WHITEPAPER

The CISO Transformation Playbook:

From Cost Centre to Chief Trust Officer

How Security Leaders Transform Regulatory Compliance into Revenue Enablement,

Board-Level Influence, and Measurable Business Value Under DORA and NIS2

Kieran Upadrasta

CISSP, CISM, CRISC, CCSP | MBA | BEng

27 Years' Cyber Security Experience | Big 4 Consulting

21 Years Financial Services | AI Governance & DORA Compliance Expert

www.kie.ie | info@kieranupadrasta.com | January 2026

Table of Contents

Executive Summary

THE CISO TRANSFORMATION PROMISE

Transform from cost centre to growth driver and Chief Trust Officer:

Board-level influence • Revenue enablement • 4:1+ Security ROI • Competitive advantage

Within 12 months of implementing the Trust Value Flywheel™

The Stakes: Why CISOs Must Transform Now

The traditional CISO operating model—focused on technical controls, cost minimisation, and IT reporting—is now both legally inadequate and commercially obsolete. For the first time in regulatory history:

- **€1,000,000 personal fines** per executive under DORA [1]
- **Temporary or permanent management bans** under NIS2 [2]
- **Criminal conviction precedent** established (Uber CSO Joe Sullivan) [3]
- **SEC enforcement actions** against CISOs for misleading disclosures [4]

Four Critical Insights from 52 Board Assessments

1

Security leaders who speak business language achieve 73% greater strategic involvement

CISOs who translate technical metrics into financial terms (FAIR quantification, revenue impact, cost avoidance) are 73% more likely to achieve board-level strategic influence. [5]

2

Only 2% of companies have implemented firm-wide cyber resilience

Despite $262 billion in global cybersecurity spending, PwC's 2025 Global Digital Trust Insights found only 2% of organisations claim full cyber resilience—revealing a governance gap, not a technology gap. [6]

3

CISO-to-CEO reporting correlates with 4:1+ security ROI

Organisations where CISOs report directly to the CEO (14%, up from 5%) demonstrate security ROI of 4:1 or higher, compared to 2:1 for traditional IT reporting structures. [7]

4

82% of compliant companies still experienced breaches

> Checkbox compliance is insufficient. Research shows 82% of organisations that achieved regulatory compliance still experienced breaches within the following year—proving culture beats compliance. [8]

Three Actions for CISOs This Quarter

ACTION 1	ACTION 2	ACTION 3
Build Financial Fluency Implement FAIR risk quantification to translate cyber risk into financial terms	**Establish Board Cadence** Secure quarterly board reporting with 12-KPI dashboard (Section 10)	**Document Business Value** Track and present security as revenue enabler, not cost centre

📌 KEY TAKEAWAYS

→ Personal liability under DORA/NIS2 makes CISO transformation legally mandatory, not optional

→ The Trust Value Flywheel™ provides a systematic framework for moving from cost centre to value driver

→ 82% of compliant organisations still breach—governance culture matters more than checkbox compliance

→ CISOs reporting to CEO achieve 4:1+ security ROI compared to 2:1 for IT-reporting structures

1. The Problem: Why Traditional CISO Models Are Failing

🎯 **STRATEGIC LENS:** *This section examines why the traditional cost-centre CISO model has become legally inadequate and commercially obsolete under DORA/NIS2—and what replaces it.*

🔴 **THE GOVERNANCE FAILURE CASCADE**

95% of breaches involve human error [9] • 82% of compliant companies still breached [8] • 38% of CISOs lack D&O coverage [10] • Only 2% of companies 'fully resilient' [6]

1.1 The Broken Model: Security as IT Expense

For two decades, organisations have treated cybersecurity as a technical expense to minimise—delegated to IT departments, measured by cost reduction, and reviewed only after incidents. This model has failed catastrophically:

- **$4.88 million** average breach cost in 2024—all-time high [11]
- **$10.22 million** U.S. average breach cost 2025—all-time regional high [11]
- **35.5% of all breaches** originated from third-party compromises (up 6.5% YoY) [12]
- **80%+ of CISOs** report significant burnout and strain [13]

> *"Compliance may be incomplete as a cybersecurity measure. Both Equifax and Target were PCI-compliant when breached."*
>
> **— MIT Sloan Management Review, 2024**

1.2 Why Checkbox Compliance Fails

❌ Checkbox Compliance	✓ Trust-Based Security
Audit-driven, annual exercises	Continuous improvement culture
Minimise security spend	Optimise risk-adjusted returns
React to incidents	Build resilience proactively
Report to CIO/IT	Board-level stewardship
82% still breached [8]	**43% higher revenue growth [14]**

📌 KEY TAKEAWAYS
→ Traditional cost-centre models have failed—$4.88M average breach cost despite $262B annual spending
→ Compliance ≠ Security: 82% of compliant organisations still experience breaches within 12 months
→ The Trust Value Flywheel™ replaces checkbox compliance with systematic value creation

2. The Trust Value Flywheel™: A Proprietary Framework

STRATEGIC LENS: *This section introduces the Trust Value Flywheel™—a proprietary framework for transforming security from cost centre to capital creation engine.*

THE TRUST VALUE FLYWHEEL™

A Self-Reinforcing Value Creation Engine

1. INVEST

Strategic security investment

↓

2. BUILD TRUST

SOC 2, ISO 27001, demonstrable resilience

↓

3. ENABLE REVENUE

Accelerated sales, reduced friction

↓

4. CAPTURE VALUE

Valuation premium, M&A positioning

↓

5. REINVEST → [Returns to Step 1]

Expand capabilities, accelerate returns

The Trust Value Flywheel™ reconceives security as a self-reinforcing value creation engine. Unlike linear compliance models, the flywheel accelerates over time as each element strengthens the others. [15]

2.1 The Five Flywheel Components

Component	Value Creation Mechanism
1. INVEST	Strategic security investment aligned with business objectives, measured by risk-adjusted returns rather than cost reduction.

2. BUILD TRUST	Transform security posture into trust capital through certifications (SOC 2, ISO 27001), transparent communications, and demonstrable resilience.
3. ENABLE	Convert trust capital into revenue enablement: accelerated sales cycles, reduced customer due diligence friction, premium positioning.
4. CAPTURE	Translate business value into valuation premium: improved M&A positioning, favorable insurance terms, reduced cost of capital.
5. REINVEST	Deploy captured value into expanded security capabilities, creating a virtuous cycle of accelerating returns.

KEY FINDING

Organisations implementing the Trust Value Flywheel™ report 43% higher revenue growth over five years and achieve security ROI of 4:1 or higher—transforming security from cost centre to competitive advantage. [14]

> *"Two-thirds of business leaders now see cybersecurity primarily as a revenue enabler rather than a cost centre."*
>
> **— IBM Institute for Business Value, 2024 [16]**

3. Research Methodology: 52 Board Assessments

🎯 **STRATEGIC LENS:** *This section documents the methodology behind our proprietary research, providing transparency for academic and professional validation.*

3.1 Study Design and Sample Composition

Between January 2023 and December 2025, we conducted comprehensive cyber governance assessments across 52 organisations in the UK and EU, using a structured evaluation framework aligned with DORA and NIS2 requirements.

Sector	Count (n)	Percentage	Avg Revenue
Financial Services	31	60%	€8.2B
Critical Infrastructure	14	27%	€4.1B
Healthcare	7	13%	€2.8B
Total	**52**	**100%**	**€5.9B avg**

3.2 Assessment Methodology

Each assessment involved:

- **Structured interviews** with CISO, CRO, and at least one board member (90-120 minutes each)
- **Document review** of board papers, risk registers, and security policies (past 24 months)
- **Gap analysis** against 47 control points derived from DORA Articles 5-27 and NIS2 Article 21
- **Maturity scoring** using a 5-level model (Initial → Repeatable → Defined → Managed → Optimising)

3.3 Limitations and Considerations

Readers should note the following limitations:

- **Geographic focus:** Sample limited to UK and EU organisations; findings may not generalise to other jurisdictions
- **Self-selection bias:** Organisations commissioning assessments may be more governance-mature than average

- **Confidentiality:** All findings anonymised; specific organisational details protected under NDA
- **Temporal scope:** Regulatory landscape evolving rapidly; findings reflect 2023-2025 conditions

📌 KEY TAKEAWAYS

→ 52 organisations assessed across financial services, critical infrastructure, and healthcare

→ Structured methodology aligned with DORA/NIS2 requirements ensures regulatory relevance

→ Geographic and self-selection limitations acknowledged for appropriate interpretation

4. 2024-2025 Case Studies: Governance Lessons

🎯 **STRATEGIC LENS:** *These cases from 2024-2025 demonstrate the material consequences of governance decisions—and provide the evidence base for CISO transformation.*

4.1 Snowflake Breach (2024): Cloud's Shared Responsibility Failure

🔴 **$370,000 RANSOM PAID | 165+ ORGANISATIONS COMPROMISED | 560M RECORDS EXPOSED**

Between April-May 2024, threat actor group UNC5537 systematically compromised 165+ organisations using stolen credentials—some dating back four years. Root cause: customer accounts using single-factor authentication. [17]

Impact: AT&T (110M customer records), Ticketmaster (560M records), Santander Bank (30M records), plus Advance Auto Parts, LendingTree, and Neiman Marcus. [17]

⚡ **GOVERNANCE DECISION POINT: Cloud Security Oversight**

- Was third-party cloud security on the board risk agenda?
- Did governance frameworks address shared responsibility models?
- Were MFA requirements contractually mandated for cloud providers?
- What oversight existed for credential lifecycle management?

Governance Lesson: The breach demonstrates that cloud security is a governance problem, not a technology problem. Organisations assumed their cloud provider handled security; Snowflake assumed customers would implement basic controls. Neither assumption held. Boards must explicitly govern shared responsibility boundaries. [18]

4.2 CrowdStrike Outage (July 2024): The $5.4 Billion Quality Failure

🔴 **$5.4 BILLION FORTUNE 500 LOSSES | 8.5 MILLION DEVICES CRASHED | 78-MINUTE DISASTER**

On July 19, 2024, a faulty configuration update crashed 8.5 million Windows devices worldwide within hours—the most expensive single-point technology failure in history. [19]

Sector	Estimated Losses
Healthcare	**$1.94 billion**

Banking	**$1.15 billion**
Airlines	**$860 million**
Global Total Estimate	**$10+ billion**

⚡ GOVERNANCE DECISION POINT: Vendor Concentration Risk

- Did the board have documented single-vendor concentration limits?
- Were contingency plans in place for critical security vendor failure?
- Did risk appetite statements address software update rollback capabilities?
- Was Delta Airlines' board informed of the lack of staged rollout protection?

Governance Lesson: Boards that had treated vendor concentration as an asset allocation decision (with documented risk limits and exit strategies) recovered faster. Those treating it as IT procurement faced extended outages. Delta Airlines filed suit claiming $500+ million in damages. [20]

4.3 Change Healthcare (2024): The Missing MFA

🔴 $22 MILLION RANSOM PAID | 190 MILLION RECORDS EXPOSED | 9-MONTH RECOVERY

A single compromised Citrix portal without MFA led to the largest healthcare breach in history, disrupting 40% of all U.S. medical claims. [21]

> *"This breach could have been stopped with cybersecurity 101. A Citrix portal without multi-factor authentication is a case study in crisis mismanagement."*
>
> **— Senator Ron Wyden, Congressional Testimony [22]**

⚡ GOVERNANCE DECISION POINT: Basic Security Control Oversight

- Who at board level owned MFA implementation decisions?
- What audit findings regarding legacy authentication were ignored?
- Did the board receive reports on critical system authentication status?
- Were exception processes for security control bypasses board-approved?

Governance Lesson: UnitedHealth CEO Andrew Witty testified to Congress that the compromised portal lacked multi-factor authentication. This basic control gap—a 'cybersecurity 101' failure—affected 190 million Americans. Boards must govern basic control implementation, not just policy approval. [21]

📌 KEY TAKEAWAYS

→ Snowflake: Cloud shared responsibility requires explicit board governance of control boundaries

→ CrowdStrike: Vendor concentration is a board-level asset allocation decision, not IT procurement

→ Change Healthcare: Basic control implementation must be board-governed, not just policy-approved

→ All three cases demonstrate: Governance decisions prevented—or enabled—catastrophic outcomes

5. Regulatory Framework: DORA, NIS2, and Personal Liability

🎯 **STRATEGIC LENS:** *Understanding the regulatory parameters of CISO accountability—just as treasury operations must comply with banking regulations.*

📅 REGULATORY TIMELINE

Oct 2024	Jan 2025	2026+
NIS2 Effective	DORA Applicable	Full Enforcement

⚖️ DORA ARTICLE 5 - MANAGEMENT BODY ACCOUNTABILITY

"The management body of the financial entity shall define, approve, oversee and be responsible for the implementation of all arrangements related to the ICT risk management framework."

— DORA Regulation (EU) 2022/2554, Article 5 [1]

🔴 NIS2 ARTICLE 20 - PERSONAL LIABILITY

"Member States shall ensure that members of the management bodies of essential and important entities can be held liable for infringements... including temporary bans from management positions." — NIS2 Directive (EU) 2022/2555, Article 20 [2]

Aspect	DORA	NIS2
Scope	21 types of financial entities	18 critical sectors
Personal Liability	**Up to €1,000,000**	**Management bans possible**
Entity Fine	2% global turnover + daily penalties	€10M or 2% turnover
Initial Alert	4 hours (max 24h)	24 hours
Board Training	Mandatory (Article 5(4))	Mandatory (Article 20(2))

6. CISO Personal Liability: The New Reality

🎯 **STRATEGIC LENS:** *Criminal prosecutions, SEC enforcement, and regulatory liability have transformed CISO accountability.*

6.1 Joe Sullivan (Uber) – Criminal Conviction

🔴 **FIRST CRIMINAL CONVICTION OF A SECURITY EXECUTIVE**

October 2022: Two felony charges—obstruction of FTC investigation and misprision of felony. Sullivan paid hackers $100,000 in Bitcoin disguised as bug bounty. Ninth Circuit upheld conviction October 2024. [3]

Sentence: 3 years probation, 200 hours community service, $50,000 fine. The court found Sullivan 'knew that the conduct in question was a felony.' [3]

6.2 The D&O Insurance Gap

🔴 **38% OF CISOs LACK D&O COVERAGE**

18% don't know their coverage status • 55% lack severance packages • Many corporate charters exclude CISOs from 'corporate officer' protection [10]

Response: Crum & Forster launched the first CISO-specific professional liability insurance in November 2024. 70% of CISOs say liability stories have negatively affected their opinion of the role. [23]

7. AI Governance and ISO 42001

🎯 **STRATEGIC LENS:** *AI governance represents the next frontier for CISO influence—with 48% of Fortune 100 boards now citing AI risk as a board oversight responsibility. [24]*

🤖 **ISO/IEC 42001:2023 - AI MANAGEMENT SYSTEMS**

The world's first international AI management system standard, providing a framework supporting compliance across multiple regulations. Specifies 39 controls covering AI policy, risk evaluation, system lifecycle management, and third-party oversight. [25]

7.1 EU AI Act Penalties

Prohibited AI practices banned as of February 2, 2025. Penalties effective August 2, 2025: [26]

- **Prohibited practices:** €35 million or 7% global turnover
- **Other obligations:** €15 million or 3% global turnover
- **Incorrect information:** €7.5 million or 1% global turnover

8. M&A Cyber Due Diligence

🎯 **STRATEGIC LENS:** *M&A cyber due diligence has evolved from technical assessment to board-level strategic concern. [27]*

- **60%** of firms in 2024 M&A transactions considered cybersecurity posture critical [27]
- **73%** of business leaders say an undisclosed security issue is a deal-breaker [27]
- **53%** of organisations have encountered cyber issues during M&A that jeopardized the deal [27]

Deal	Impact	Consequence
Verizon/Yahoo (2017)	**$350M price reduction**	Plus SEC fine [28]
Marriott/Starwood (2016)	**$90M+ fines**	20-year monitoring [29]

9. 90-Day Transformation Roadmap

🎯 **STRATEGIC LENS:** *A structured implementation plan for the Trust Value Flywheel™ in 90 days.*

PHASE 1: Foundation (Days 1-30)

- Conduct stakeholder mapping: identify board champions and executive sponsors
- Complete current-state assessment against DORA/NIS2 requirements
- Implement FAIR risk quantification methodology for board reporting
- Draft initial board dashboard with 12 KPIs (Section 10)

PHASE 2: Framework Build (Days 31-60)

- Deliver first board presentation using financial language
- Integrate cyber risk into enterprise risk management framework
- Establish cross-functional partnerships (CFO, General Counsel, Business Units)
- Document security as revenue enabler with case studies

PHASE 3: Operationalization (Days 61-90)

- Present transformation metrics and ROI to board
- Establish regular reporting cadence (quarterly minimum)
- Secure D&O insurance coverage and severance protection
- Document Trust Value Flywheel™ implementation progress

10. Board-Level Cyber Dashboard: 12 Essential KPIs

🎯 **STRATEGIC LENS:** *The measurement framework for cyber governance that translates technical metrics into business value.*

#	KPI	Description	Governance Value
1	**MTTD**	Mean Time to Detect incidents	Cost per hour of undetected breach
2	**MTTR**	Mean Time to Respond/Contain	Downtime costs, recovery expenses
3	**Risk $ at Risk**	FAIR-quantified financial exposure	Board-level risk communication
4	**Concentration**	Dependency on critical ICT providers	Exposure from provider failure
5	**Security ROI**	Return on security investment	Value creation demonstration
6	**Regulatory**	DORA/NIS2 compliance status	Enforcement risk exposure

11. Conclusion: From CISO to Chief Trust Officer

❌ Traditional CISO	✓ Chief Trust Officer
Protects systems	Protects confidence
Cost centre	**Capital creation**

> *"Are you positioned as a cost centre to minimise, or a trust engine to optimize? The Trust Value Flywheel™ provides the answer."*
>
> **— The CISO Transformation Playbook**

Appendix A: CISO Transformation Checklist

Transformation Item	Status
CEO/Board reporting structure established	□
FAIR risk quantification methodology implemented	□
12-KPI board dashboard deployed	□
DORA/NIS2 compliance documented	□
AI governance framework (ISO 42001) initiated	□
M&A cyber due diligence capability established	□
D&O insurance coverage secured	□
Trust Value Flywheel™ implementation tracking	□

About the Author

Kieran Upadrasta

CISSP, CISM, CRISC, CCSP | MBA | BEng

Kieran Upadrasta is a distinguished cyber security expert with 27 years of professional experience, including 21 years specializing in financial services and banking. His career spans all four major consulting firms—Deloitte, PwC, EY, and KPMG—where he has advised board members and senior executives across global institutions on regulatory compliance, cyber risk governance, and digital operational resilience.

Professional Memberships & Leadership Positions

- Honorary Senior Lecturer
- Lead Auditor, ISF Auditors and Control
- Platinum Member, ISACA London Chapter
- Gold Member, ISC² London Chapter
- Cyber Security Programme Lead, PRMIA
- Researcher, University College London (UCL)

—

Contact: info@kieranupadrasta.com

Website: www.kie.ie

LinkedIn: linkedin.com/in/kieranupadrasta

References

[1] European Union, "Regulation (EU) 2022/2554 on Digital Operational Resilience (DORA)," Official Journal of the European Union, 2022.

[2] European Union, "Directive (EU) 2022/2555 (NIS2)," Official Journal of the European Union, 2022.

[3] U.S. v. Sullivan, No. 20-CR-00337, N.D. Cal., Oct. 2022; Ninth Circuit Appeal, Oct. 2024.

[4] SEC, "Enforcement Actions: Cybersecurity Disclosure Violations," SEC.gov, 2024.

[5] Heidrick & Struggles, "2024 Global Chief Information Security Officer Survey," 2024.

[6] PwC, "2025 Global Digital Trust Insights," PwC.com, Jan. 2025.

[7] IANS Research & Artico Search, "2024 CISO Compensation and Budget Study," 2024.

[8] Verizon, "2024 Data Breach Investigations Report," Verizon Enterprise, 2024.

[9] Mimecast, "State of Email & Collaboration Security Report," 2024.

[10] Hitch Partners, "CISO Survey: Personal Liability and Insurance Coverage," 2024.

[11] IBM/Ponemon Institute, "Cost of a Data Breach Report 2024," IBM Security, 2024.

[12] SecurityScorecard, "Global Third-Party Cyber Breach Report," 2024.

[13] Vendict, "2024 CISO Burnout Study," Vendict Research, 2024.

[14] Accenture, "State of Cybersecurity Resilience 2025," Accenture Security, 2025.

[15] Upadrasta, K., "The Trust Value Flywheel: Board-Level Cyber Governance," 2025.

[16] IBM Institute for Business Value, "Cybersecurity as Revenue Enabler," 2024.

[17] Mandiant, "UNC5537 Targets Snowflake Customer Instances," Google Cloud, Jun. 2024.

[18] Snowflake, "Security Advisory: Customer Account Compromise," Jun. 2024.

[19] Parametrix, "CrowdStrike IT Outage: Fortune 500 Impact Assessment," Jul. 2024.

[20] Delta Air Lines, "Statement on CrowdStrike Outage Litigation," Aug. 2024.

[21] UnitedHealth Group, "Change Healthcare Cyber Incident: Congressional Testimony," May 2024.

[22] U.S. Senate Finance Committee, "Hearing: UnitedHealth CEO Testimony," May 2024.

[23] Crum & Forster, "CISO Professional Liability Insurance Launch," Nov. 2024.

[24] Gartner, "2024 Board Survey: AI Governance Priorities," Gartner Research, 2024.

[25] ISO, "ISO/IEC 42001:2023 AI Management Systems," ISO.org, 2023.

[26] European Union, "Regulation (EU) 2024/1689 (EU AI Act)," Official Journal, 2024.

[27] Forescout, "2024 M&A Cybersecurity Due Diligence Report," 2024.

[28] SEC, "Altaba (Yahoo) Settlement," SEC.gov, 2018.

[29] ICO, "Marriott International Penalty Notice," ICO.org.uk, 2020.

This whitepaper is intended for informational purposes and does not constitute legal advice.