not technical metrics)
5. Investment decisions tied to risk and value
6. Board participation in cyber resilience exercises

It also introduces a high-value analogy: how Boards in high-hazard safety industries (oil & gas, mining, aviation) learned to govern complex risks effectively — and how that same model and learnings can be applied to cybersecurity governance.

1. CYBERSECURITY IS NOW A BUSINESS RISK

1.1 CYBERSECURITY IS NOT AN IT PROBLEM

Cyber risk is now a business issue not just an IT problem. Cyber incidents translate to business risks very quickly as the table below shows:

BUSINESS DIMENSION	CYBER IMPACT
Revenue	Ransomware can halt production, sales, or fulfilment
Operations	Cloud or OT disruption can stop business-critical functions
Shareholder value	Public breach notifications causes a share price drop
Regulation	Fines, sanctions, licence suspension (e.g., DORA)
ESG & trust	Data breaches damage brand and credibility

Most breaches are not caused by lack of technology — they are caused by gaps in governance:

- unclear accountability
- insufficient challenge from the Board
- no linkage between cyber spend and business value
- fragmented ownership between CIO and CISO
- lack of understanding of the IT and Operational Technology risk landscape

1.2 REGULATION MAKES CYBER GOVERNANCE A BOARD RESPONSIBILITY

Globally regulation is making cybersecurity a board issue

REGULATION / STANDARD	GOVERNANCE EXPECTATION ON THE BOARD
Cyber Security & Resilience Bill (UK)	Expands industries covered and make boards accountable for cyber governance at the strategic level. Organisations may face civil, fiduciary and regulatory penalties if harm to organisation, stakeholders or critical infrastructure. This also places specific responsibility on suppliers to public sector bodies and critical infrastructure operators.
NIS2 (EU)	Board members can be held personally liable for cyber governance failures; mandatory board cyber training.
DORA (Financial services, EU)	Board accountable for ICT resilience, testing, and third-party cyber risk.
ISO/IEC 27001:2022 & ISO/IEC 42001	Board must approve security governance, risk appetite, policies.
NIST CSF 2.0 (2024)	Introduces a Governance pillar emphasising accountability at executive and board level.

Cyber governance is no longer optional — it is a core part of business risk management.

2. WHY BOARDS STRUGGLE WITH CYBER ACCOUNTABILITY

Boards are being held responsible for cybersecurity, but many lack the company structure, information and knowledge to govern it.

Structural barriers:

BARRIER	IMPACT
Cybersecurity reported as technical detail	Board cannot assess business exposure or risk level
CISO buried under CIO hierarchy	Cloud or OT disruption can stop business-critical functions
CISO excluded from OT decisions	Public breach notifications causes a share price drop
Cyber investment framed as cost, not value	Fines, sanctions, licence suspension (e.g., DORA)
No standardised Board reporting	Data breaches damage brand and credibility
Lack of cyber literacy on the Board	Inability to challenge or probe management assertions

The end result is that even though boards are accountable, they are structurally blind with many cybersecurity decisions being made in a fragmented and incoherent way.

3. CYBER GOVERNANCE FRAMEWORK FOR BOARDS

Boards should govern cyber risk in the same way as they do financial risk or health and safety risks:

Board responsibilities:

1. Approve cyber risk appetite
   - Define what level of cyber exposure the organisation is willing to tolerate.
2. Hold executive leadership accountable
   - Require ownership, action plans, and maturity objectives.
3. Receive business-oriented reporting
   - Ask for financial and operational impact as well as cyber incidence frequency, not patch counts.
4. Participate in cyber crisis simulations
   - Validate that escalation, decisions, and communications work under pressure.

4. RISKS, STRUCTURAL ISSUES & GOVERNANCE SOLUTIONS

So how does business risk and structural issues interact and how can boards address the issue? The following table looks at each challenge and proposes a simple to implement solution.

CATEGORY	BUSINESS RISK	STRUCTURAL ISSUE	BOARD-LEVEL SOLUTION
Strategy	Cyber not considered in digital programmes or M&A	Cyber viewed as technology workstream	Require cyber impact assessments for all major initiatives
Oversight	Board blindsided by incidents	Reporting too technical, not risk-based	Require business-aligned dashboards (risk, exposure, trend)
Accountability	No single point of ownership	CISO reports through CIO (budget dependency)	CISO must have direct reporting access to Board/ Risk Committee
Resourcing	Underfunding increases probability of breach	Cyber investment framed as cost	Use business-case logic: avoided loss > cost of mitigation
Third-Party Risk	Supplier breach impacts operations	No standardised supplier assurance	Minimum security requirements + third-party cyber scorecard
Incident Response	Delayed board decisions worsen impact	Board not involved in simulations	Annual board cyber drill with decision points

5. WHAT BOARDS NEED IN CYBER REPORTING

Boards need to move to reporting focusing on the following:

REPORT TYPE	WHAT IT SHOULD ANSWER
Cyber risk heatmap	What could disrupt us, financially or operationally? So what systems are vulnerable and what would be the impact
Exposure reduction trend	Are risks increasing or reducing? What is the frequency of attack attempts, successful breaches (but no operational impact), and serious breaches (operational impact)
Maturity progression (NIST/ISO)	Are we improving year-on-year? Periodic audits to ascertain maturity. Clear analysis of breaches and action plan to prevent repeat
MTTR (Mean Time to Respond)	How fast can we detect and stop a breach? Regular testing and exercising of systems and processes to detect how quickly an organisation can response on contain.

A board level strategic KPI dashboard looking at organisational readiness and maturity:

STRATEGIC KPIS	CURRENT	TARGET	TREND
Cyber risk reduction (% critical risks with mitigations delivered)	50%	90%	↑
High Severity Incident Count (quarterly)	1	0	↓
Cyber crisis simulation cadence	Annual	Quarterly	↑
Third-party critical vendor compliance	70%	95%	→
Overall cyber maturity (1–5)	2	4	↑
Cyber budget adequacy (budget as % of IT spend)	10	15%	→

A board level operational KPI dashboard looking at technical maturity:

OPERATIONAL KPIS	CURRENT	TARGET	TREND
Detect and contain a breach - Mean Time to Respond (hours)	72	24	→
% of critical patches implement in X day target	70%	95%	↓
Privileged access recertified (users verified and MFA implemented)	90%	99%	↑
Zero Trust Adoption (% apps using strong authentication & least privilege)	50	100%	→

6. INVESTMENT AND ROI: CYBER SPEND AS VALUE PROTECTION

Boards need to see cybersecurity in business terms. Most organisations reject cybersecurity funding when it's framed as:

"We need money for MFA, SIEM upgrades, network segmentation..."

However boards approve cybersecurity funding when framed as:

"A breach would cause direct mitigation costs of £X, operational losses of £Y and indirect loss from brand damage of £D.

Mitigating it costs £A

Cyber ROI = Avoid loss – Mitigation cost"

7. CYBER GOVERNANCE OPERATING MODEL

Reporting lines need to change from going via the CIO to all other parts reporting through the CISO on cybersecurity risk and investment.

Key governance rule:

CISO independence is critical. A CISO reporting through a CIO introduces inherent conflict (delivery speed vs security) and tends to exclude operations and engineering functions who make a lot of decisions that also impact an organisation's cybersecurity posture.

8. SAFETY GOVERNANCE AS THE BLUEPRINT FOR CYBER

High-hazard industries (oil & gas, mining, aviation, nuclear) introduced safety governance decades ago. They succeeded because:

- Potential business risks were clear: loss of operating licenses, criminal and civil liabilities, withdrawal of insurance cover, loss of business due to brand damage
- Accountability could not be delegated as management and board held legally responsible
- Reporting focused on leading indicators such as near misses and long-term injury frequency which provided a good indicator of likelihood of a serious injuries or deaths occurring.
- Culture made safety everyone's responsibility. Everyone encouraged to share safety concerns and learnings as often as possible. Managers who cut corners on safety subject to serious disciplinary action.

Cybersecurity is following the same trajectory.

Safety vs Cyber Governance (Comparative Model)

DIMENSION	SAFETY GOVERNANCE (HIGH-RISK INDUSTRIES)	CYBER GOVERNANCE (TARGET STATE)
Business risk	Loss of operating licenses, loss of insurance, loss of customer business, criminal and civil liabilities	Loss of operating licenses, loss of insurance, loss of customer business, civil liabilities
Accountability	Board personally accountable	Board accountable under forthcoming Cyber Security and Resilience Act & UK Companies Act 2006; NIS2; DORA
Reporting	Leading indicators + risk controls	Risk dashboards + maturity trend
Culture	"Safety is everyone's job"	"Cyber is everyone's job"
Controls	Critical controls tested routinely	NIST/ISO control validation
Escalation	Board participates in drills	Board participates in cyber simulations

Cyber is simply the modern equivalent of organisational safety.

9. HOW ORGANISATIONS SHOULD IMPLEMENT THESE RECOMMENDATIONS (12–24 MONTHS)

PHASE	BOARD ACTION	OUTCOME
Quarter 1	Approve cyber charter, define risk appetite	Clear accountability
Quarter 2	Implement reporting and dashboards	Visibility of risk posture
Quarter 3	Conduct board cyber crisis simulation	Board readiness
Quarter 4	Introduce third-party cyber assurance	Supply chain resilience
Quarter 5–8	Mature controls and continuous improvement	Target maturity achieved

CONCLUSION

Cybersecurity has become a defining component of enterprise resilience.

Boards that govern cyber effectively:

- accelerate digital transformation safely
- increase shareholder and customer trust
- avoid regulatory and reputational damage
- build organisational resilience and competitive advantage

Boards that fail to govern cyber:

- will be held accountable — legally, reputationally, and financially.

Cybersecurity is not a technology issue. It is corporate stewardship.

THALES

Building a future we can all trust

350 Longwater Avenue
Green Park
Reading
RG2 6GF
United Kingdom

+44 (0) 118 943 4500

>thalesgroup.com<