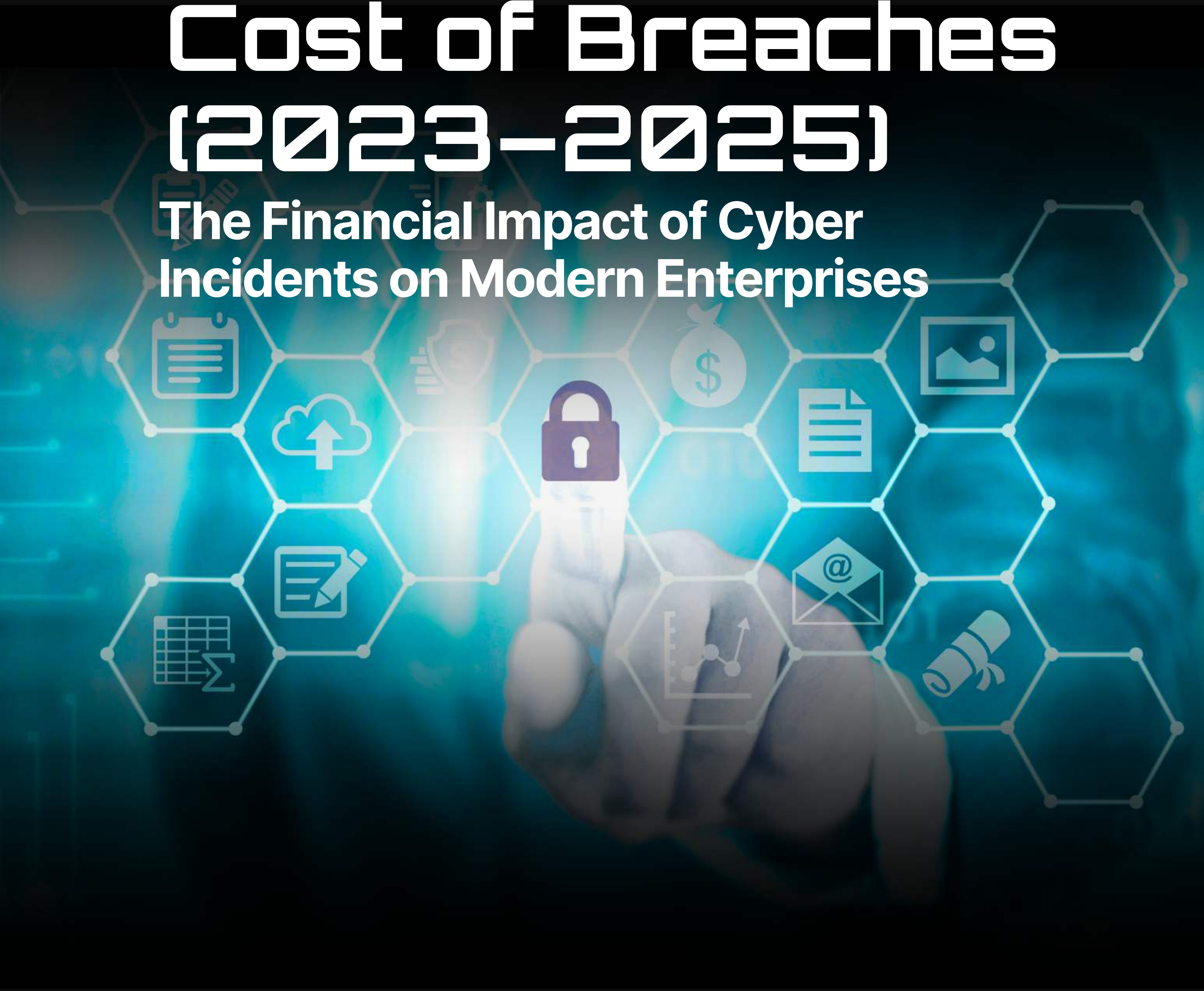
The Business Cost of Breaches (2023-2025)

The Financial Impact of Cyber Incidents on Modern Enterprises



TRESCUDO

Table Of Contents

The Business Cost of Breaches (2023–2025)

A CISO's Report to the Board on Why Cyber Resilience Is a Competitive Advantage

Trescudo | July 2025

1. Executive Summary

Cyber incidents are no longer rare "black swan" events—they are budget-line inevitabilities. From 2023 to 2025, the average global cost of a data breach has climbed to ~USD 4.8–5.0M (1), with lifecycles still hovering around 250+ days from identification to full containment(1). Ransomware and supply-chain compromises continue to deliver outsized financial shocks(2), while regulatory exposure under NIS2, GDPR, and sectoral rules like DORA raises the stakes for non-compliance(3).

Three board-level truths:

1. ***Time is money:*** *Every day shaved off Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) meaningfully reduces loss—often by* ***USD 1M+*** *per incident.(1)*
2. ***Framework-driven maturity pays for itself:*** *Organizations with mature controls (Zero Trust, security AI/automation, continuous monitoring) save* ***millions per breach*** *and bounce back faster*(1)(4)*.*
3. ***Regulatory fines are only the tip of the iceberg:*** *NIS2's penalties (up to 2% global turnover) are dwarfed by indirect costs—lost business, churn, and reputational damage.(3)*

Ask the Board: Approve a 24-month cyber resilience investment program focused on: accelerated detection/response, Zero Trust segmentation, supply-chain assurance, and continuous compliance automation. The modeled ROI surpasses 100% over three years.(4)

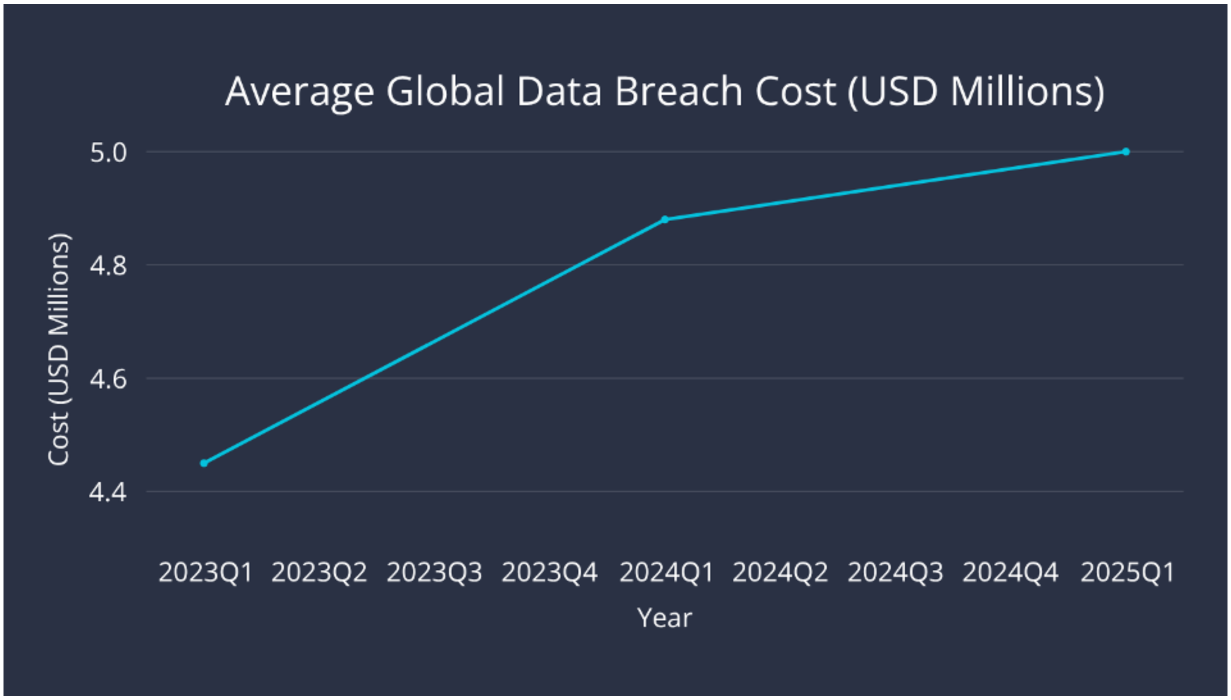
2. Current Threat & Cost Landscape (2023–2025)

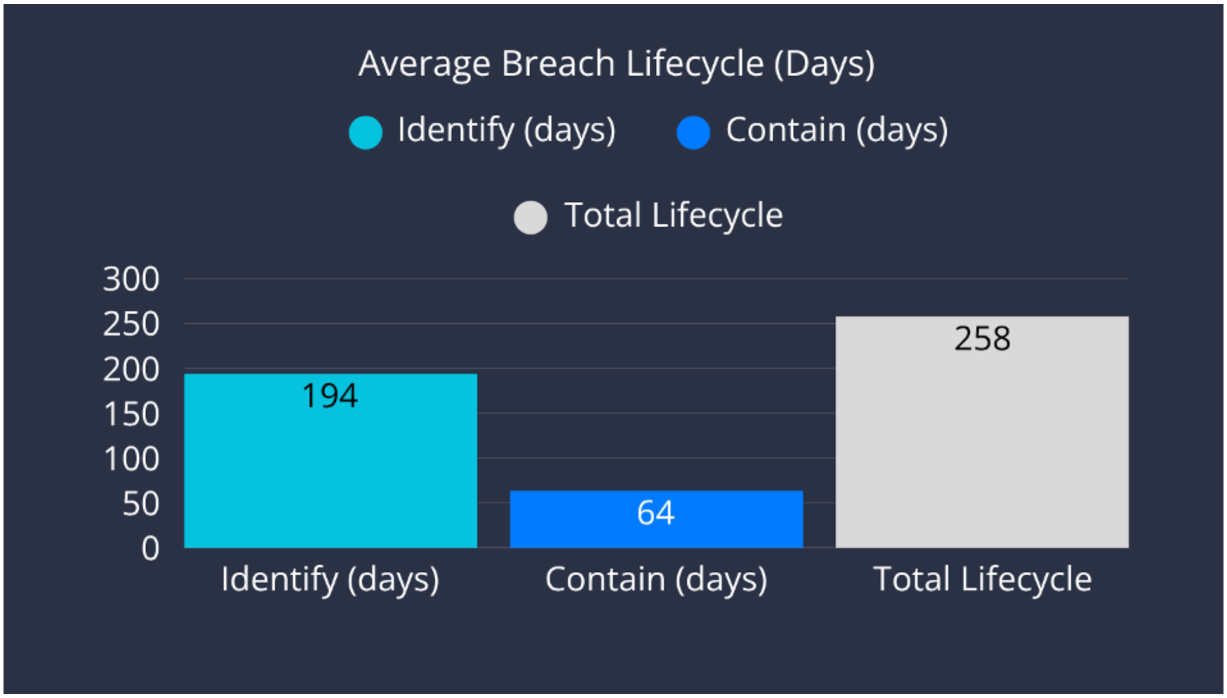
Key Metrics at a Glance

- ***Avg. total breach cost:*** *~USD 4.8–5.0M (10% YoY rise since 2023)(1)*
- ***Cost per compromised record:*** *~USD 160–175 (higher for IP and PHI)(1)*
- ***Lifecycle:*** *~190 days to identify + ~65 days to contain (≈ 255 total)(1)*
- ***Top cost components:*** *Lost business (downtime, churn) and post-breach response*1
- ***Savings levers:*** *Security AI/automation (≈40% cost reduction)*1*, IR planning/testing, Zero Trust*4

Macro Trends

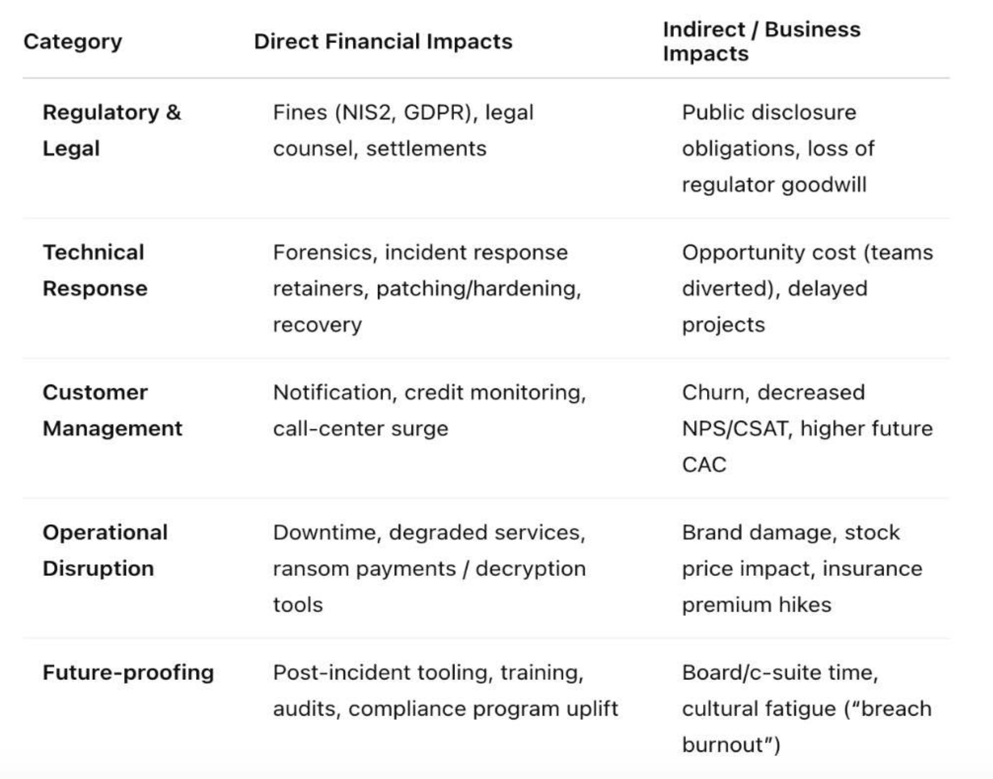
- ***Attack velocity:*** *Ransomware payouts up sharply; data exfiltration often precedes encryption.(2)*
- ***Supply-chain blast radius:*** *Third-party and managed file transfer flaws (e.g., MOVEit) amplify exposure.(2)*
- ***Credential-driven breaches:*** *Still the longest to detect; identity-centric controls remain underfunded.(1)*


Average Global Data Breach Cost (USD Millions)
Cost (USD Millions)
5.0
4.8
4.6
4.4
2023Q1
2023Q2
2023Q3
2023Q4
2024Q1
2024Q2
2024Q3
2024Q4
2025Q1
Year

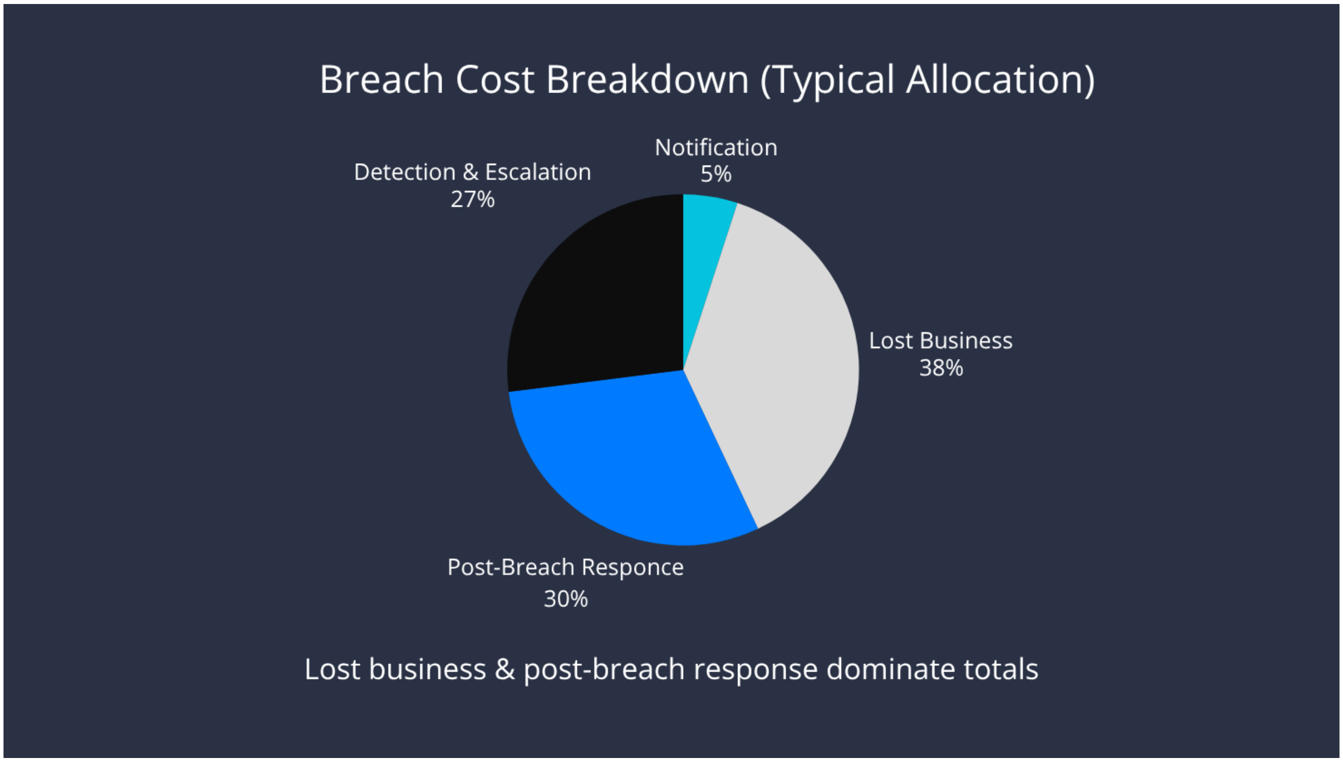

Average Breach Lifecycle (Days)
● Identify (days)
● Contain (days)
● Total Lifecycle
300
250
200
150
100
50
0
194
64
258
Identify (days)
Contain (days)
Total Lifecycle

3. Anatomy of a Breach: Direct vs. Indirect Costs

Insight: Indirect costs often outstrip direct ones, particularly in B2C sectors where trust is the primary currency.



Category	Direct Financial Impacts	Indirect / Business Impacts
Regulatory & Legal	Fines (NIS2, GDPR), legal counsel, settlements	Public disclosure obligations, loss of regulator goodwill
Technical Response	Forensics, incident response retainers, patching/hardening, recovery	Opportunity cost (teams diverted), delayed projects
Customer Management	Notification, credit monitoring, call-center surge	Churn, decreased NPS/CSAT, higher future CAC
Operational Disruption	Downtime, degraded services, ransom payments / decryption tools	Brand damage, stock price impact, insurance premium hikes
Future-proofing	Post-incident tooling, training, audits, compliance program uplift	Board/c-suite time, cultural fatigue (“breach burnout”)



Breach Cost Breakdown (Typical Allocation)

Lost business & post-breach response dominate totals

4. Regulatory Exposure: NIS2, GDPR, DORA (EU Focus)

NIS2 Directive (Effective October 2024 EU-wide)

Penalties at a Glance

Entity Type	Max Fine (Euro)	Turnover % Cap
Essential	10, 000, 000	2%
Important	7, 000, 000	1.4%

Scope & fines defined in Directive (EU) 2022/2555

GDPR

- *Fines up to €20M or 4% global turnover (Regulation (EU) 2016/679)(3)*
- 72-hour breach notification requirement.

DORA (Financial Sector)

- *Regulation (EU) 2022/2554 mandates ICT risk management & testing for finance(3)*
- ***Fines:*** *Up to* ***€20M or 4%*** *of global annual turnover. Breach notification within 72 hours; failure escalates penalties.*
- ***Focus:*** *Lawful processing, data minimization, privacy by design.*

- ***Goal:*** *Operational resilience for financial entities and critical ICT providers.*
- ***Requirements:*** *Rigorous testing, incident classification/reporting, third-party risk oversight.*
- ***Penalties:*** *National competent authorities empowered to levy significant fines and impose remediation.*

Board takeaway: Regulatory risk is quantifiable and sizable—but often still smaller than the strategic damage of eroded trust.

5. Threat Vector Economics

Ransomware

- ***Avg. recovery cost (excl. ransom):*** *~USD 2.5–3.0M*
- ***Avg. ransom payment (2024/25):*** *~USD 1.5M, but "double extortion" (data theft + encryption) inflates total.*
- ***Key mitigations:*** *Immutable backups, segmentation, rapid IR playbooks, tabletop exercises.*

Business Email Compromise (BEC)

- ***Losses:*** *Multi-billion annually (largest single-category loss per FBI IC3)*
- ***Mechanism:*** *Social engineering + payment redirection; low-tech but high-return for attackers.*
- ***Key mitigations:*** *Out-of-band payment verification, DMARC/SPF/DKIM, user awareness ("Human Perimeter").*

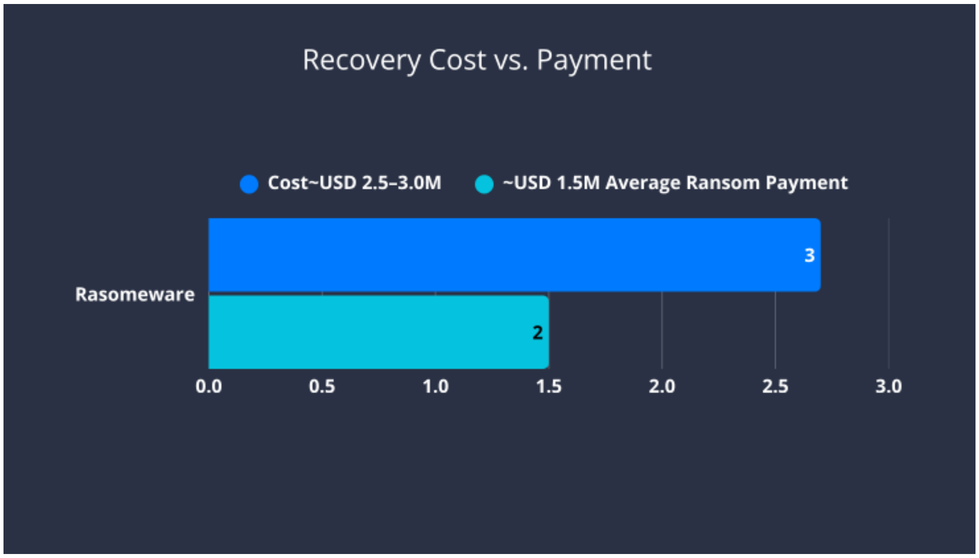
Supply-Chain / Third-Party Attacks

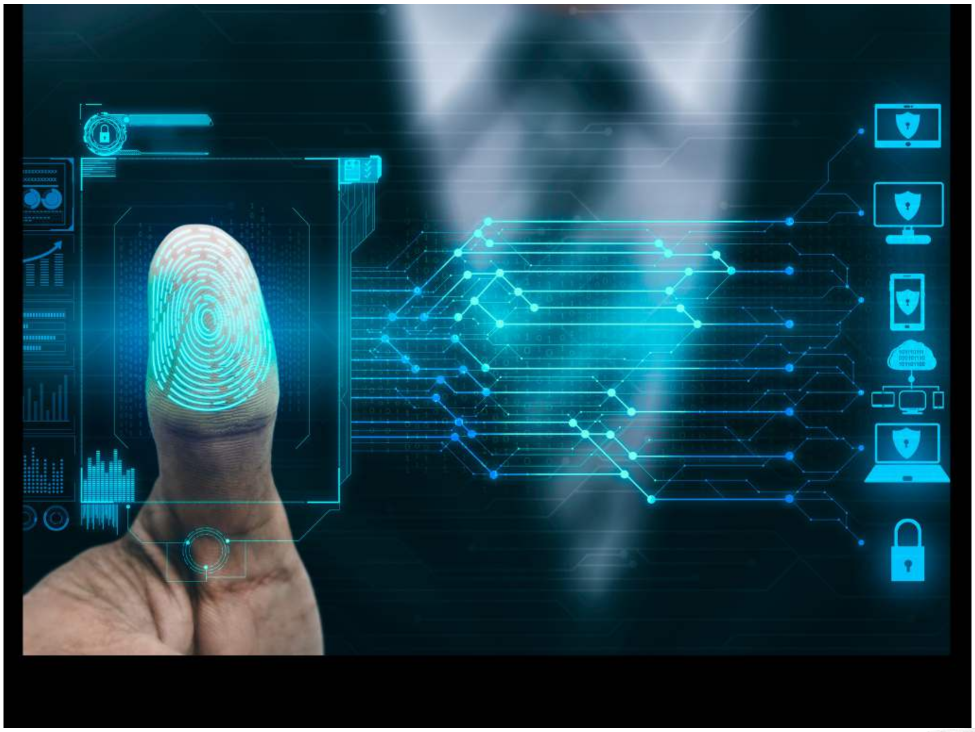
- ***Impact:*** *Cascading effects—single exploited vendor → thousands of downstream breaches (MOVEit, SolarWinds)*
- ***Projected 2025 costs:*** *USD ~60B globally (steep climb expected into 2030s)*
- ***Key mitigations:*** *Vendor risk scoring, SBOM requirements, contract clauses, continuous monitoring.*

Credential & Identity Attacks

- ***Longest dwell times:*** *>290 days to detect/contain on average*
- ***Key mitigations:*** *Zero Trust identity, MFA everywhere (including admins/service accts), continuous authentication.*

The Business Cost of Breaches (2023–2025)

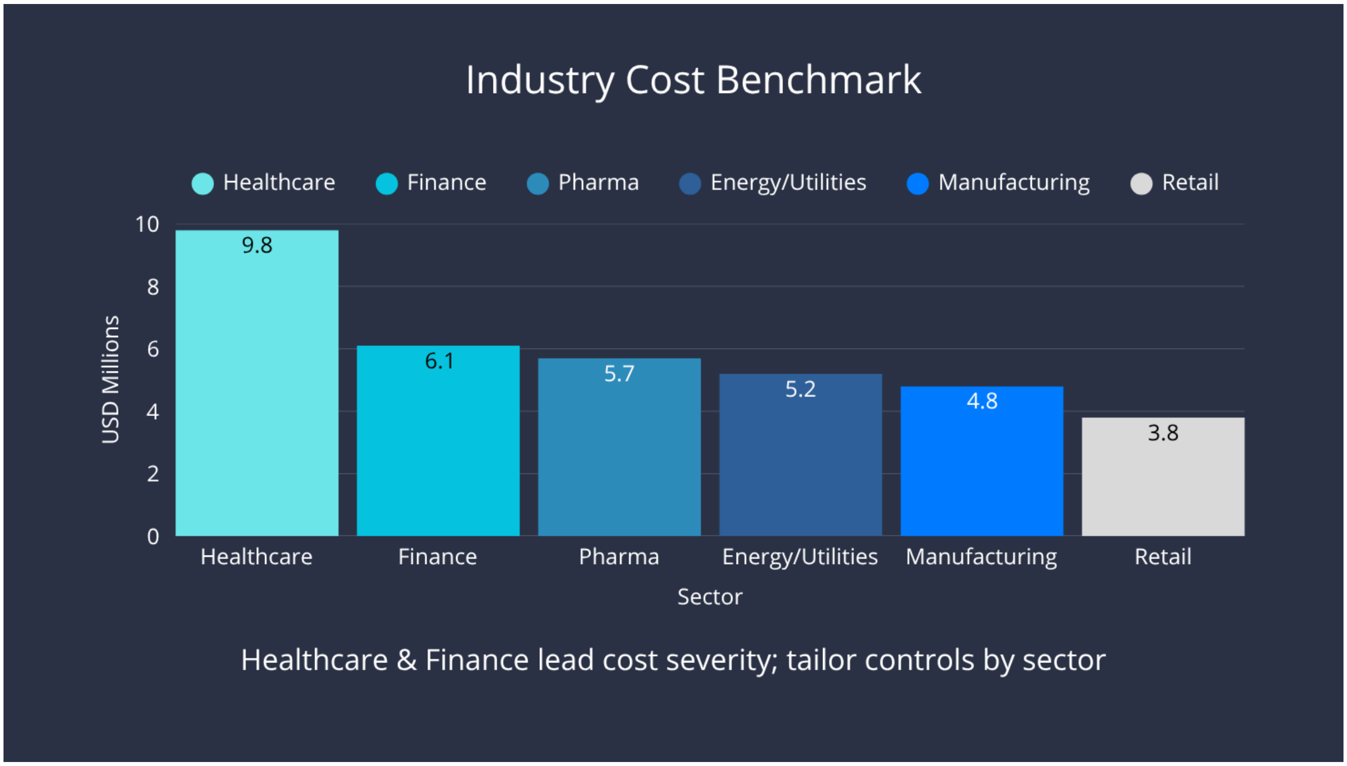




6. Sector Benchmarks (Avg. Breach Cost)

Industry	Notable Drivers	Avg. Cost (USD)
Healthcare	PHI sensitivity, complex legacy systems, regulatory fines	~9.5–10.0M
Finance	High-value data, stringent regulatory requirements	~6.0–6.5M
Pharmaceuticals	IP theft risk, long R&D cycles	~5.5–6.0M
Energy/Utilities	OT/IT convergence, critical infrastructure implications	~5.0–5.5M
Manufacturing	Supply-chain dependencies, downtime cost	~4.5–5.0M
Retail	Card data exposure, seasonal peaks	~3.5–4.0M

Use these benchmarks to personalize risk narratives when engaging BU leaders.



Industry Cost Benchmark

Healthcare & Finance lead cost severity; tailor controls by sector

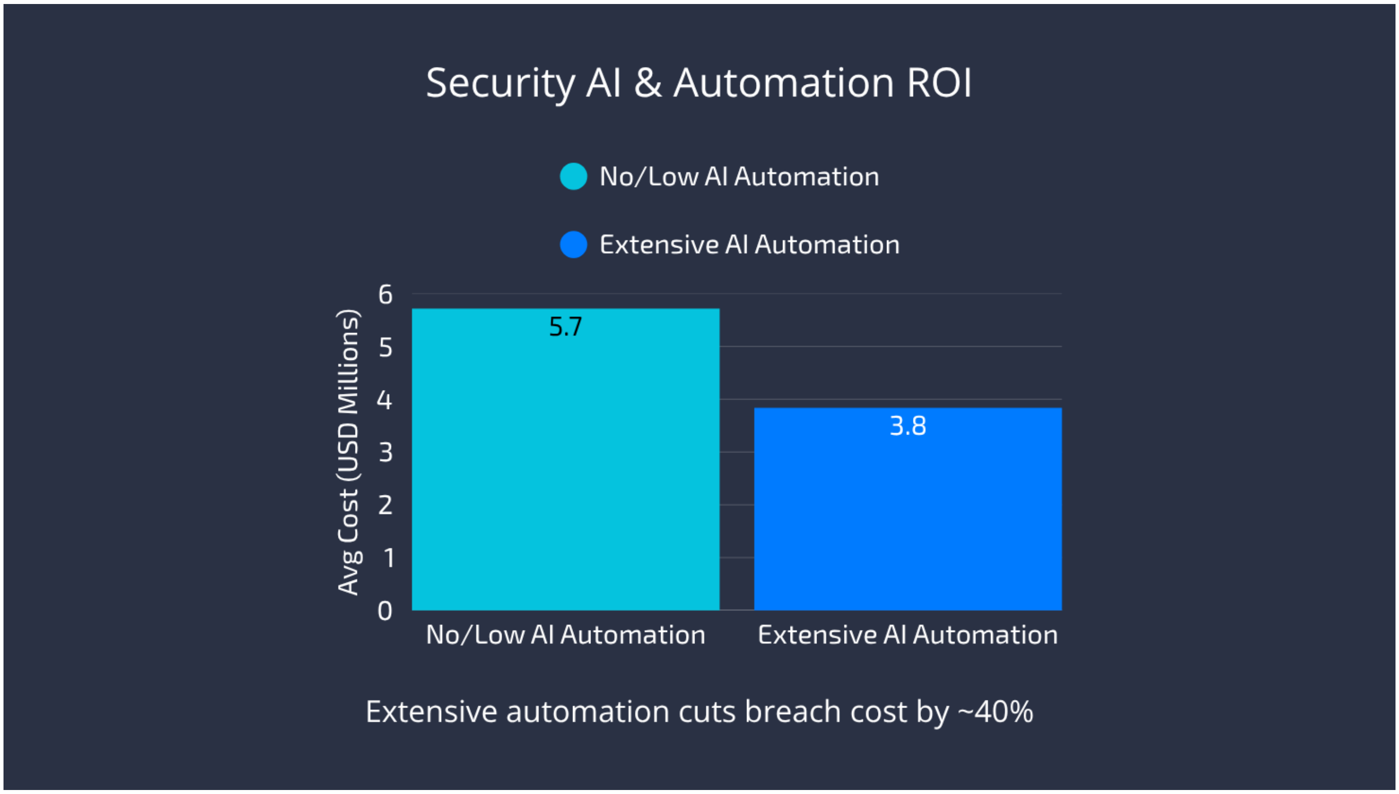
7. The ROI of Proactive Security

Proven Savings Levers

- ***Security AI & Automation:*** *Avg. ~USD 2.2M saved per breach(1)*
- ***Zero Trust & Segmentation:*** *111% ROI (Forrester TEI, Illumio) and multi-million savings in TEI studies for major platforms(4)*
- ***IR Readiness:*** *Regularly tested plans save ~USD 1.3M per incident(1)*
- ***DevSecOps:*** *Early fixes 10–30x cheaper than post-production remediation(5)*
- ***Security AI & Automation:*** *Avg.* ***~USD 2.2M saved per breach****; faster MTTD/MTTR.*
- ***Zero Trust & Segmentation:*** *Independent TEI (Total Economic Impact) studies show* ***100%+ ROI*** *over 3 years, driven by reduced breach scope and compliance efficiency.*
- ***IR Readiness (Tabletops, Playbooks):*** *Organizations that regularly test IR plans save* ***~USD 1.3M*** *on average per incident.*
- ***DevSecOps & Shift-Left Security:*** *Early vulnerability catch reduces remediation cost by 10–30x vs. post-production fixes.*

Value Articulation to Finance

- ***Cost Avoidance:*** *"Every avoided breach = ~$5M saved" (plus reputational shield).*
- ***Operational Uptime:*** *Cyber resilience protects revenue continuity—model the daily revenue at risk.*
- ***Insurance Synergy:*** *Mature controls lower cyber insurance premiums and deductibles.*


Security AI & Automation ROI
● No/Low AI Automation
● Extensive AI Automation
Avg Cost (USD Millions)
6
5
4
3
2
1
0
5.7
3.8
No/Low AI Automation
Extensive AI Automation
Extensive automation cuts breach cost by ~40%

8. Strategic Roadmap (24 Months)

Phase 1: Stabilize & See (0–6 Months)

- Deploy continuous monitoring & EDR/XDR across critical assets
- Stand up a formalized IR function (SLAs, playbooks, comms plans)
- Quick wins: MFA enforcement, privileged access hardening, backup validation

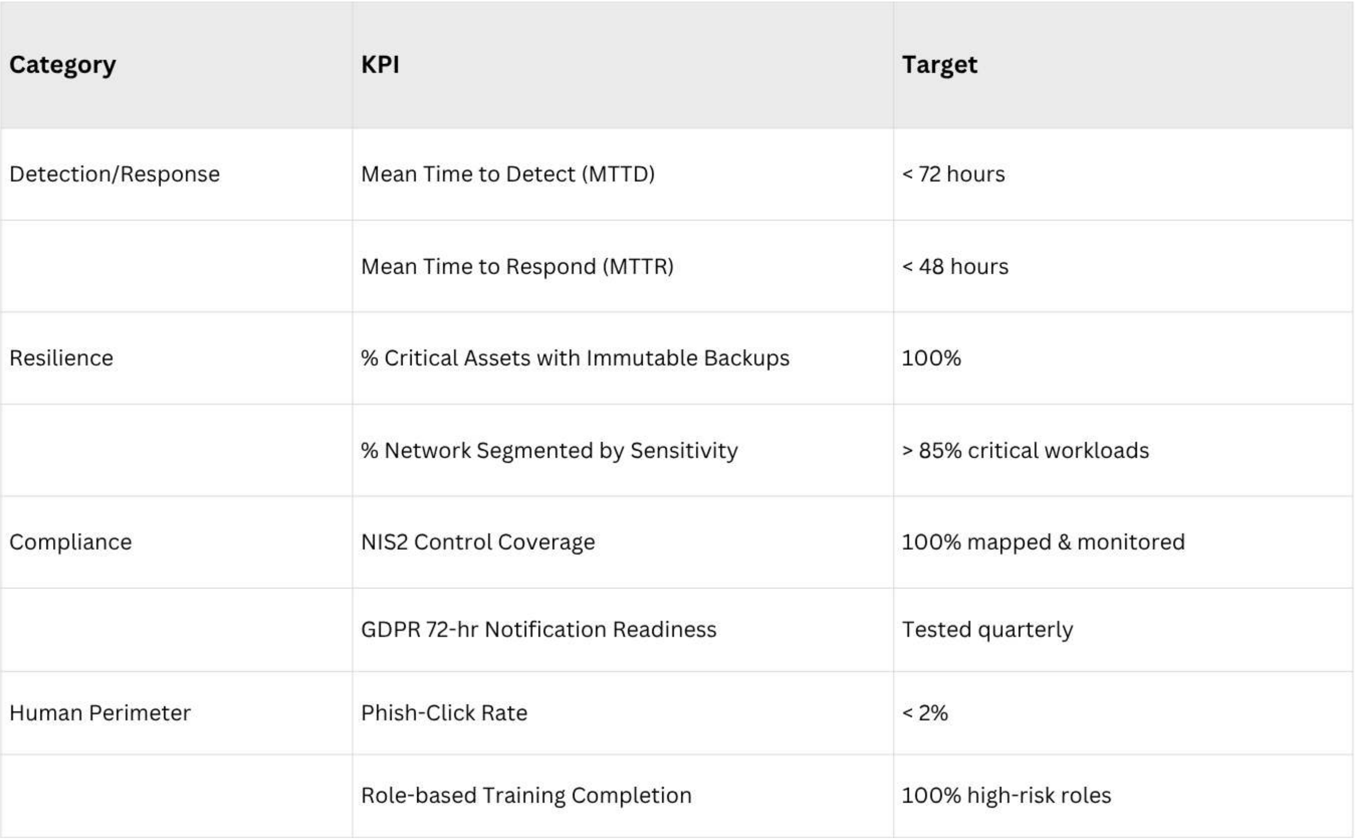
Phase 2: Segment & Automate (6–18 Months)

- Implement Zero Trust segmentation (network & workload level)
- Automate detection & response with SOAR/SIEM enhancements
- Roll out security awareness focused on the Human Perimeter (role-based training)
- Third-party risk program: SBOMs, continuous vendor scans

Phase 3: Optimize & Govern (18–24 Months)

- Continuous compliance automation (NIS2, ISO 27001 mapping)
- Red-team/purple-team exercises; chaos engineering for cyber
- KPI dashboarding to executives (MTTD, MTTR, patch cadence, % assets segmented)

9. KPIs & Board Dashboards



Category	KPI	Target
Detection/Response	Mean Time to Detect (MTTD)	< 72 hours
	Mean Time to Respond (MTTR)	< 48 hours
Resilience	% Critical Assets with Immutable Backups	100%
	% Network Segmented by Sensitivity	> 85% critical workloads
Compliance	NIS2 Control Coverage	100% mapped & monitored
	GDPR 72-hr Notification Readiness	Tested quarterly
Human Perimeter	Phish-Click Rate	< 2%
	Role-based Training Completion	100% high-risk roles

10. Appendix

A. Data Sources

1. ***IBM Security & Ponemon Institute*** – *Cost of a Data Breach Reports 2023, 2024, 2025 (https://www.ibm.com/security/data-breach)*
2. ***FBI IC3 / Coveware / Sophos / Progress Software / ENISA / Mandiant / CrowdStrike*** – *Threat vector economics, ransomware, BEC, supply-chain (https://www.ic3.gov), (https://www.coveware.com), (https://www.sophos.com/en-us/content/state-of-ransomware), (https://www.progress.com/moveit), (https://www.enisa.europa.eu), (https://www.mandiant.com), (https://www.crowdstrike.com)*
3. ***EU Regulations*** – *NIS2 Directive (EU) 2022/2555, GDPR (EU) 2016/679, DORA (EU) 2022/2554 (https://eur-lex.europa.eu)*
4. ***Forrester / IDC / Gartner TEI & ROI Studies*** – *Zero Trust & automation ROI (https://www.forrester.com/tei)*
5. ***NIST CSF 2.0*** – *Framework for Improving Critical Infrastructure Cybersecurity (https://www.nist.gov/cyberframework)*

6. ***Politico Europe / AP News / Reuters / Computing.co.uk / HackRead / CPO Magazine*** *– ICC cyberattack & major breach coverage (e.g.,*https://www.politico.eu/article/icc-hit-by-cyberattack-around-nato-summit/*)*
7. ***CISA & ITPro*** *– Microsoft SharePoint CVE-2025-53770 alerts & guidance (*https://www.cisa.gov*), (*https://www.itpro.com/security/microsofts-new-sharepoint-vulnerability-everything-you-need-to-know*)*
8. ***The New Arab*** *– Pentagon Pizza Meter article (*https://www.newarab.com/news/what-pentagon-pizza-meter-and-can-it-predict-wars*)*
9. ***Verizon DBIR 2024*** *– Breach patterns & dwell time (*https://www.verizon.com/business/resources/reports/dbir/*)*
10. ***ISO/IEC 27001:2022*** *– Information security management systems standard (*https://www.iso.org/standard/82875.html*)*

B. Glossary

- ***MTTD/MTTR:*** *Mean Time to Detect/Recover*
- ***TEI:*** *Total Economic Impact (Forrester methodology)*
- ***SBOM:*** *Software Bill of Materials*
- ***Human Perimeter:*** *The people-centric boundary where social engineering, insider risk, and process lapses occur*

About the Expert

Marçal Santos, CISM, CDPSE

Virtual CISO & Security Compliance Strategist

With more than 20 years in cybersecurity—ranging from Information Security Officer in the early 2000s to leading security programmes for fast-growing SaaS providers—Marçal Santos specialises in turning security hurdles into competitive strengths.

- **Virtual CISO for SMBs & Mid-Market:** Guides executive teams in Europe and North America through pragmatic, framework-driven roadmaps that win enterprise deals and satisfy auditors.
- **Compliance Authority:** Has led several successful SOC 2 Type II, ISO 27001 and GDPR readiness projects, helping companies reduce sales friction and accelerate time-to-market.
- **Chief Information Security Officer Ratchet Capital:** Built a zero-trust architecture that slashed Mean Time to Detect by 60 %.
- **Trusted Advisor:** Frequently quoted in industry panels and podcasts on supply-chain risk and the "Human Perimeter."
- **Community Mentor:** Shares weekly #CyberCareerTips with 3 000+ LinkedIn followers, advocating for diversity and skill-building in InfoSec.

Marçal architected the strategic modelling and ROI analysis that underpin this report.

Closing Statement

Resilience is strategy. Cybersecurity spend is not a sunk cost—it's an investment in uninterrupted revenue, regulatory peace of mind, and brand credibility. By quantifying both the downside risk and the upside ROI, we shift the conversation from fear to value. Trescudo stands ready to help execute this roadmap with precision and measurable outcomes.

Prepared by the Trescudo Research Team under the guidance of in-house subject-matter expert Marçal Santos.

TRESCUDO

The Business Cost of Breaches (2023-2025)

In "The Business Cost of Breaches (2023–2025)," Trescudo reveals that cyber incidents have evolved into unavoidable financial burdens, with data breach costs averaging USD 4.8–5.0 million and significant indirect damages often surpassing direct expenses. This essential report advocates for a robust 24-month cyber resilience investment strategy, emphasizing that proactive security measures not only reduce breach-related losses but also yield substantial ROI. By illustrating the critical importance of time, mature controls, and regulatory compliance, this report empowers boards to recognize cybersecurity as a strategic advantage rather than an expense.

TRESCUDO