Cyber Resilience as a Business Priority

Why boards, CXOs, and investors can no longer treat cybersecurity as an IT problem

The global economy runs on digital infrastructure and that infrastructure is under siege. Ransomware, supply-chain attacks, nation-state intrusions, and insider threats are no longer hypothetical. They are daily realities that have toppled market caps, halted production lines, and destroyed customer trust overnight. Cyber resilience —the ability not just to defend but to withstand, adapt, and recover from attacks, has become the defining operational and reputational challenge of this decade.

$10.5T	$4.44M	241 days	30%
Global cybercrime cost, 2025 *Cybersecurity Ventures [1]*	Avg. data breach cost, 2025 *IBM Cost of a Data Breach [2]*	Avg. breach lifecycle, 2025 (9-yr low) *IBM Cost of a Data Breach [2]*	Third-party breaches, 2025 *Verizon DBIR 2025 [3]*

THE GLOBAL STORY

Cyber threats have moved from the periphery of corporate risk registers to the very top. The WEF Global Cybersecurity Outlook 2025 found that 72% of organisations reported a rise in cyber risks over the past year, with geopolitical tensions influencing cybersecurity strategy in nearly 60% of organisations.[4]

Four structural shifts are driving this elevation.

01. Scale & Sophistication — Ransomware

Ransomware-as-a-Service has lowered the barrier to entry for organised criminal groups

44%	$115K	64%
of confirmed breaches involved ransomware (2025) *↑ up from 32% in 2024*	median ransom payment in 2024	of victims refused to pay *Highest refusal rate on record*

02. Expanding Attack Surface — The Rise of AI

Cloud, IoT, remote work & APIs have exponentially enlarged potential entry points

1 in 6	Phishing	20%
breaches globally used attacker AI tools (2025)	& deepfake impersonation — most common AI tactics	of breaches involved Shadow AI — adding avg. $670K to costs

03. Supply Chain Risk Has Doubled

Third-party involvement saw the steepest single-year jump in Verizon's DBIR history

Third-party breach involvement:

15% — 2024

30% — 2025 ↑ DOUBLED

Case study: The Snowflake breach cascaded across AT&T, Ticketmaster, and thousands of organisations simultaneously — a single vendor vulnerability with industry-wide impact.

04. Regulatory & Liability Pressure

Governments have moved from voluntary guidance to binding obligations with personal liability

EU NIS2 Directive Effective October 2024. Senior executives are personally liable for cybersecurity failures in their organisations.	**US SEC Rule** Public companies must disclose material cyber incidents within four business days of discovery.
Singapore, Australia & UK Parallel binding frameworks issued — creating a global web of mandatory cyber obligations.	**The bottom line** Legal and reputational consequences of inaction have never been higher.

> *Cyber resilience today is as much a boardroom and legal concern as it is a technology challenge — and regulators worldwide are beginning to hold executives personally accountable for failures.*

THE INDIA STORY

India presents a paradox: it is simultaneously one of the world's fastest-growing digital economies and one of the most targeted by cyber adversaries. Indian organisations faced an average of **2,011 cyberattacks per week in 2025** — nearly double the global average — according to Check Point Software's State of Cyber Security in India 2025 report[5]

Metric	India Snapshot (2025)
Avg. weekly attacks per org	~2,011 [5]
Most targeted sectors	Education, Government, Telecom, BFSI, Healthcare[5]
Cyber fraud losses (NCRP)	₹36,450 crore reported as of Feb 2025[5]
Total cyber incidents (2024)	~2.27 million (up from 1.03M in 2022)[5]
Cybersecurity market (2026)	~USD 6.56 billion, growing at 18% CAGR[6]

India's Digital Public Infrastructure — UPI, Aadhaar, DigiYatra, ONDC, and the Account Aggregator framework — has made the country a global exemplar of state-led digitisation. But scale brings exposure. Cyber incidents in India more than doubled between 2022 and 2024.[5] Financial cyber fraud losses reported on the National Cyber Crime Reporting Portal reached ₹36,450 crore as of February 2025, largely driven by phishing-led UPI fraud, AI-assisted social engineering, and deepfake-enabled scams.[5]

Regulatory Momentum

India has accelerated its cyber governance architecture significantly. The Digital Personal Data Protection Act (DPDPA), 2023, introduces data breach notification obligations and significant financial penalties for non-compliance. SEBI mandates cybersecurity frameworks for market infrastructure institutions and listed companies. RBI's Master Direction on IT Governance compels banks and NBFCs to implement board-level oversight of cyber risks. CERT-In's six-hour breach reporting directive for covered entities marked a pivotal shift in regulatory posture.

> *India's IT and ITES sector — serving clients across 80+ countries — faces a compounded risk: a breach does not just impact domestic operations; it can expose global clients and trigger multi-jurisdictional regulatory consequences.*

KEY RISKS

Cyber risks vary by sector and maturity, but five categories consistently emerge as the most consequential for business leaders.

Risk Category	Business Impact	Severity (Global)
Ransomware	Operational shutdown, data destruction, ransom payments, regulatory fines — present in 44% of 2025 breaches (Verizon DBIR)	**Critical**
Supply Chain Attacks	Third-party compromise cascades across clients; third-party involvement doubled to 30% of all breaches in 2025 (Verizon DBIR)	**Critical**
AI-Enabled Attacks	AI used in 1-in-6 breaches in 2025 for phishing and deepfakes; shadow AI added $670K to average breach costs (IBM)	**High**
Data Breaches	Regulatory penalties (DPDPA, GDPR), litigation, customer churn — avg. cost $4.44M globally in 2025 (IBM)	**Critical**
Cloud Misconfigurations	Exposed databases and APIs; a key driver of India-specific breaches per Check Point India 2025 report	**High**

OPPORTUNITIES

The urgency of cyber risk is simultaneously generating a significant economic and strategic opportunity. Organisations that invest in cyber resilience early are not just buying protection — they are building a competitive differentiator.

Market Opportunity: The Cybersecurity Industry

Global information security spending hit $211.6 billion in 2025 — a 15.1% year-on-year increase. [7] In India, the cybersecurity market is valued at approximately USD 6.56 billion in 2026, growing at an 18% CAGR.[6] Indian MSSPs and cybersecurity product companies are gaining traction in global markets, building on the country's deep IT services talent base.

Strategic Opportunities for Enterprises

- **Cyber Resilience as a Trust Signal** — organisations that can credibly demonstrate security posture win contracts and retain enterprise clients, especially in regulated sectors.
- **Insurance and Capital Cost Advantages** — cyber-mature companies attract lower premiums and, increasingly, better terms from institutional investors who factor cyber risk into ESG assessments.
- **AI-powered Security Operations** — organisations using AI extensively in their security operations saved an average $1.9 million per breach and reduced the breach lifecycle by 80 days in 2025.
- **Zero Trust Architecture Adoption** — a shift from perimeter-based to identity-and-access-centric security models is creating both a technology refresh cycle and consulting demand.

- **Global Gap:** Talent and skilling ecosystems — the global shortfall of over 4 million cybersecurity professionals (ISC2, 2024) represents a significant opportunity for Indian training institutions and staffing providers. [8]
- **Workforce and Culture as a Competitive Edge** — organisations that embed security awareness into everyday culture — through regular training, phishing simulations, and clear incident reporting norms — reduce human-error-driven breaches significantly.
- **Incident Response Maturity Reduces Business Disruption** — organisations with tested, well-rehearsed incident response plans contain breaches faster, limit regulatory exposure, and resume normal operations with far less reputational damage.

For Technology Companies

Build security-by-design into product development. Obtain recognised certifications (ISO 27001, SOC 2 Type II). Monetise security posture as a go-to-market advantage in enterprise and government segments. Address shadow AI risk with formal AI governance policies.

For Traditional Enterprises

Treat cyber resilience as a board-level agenda item. Invest in CISO-level leadership, incident response planning, and third-party risk management. Move beyond compliance checkboxes to continuous risk assessment and AI governance.

> *Cyber resilience is not a destination — it is an operating posture. The question for business leaders is not whether their organisation will face a serious cyber incident, but whether they will have the architecture, governance, and culture to absorb the impact and recover faster than the competition.*

FUTURE OUTLOOK

The cybersecurity landscape over the next three to five years will be shaped by two dominant forces: the offensive use of AI by threat actors, and the defensive use of AI by security practitioners. Whoever deploys AI more effectively will hold the advantage — and right now, that race is far from decided.

- ### AI as Both Threat and Shield

  Generative AI has dramatically lowered the cost of sophisticated phishing, social engineering, and malware creation. 1 in 6 breaches in 2025 already involved AI-enabled attacks.[2]Simultaneously, organisations using AI-powered security tools cut their breach lifecycle by an average of 80 days and saved $1.9 million per breach.[2] The organisations that govern and deploy AI in their security stack over the next 18 months will have a material resilience advantage.

- ### Quantum Computing and Post-Quantum Cryptography

  While large-scale quantum computing remains three to seven years from breaking current encryption standards, organisations in defence, banking, and healthcare must begin transitioning to post-quantum cryptographic protocols now. NIST finalised its first post-quantum encryption standards in 2024; regulatory requirements for adoption will follow. The window for proactive migration is open — but narrowing.

- ### Cyber Insurance Maturation

  The cyber insurance market is approaching an inflection point. After years of sharp premium hikes, pricing has stabilised — but underwriters have raised the bar on what they require from insured organisations. Evidence of real operational controls — MFA, endpoint detection, tested incident response plans, and patch management — is now a prerequisite for coverage, not just a questionnaire checkbox.

- ### Critical Infrastructure as a Priority Battleground

  Manufacturing saw a nearly sixfold surge in espionage-motivated breaches in 2025 (from 3% to 20% of sector breaches, per Verizon DBIR).[3] India's move toward smart grids, connected ports, and digitised public services amplifies this risk. Public-private collaboration on critical infrastructure protection — sharing threat intelligence and hardening industrial control systems — will become a strategic national priority over the coming decade.

- **Data Protection as the Last Line of Defence**

  As perimeter defences prove fallible, organisations are increasingly recognising that the ability to recover clean, verified data rapidly is as strategically important as the ability to prevent attacks. The focus is shifting toward immutable, isolated data vaults, AI-assisted anomaly detection within backup environments, and recovery guarantees that are contractual — not just claimed.

- **Multicloud and AI Workloads Are Expanding the Protection Perimeter**

  As organisations distribute workloads across on-premises, cloud-native, and SaaS environments — and begin standing up AI infrastructure — data protection strategies built for a single-environment world are breaking down. The next frontier of cyber resilience requires unified protection that follows the data regardless of where it lives, with consistent recovery capabilities across every environment.

- **From Reactive Recovery to Measurable Resilience**

  The market is maturing beyond capability claims toward measurable, outcome-based resilience — where organisations can demonstrate, test, and guarantee their ability to recover within defined timeframes. Boards, regulators, and insurers are beginning to demand this level of evidence. Organisations that can prove resilience — not just assert it — will hold a distinct advantage in an environment where trust is increasingly a commercial currency.

Horizon	Key Developments to Watch
2026 — 2027	AI-SOCs standard in large enterprises; SEBI and RBI frameworks tighten; cyber insurance becomes a procurement prerequisite in key sectors; post-quantum cryptography migration begins
2028 — 2030	Post-quantum cryptography mandatory in critical sectors; cyber resilience scores integrated into credit and ESG ratings; India emerges as a net exporter of cybersecurity services and products

SOURCES & REFERENCES

[1] Cybersecurity Ventures — Cybercrime to Cost the World $10.5 Trillion Annually in 2025 — https://cybersecurityventures.com/official-cybercrime-report-2025/

[2] IBM Cost of a Data Breach Report 2025 (Primary Report & Press Release) — https://www.ibm.com/reports/data-breach

[3] Verizon 2025 Data Breach Investigations Report (DBIR) — Press Release — https://www.verizon.com/about/news/2025-data-breach-investigations-report

[4] World Economic Forum — Global Cybersecurity Outlook 2025 — https://www.weforum.org/publications/global-cybersecurity-outlook-2025/

[5] Check Point Software — State of Cyber Security in India 2025 — https://cxotoday.com/press-release/india-sees-2000-weekly-cyberattacks-per-organization-in-2025-check-point/

[6] Mordor Intelligence — India Cybersecurity Market Report 2026 — https://www.mordorintelligence.com/industry-reports/india-cybersecurity-market

[7] Gartner — Global Information Security Spending Forecast (via Programs.com 2025 compilation) — https://programs.com/resources/cybercrime-cost/

[8] ISC2 Cybersecurity Workforce Study 2024 — 4 Million Professional Gap — https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study

This research document comes from Siglap Consulting OPC Private Limited, a boutique technology research, insights, and marketing firms that provide tailored, agile, and prescriptive intelligence. Santanu Ganguly is the Founder & CEO of Siglap Consulting OPC Pvt. Ltd. and the driving force behind the brand Manifest Customer Success. A seasoned IT and Digital Transformation (DX) thought leader, he brings over 31 years of proven excellence

in solution sales and consulting across ASEAN, Asia Pacific, and India. He is known for his ability to build businesses, coach CEOs, and enable high-impact communities, by combining strategic vision with execution depth.