Deloitte.

Beyond the breach: Redefining cyber resilience for the modern enterprise

June 2025

Table of contents

Foreword

Cyber resilience is the new leadership. The future belongs to those who anticipate threats and use security as a launchpad for innovation and transformation.

In today's world, digital transformation is crucial for businesses. The ability to withstand cyber threats is now tied directly to an organisation's overall strength. As organisations accelerate their digital journeys, the velocity and sophistication of cyberthreats have outpaced traditional defence models, demanding a fundamental shift in how we perceive, plan and protect our digital ecosystems, business continuity and trust.

This whitepaper is both a call to action and a blueprint for transformation. It challenges the outdated view of cybersecurity as a reactive function and repositions it as a proactive, intelligence-driven and strategically integrated capability that fuels innovation, safeguards trust and ensures operational continuity amid relentless digital risk.

This strategy is driven by the convergence of anticipatory threat intelligence, offensive security validation and continuous improvement, reshaping how organisations stay ahead of threats. This model adapts to emerging risks, validates real-time defences and quantifies resilience as a measurable business outcome.

This whitepaper serves as a strategic imperative for organisations navigating the complexities of today's digital landscape. As cyberthreats grow in scale and sophistication, resilience must evolve from a technical aspiration to a boardroom priority.

Aligning with the principles of Cyber Surakshit Bharat, a national initiative aimed at strengthening the cybersecurity posture of India's digital ecosystem, this whitepaper empowers enterprises to fortify their defences and contribute to a secure and self-reliant digital India. This collective resilience will define the next generation of trusted businesses and digital leaders.

The path forward demands more than just technology. It calls for vision, agility and a commitment to continuous improvement. Those who adopt this mindset will withstand disruption and lead confidently, shaping a future where security and innovation go hand in hand.

Anand Tiwari
Partner
Deloitte India

Introduction: The evolving threat imperative

The global business landscape continuously transforms, driven by unprecedented interconnectedness and digital innovation. This evolution has unlocked great potential but also expanded the cyberattack surface, exposing organisations to more sophisticated and frequent threats.

The question is no longer about whether you will be breached but when. True leadership lies in preparing for and responding to that inevitability.

This stark reality necessitates a strategic pivot from reactive defence and mere prevention to inherent resilience; a proactive, threat-informed capability that ensures business continuity amid compromise.

Deloitte champions this paradigm shift, guiding organisations to reimagine cybersecurity not as a cost centre, but as a strategic enabler. By embedding advanced threat intelligence and offensive security methodologies into a continuous resilience lifecycle, enterprises can enhance their cyber defences. This approach allows them to anticipate, withstand and recover from even the most sophisticated cyberattacks, building bulletproof cyber defences. This paper outlines how a threat-informed resilience strategy is crucial for sustainable growth, regulatory compliance and enduring customer trust, serving as the "foundation of sustainable cyber defence" and the "new engine" for performance and long-term growth.

The shifting battleground: Cybersecurity in an era of unprecedented digital transformation

The digital transformation of enterprises goes far beyond isolated technological upgrades; it reshapes entire ecosystems, spanning core operations, supply chains, customer interactions and data flows. While this interconnectivity enhances operational efficiency and market responsiveness, it expands the cyberattack surface. Traditional perimeters are dissolving, replaced by complex, interwoven digital infrastructures.

This shift has revolutionised businesses, often replacing legacy systems with software-driven, cloud-integrated technologies. Modern enterprises rely heavily on connected systems, real-time data analytics and AI-powered automation to drive efficiency and innovation. However, this presents new cybersecurity challenges, making it more critical than ever to secure software and hardware and the vast volumes of data they generate. The very nature of value creation is now intrinsically linked to digital integrity and availability, making cybersecurity a foundational pillar of business strategy itself.

Per a recent Deloitte survey, 58 percent of organisations are integrating cybersecurity budgets with digital transformation, cloud and IT initiatives.[1]

Key resilience imperatives: Proactively countering advanced adversaries in today's landscape

A passive or purely defensive cybersecurity posture is no longer tenable in this dynamic threat environment. Organisations must embrace key resilience imperatives that enable them to proactively anticipate, counter and recover from advanced adversary actions. This requires a fundamental shift in mindset and methodology.

The critical role of anticipatory threat intelligence

The moment you anticipate the adversary, you gain the upper hand. With actionable intelligence, that advantage becomes a shield.

Effective cyber resilience begins with a profound and anticipatory understanding of the adversary. Reacting is no longer sufficient; organisations must proactively shape their defences based on a clear view of evolving threats.

Deloitte's global Cyber Threat Intelligence (CTI) provides these deep, actionable insights into adversary Tactics, Techniques and Procedures (TTPs), moving beyond generic alerts to deliver context-rich intelligence. This evidence-based approach is crucial for modern enterprise security programmes. It helps organisations to define "minimum operational viability" by identifying critical applications, assets, processes and key operational roles required to sustain business functions during and after a cyberattack.

Deloitte's CTI assessments emphasizes the growing impact of ransomware and identity-based attacks. In 2024, ransomware was linked to 44 percent of reviewed breaches.[2] Credential abuse accounted for 44.7 percent of data breaches in 2023,[3] up from 41.6 percent in 2022, highlighting its persistent prevalence. Other industry findings confirm a resurgence in stolen credentials as an initial access method, rising to 16 percent of intrusions in 2024.[4] Additionally, nearly 60 percent of all breaches involved a human element, with 32 percent explicitly attributed to credential abuse.[5] These insights are critical for guiding resilience strategies and prioritising cybersecurity resources effectively.

Furthermore, the exploitation of vulnerabilities, particularly zero-days (previously unknown security flaws with no available patches at the time of attack), accounted for 20 percent of initial access vectors in 2024, a 34 percent increase, largely targeting edge devices and VPNs.[6] The doubling of third-party involvement in breaches, from 15 percent to 30 percent in 2024, underscores the pervasive supply chain risk, exemplified by myriad incidents.[7]

The necessity of offensive security validation

Defence is just a theory. Offence is truth. Simulation is the test.

Anticipatory intelligence requires validation through simulated attacks and empirical data to confirm its operational value. Offensive security is critical in proactively identifying blind spots within an organisation's cyber defences before adversaries can exploit them. This involves simulating realistic attack scenarios to test the effectiveness of existing security measures and recovery playbooks.

- **Threat-Led Penetration Testing (TLPT):** Deloitte's TLPT services move beyond standard compliance checks, mimicking the TTPs of advanced adversaries based on up-to-date threat intelligence. This approach uncovers vulnerabilities and actual compromise paths that traditional testing often misses, providing critical insights to strengthen overall cyber resilience. By simulating realistic attack scenarios, TLPT uncovers vulnerabilities that compliance tests might miss, providing a more nuanced understanding of an institution's security posture.[8]

- **Purple teaming:** This simulation-driven collaborative strategy brings Red (offensive) and Blue (defensive) teams together to rapidly improve detection rules, enhance Security Information and Event Management (SIEM) systems and refine response strategies in real time, driving continuous improvement.

- **Adversary emulation:** Systematically mimicking the behaviour of known threat actors allows organisations to evaluate defensive capabilities against specific, real-world threats, prioritising defences around actual adversary behaviour. A study highlights that these solutions help optimise defence, improve exposure awareness and scale offensive-testing capabilities.[9]

Emerging risks and the offensive edge: Navigating the next wave of cyberthreats

The only constant in cybersecurity is change. As threats evolve, so must our vigilance and strategies to outpace them.

The threat landscape is not static; it evolves with technological advancements and attacker ingenuity.

To maintain an offensive edge, organisations must proactively anticipate emerging risks that target the core of modern IT infrastructure and enterprise operations. This requires a clear understanding of the emerging frontiers where adversaries are concentrating their efforts. Key areas include:

AI-augmented attack campaigns

Adversaries are increasingly using AI and ML to enhance reconnaissance, automate attack processes and scale sophisticated cyberthreats. This includes crafting highly convincing phishing campaigns, evading detection through adaptive malware and rapidly exploiting newly discovered vulnerabilities (zero-days) with unprecedented speed and precision.

Exploitation of interconnected ecosystems and APIs

Interconnected cloud services, third-party applications and APIs have become prime targets as organisations increasingly depend on them to power their operations. A compromise in one part of the ecosystem can rapidly propagate, leading to widespread data breaches or operational disruptions. Securing these complex digital supply chains is paramount.

Attacks on Operational Technology (OT) and IoT at scale

The convergence of IT and OT, along with the rapid growth of Internet of Things (IoT) devices in enterprise environments, expands the physical attack surface. Threats range from disrupting industrial control systems to weaponising large fleets of insecure IoT devices for Distributed Denial of Service (DDoS) attacks or as entry points into corporate networks.

Deepfakes and disinformation targeting business integrity

Sophisticated AI-generated deepfakes (audio and video) and targeted disinformation campaigns pose a growing threat to business reputation, financial stability (stock manipulation via fake executive statements) and internal security (social engineering using fake CEO voice commands).

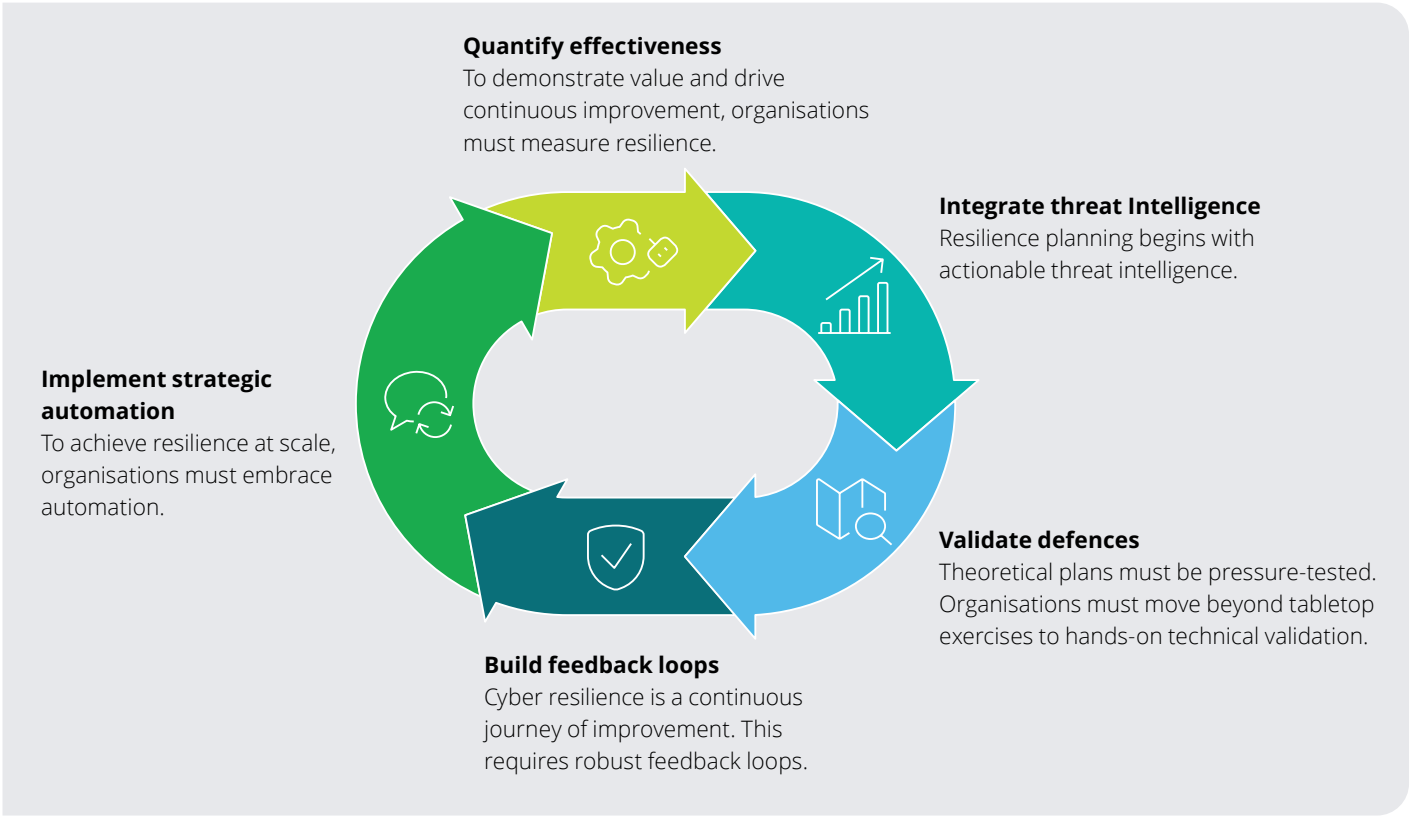
Quantum computing's impending cryptographic threat

While still nascent, the advancement of quantum computing poses a long-term existential threat to current public-key cryptography standards. Organisations must transition strategically to Post-Quantum Cryptography (PQC) to protect sensitive data and secure communications against future decryption capabilities.

Anticipating these multifaceted threats requires a forward-leaning security posture, continuously evaluating how new technologies can be weaponised and how defences, including resilience and recovery strategies, must adapt proactively.

A blueprint for bulletproof resilience

A multi-layered strategic framework



Mitigating today's complex cyber risks requires more than a collection of point solutions; it demands a multi-layered, strategic framework that embeds organisational resilience.

Integrating threat intelligence into strategic planning

To build effective resilience strategies, organisations should anchor their efforts in actionable threat intelligence. This involves:

- Continuously mapping adversary TTPs to the organisation's specific environment.
- Prioritising critical assets and processes based on threat actor focus and potential business impact.
- Developing specific recovery scenarios and resilience goals aligned with anticipated attack methods and system vulnerabilities.
- Establishing a "threat intelligence to resilience flow", where raw threat data is processed into actionable intelligence, informing risk assessments, critical asset identification and developing targeted recovery playbooks.

Validating defences through rigorous, hands-on technical exercises

Theoretical plans must be pressure-tested. Organisations must move beyond tabletop exercises to hands-on technical validation:

- **Cleanroom recovery simulations**
  Deloitte's Cyber Incident Readiness, Response and Recovery (CIR3) services emphasize these controlled, isolated environments to test recovery protocols rigorously. This ensures restored data and systems are clean and fully functional, mitigating reinfection risks.[10]
- **Cyber ranges and immersive simulations**
  These platforms provide realistic training environments, generating sophisticated threat scenarios that allow teams to train under conditions mimicking real-world attacks, evaluating their ability to detect, respond and recover effectively. SANS Institute consistently underscores the value of such hands-on training environments for honing practical skills and validating defensive postures against evolving threats.

Building dynamic feedback loops: From incident response to proactive evolution

Cyber resilience is a continuous journey of improvement. This requires robust feedback loops:

- **Post-incident reviews**
  Structured reviews after any incident (or near-miss) to determine root causes, identify how breaches occurred and resolve vulnerabilities to prevent recurrence. This includes refining your IR plan and playbooks to adapt to abrupt changes in staff. SANS incident response methodologies also stress the critical importance of comprehensive post-incident analysis to prevent recurrence and improve future response.
- **Integrating threat hunting insights**
  Proactive threat hunting uncovers undetected threats. Per a study, threat intelligence platforms integrate AI-backed threat hunting models for real-time visibility. SANS often highlights proactive threat hunting as a key discipline for reducing attacker dwell time and identifying compromises that automated defences may miss. These findings, including new TTPs or vulnerabilities, must be directly integrated into defensive strategies and recovery playbook updates.
- **Offensive security learnings**
  Insights from TLPT, purple teaming and adversary emulation must drive continuous improvements in technology, processes and security awareness.

Strategic automation: The role of AI in security operations

To achieve resilience at scale, organisations must embrace automation:

- **AI in security operations**
  Integrating AI and automation is increasingly prevalent. As highlighted by the SANS Detection and Response Survey 2024,[12] most organisations plan to expand their use of AI/ML. The SANS 2024 AI Survey[13] recognises AI's role as a "co-pilot," enabling automation of routine tasks. A study predicts that by 2027, AI agents will reduce the time it takes to exploit account exposures by 50 percent.[14] Deloitte's "Global Future of Cyber Survey"[15] also shows that 39 percent of organisations are using AI in cybersecurity to a large extent. Top concerns include explainability, data poisoning and integrity risks.
- **SOAR for orchestrated response**
  Security Orchestration, Automation and Response (SOAR) platforms are vital for automating repetitive incident response processes such as phishing remediation and endpoint isolation, enabling consistent, rapid execution and reducing manual workload. By identifying and automating feasible security operations, organisations can enhance efficiency, minimise response times and strengthen overall cyber resilience.

- **Deloitte's "Cybersecurity meets AI and GenAI"[16]**
  This report emphasizes that while these technologies offer new defensive opportunities, they also empower attackers. A comprehensive framework is needed to secure AI/GenAI systems and use them for defence and combat AI-driven threats. According to Gartner, GenAI is most effective with quick scans, fast threat detection and responses and building models that predict vulnerabilities.

Measuring what matters: Quantifying resilience effectiveness

To demonstrate value and drive continuous improvement, organisations must measure resilience:

- **Outcome-driven metrics and risk quantification**
  Solutions such as Deloitte's Cyber-Strategic Measurement and Quantification (CMAQ)[17] offer enhanced cyber risk visibility, continuous evaluation and standardised risk scoring. This supports data-driven decision-making to reduce exposure, aligned with the NIST Cybersecurity Framework (CSF). CMAQ delivers near real-time data-based risk insights across your organisation to drive strategic decisions that help manage and reduce cyber risk exposure.
- **Resilience metrics**
  Tracking KPIs such as Mean Time to Detect (MTTD), Mean Time to Recover (MTTR), breach cost reduction, ROI of security investments and compliance scores provides tangible evidence of resilience effectiveness. Standardised outcome-driven metrics,[18] are essential. The NIST Cybersecurity Framework (CSF) 2.0 and a Digital Value Management System (DVMS) offer an outcome-based governance approach for continuous improvement.[19] SANS also emphasizes the importance of metrics such as MTTD and MTTR, highlighting them as critical indicators of a Security Operations Centre's (SOC) effectiveness and overall security posture maturity.
- **Cyber maturity as a driver of resilience**
  Deloitte's "Global Future of Cyber" Survey[20] shows that High-cyber-maturity organisations are 2.4x more likely to expect positive outcomes from cybersecurity investments and demonstrate significantly higher resilience, even when facing more breaches.

Accelerating your resilience journey: Embedding continuous improvement for a connected future

Achieving robust cyber resilience is not a one-time project but an ongoing commitment to adaptation and improvement. With the constant evolution of the digital landscape and threat actors, organisations must continuously adapt their resilience strategies. Driving this evolution forward requires:

Leadership commitment

Resilience must be championed from the top, with clear mandates and resource allocation.

Cross-functional collaboration

A holistic approach requires breaking down silos among IT, security, business units and risk management.

Talent development

Investing in the skills and expertise needed to manage sophisticated threat intelligence, conduct offensive security and operate advanced defensive technologies. The industry-recognised certifications and training programmes from organisations such as SANS Institute are invaluable in building and validating these critical cybersecurity skills across teams.

Strategic collaborations

Collaborating with trusted advisors and technology providers who bring expertise and leading-edge capabilities.

A culture of security awareness

Embedding security consciousness throughout the organisation, making every employee a part of the human firewall. SANS strongly advocates for continuous security awareness training, recognising that a well-informed workforce is a crucial layer of defence.

By treating resilience as a dynamic capability, organisations can ensure they are prepared for today's threats and agile enough to adapt to tomorrow's unforeseen challenges, safeguarding their operations and stakeholder trust in an increasingly connected world.

CXO watch: Why threat-informed resilience is a boardroom mandate

Cybersecurity is no longer an IT issue but a fundamental business enabler. Resilience underpins trust, innovation and sustainable growth.

For CXOs, particularly CISOs, CEOs, CROs and Boards, threat-informed cyber resilience is not just a technical concern but a foundational strategic business priority. The modern digital ecosystem touches every enterprise facet: critical infrastructure, customer trust, operational continuity and digital commerce. A significant breach can trigger devastating reputational damage, severe regulatory penalties, prolonged service disruptions and critical risks to safety.

Cybersecurity in this new era is not about avoiding hypothetical threats; it is about protecting the very lifeblood of the organisation, maintaining customer confidence and enabling secure growth at scale. To secure the enterprise ecosystem, CXOs must embed threat-informed resilience into their core digital and product transformation strategy by championing the following mandates:

01

Executive-backed secure-by-design and resilience mandate
Adopt a zero-trust, threat-informed approach across the entire business lifecycle, from innovation and design to decommissioning. Make resilience architecture reviews, threat modelling and recovery validation a board-level KPI.

Proactive threat alignment and offensive validation
Prepare for converging global cyberthreats by actively using Threat Intelligence (TI) and offensive security. Use Deloitte's advanced TLPT and Purple teaming to uncover hidden risks and validate defences against real-world adversary TTPs. Early and aggressive validation of your security posture provides a distinct competitive advantage.

02

03

Validate to operate
Transition from tabletop discussions to rigorous, hands-on technical validation of recovery capabilities. Use Cleanroom recovery simulations and advanced Cyber Ranges, like those facilitated by Deloitte's CIR3 services, to ensure that critical systems can be restored cleanly, and operations can resume swiftly post-incident.

Foster a culture of continuous learning and adaptation
Establish robust feedback loops from incident response, threat hunting and offensive security exercises directly into resilience planning. This ensures defensive strategies and recovery playbooks dynamically evolve with the threat landscape.

04

05

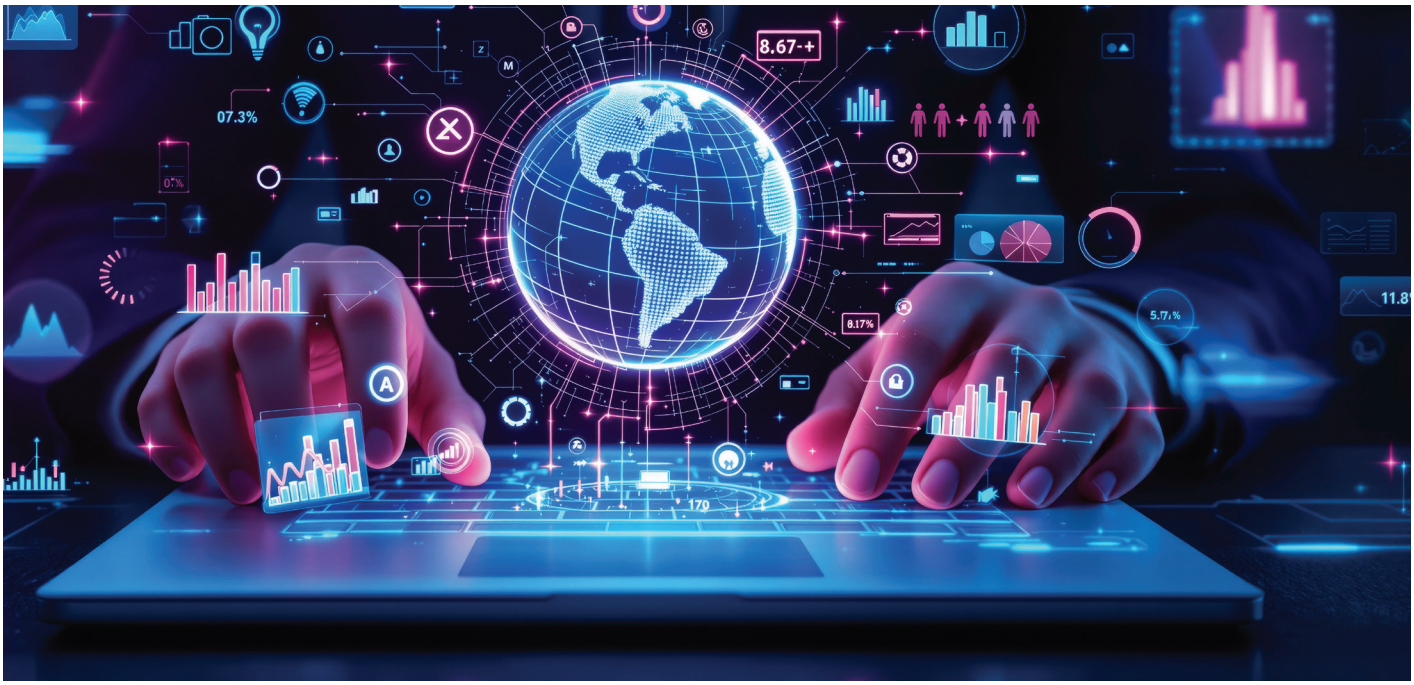
Embrace strategic automation and AI-powered defence
Collaborate with leading providers to adopt advanced, SaaS-like Managed Detection and Response (MDR) and SOAR capabilities. As AI is becoming integral to security operations, a machine-led, human-empowered Security Operations Centre is crucial to outpacing attackers.

Measure what matters
Implement outcome-driven metrics and cyber risk quantification solutions, such as CMAQ, to gain near real-time, data-based risk insights. This enables strategic decisions that demonstrably reduce cyber risk exposure and articulate the business value of resilience investments, aligning with frameworks such as NIST CSF 2.0.

06

07

Build trust, not just defences
The future of business is undeniably digital, but trust will be its true currency. As attack surfaces expand, CXOs have a unique opportunity to position cybersecurity as a brand promise, a regulatory safeguard and a catalyst for revenue growth. A resilient enterprise accelerates customer adoption by ensuring privacy and safety, preventing costly downtime through robust threat detection, enabling global regulatory compliance, protecting R&D and IP and driving investor confidence for long-term growth.



Conclusion: The new engine of business performance

In the digital economy, trust is the ultimate currency. Cyber resilience is how you earn and protect it.

As organisations navigate an era of profound digital transformation, integrating threat-informed cyber resilience into every facet of the enterprise is essential. With the relentless evolution of cyberthreats, security must extend across all systems, data, infrastructure and interconnected digital services. This complex landscape demands a proactive, collaborative and adaptive resilience strategy from businesses, governments and innovators.

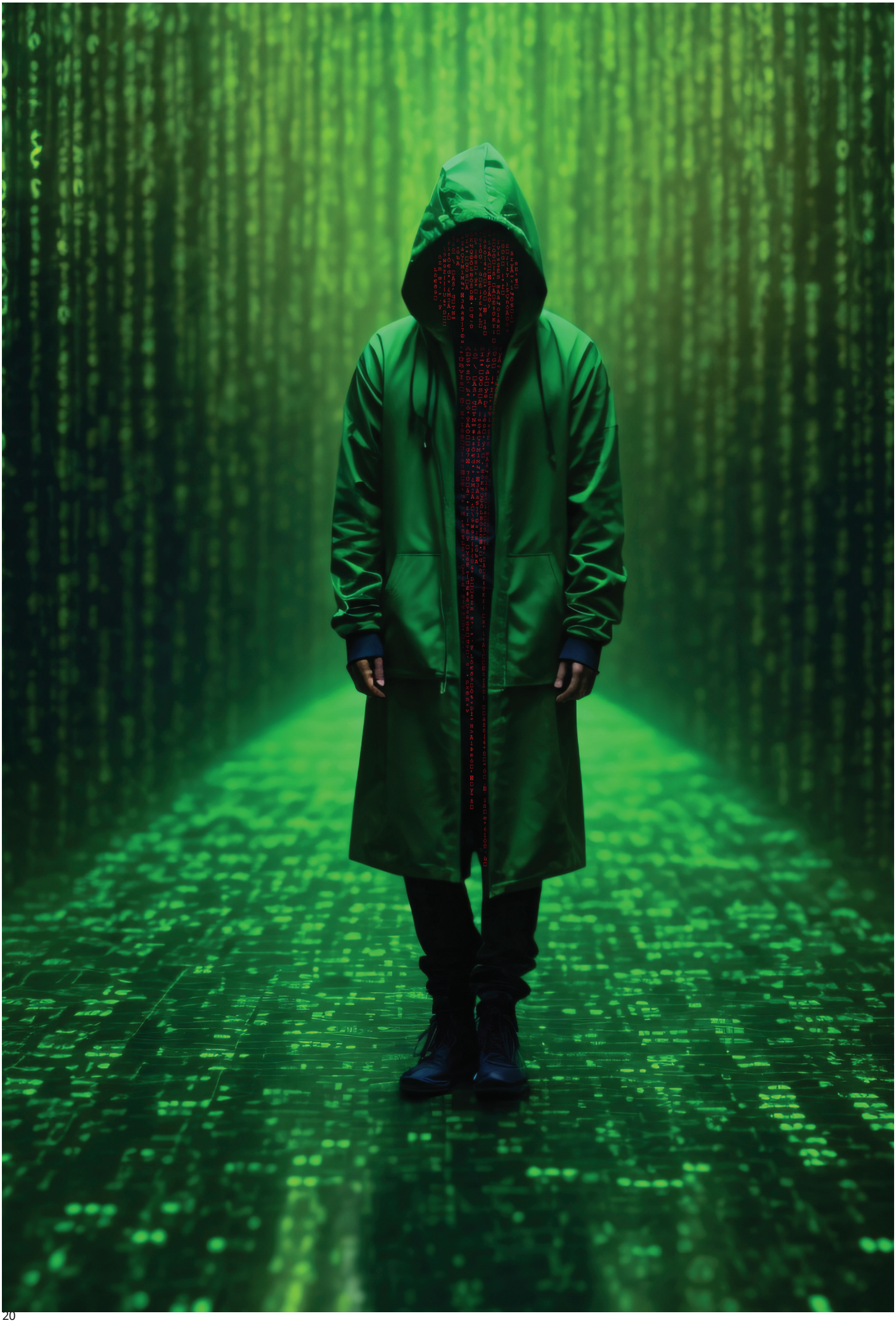
Cyber resilience is the first line of defence in a landscape of evolving digital threats. For organisations, adopting strong, threat-aware cybersecurity practices is essential for long-term growth, meeting regulatory requirements and maintaining customer trust. For leaders, it provides the confidence to innovate and seize market opportunities securely.

As we accelerate towards an increasingly digitised future, resilience must be engineered from the ground up, protecting critical operations, data and stakeholder value. Those prioritising threat-informed resilience today will safeguard their enterprises and lead the charge into tomorrow's competitive landscape. Ultimately, cyber resilience is a strategic growth driver, and as the digital ecosystem expands, it will differentiate those prepared for the next era of business.

True transformation lies in adopting new technologies and securing them with inherent, adaptive resilience. Cyber resilience must become the new engine of business performance, powering operational stability, trust, safety and long-term growth. Tomorrow’s business leaders will act today, embedding security by design, strengthening digital trust through proven resilience and driving a secure, sustainable future.

References

1. Deloitte "Global Future of Cyber" survey, https://www.deloitte.com/global/en/services/consulting-risk/research/global-future-of-cyber.html
2. Verizon DBIR 2025, Page 10, https://www.verizon.com/business/resources/Tea/reports/2025-dbir-data-breach-investigations-report.pdf
3. Deloitte CTI Cybersecurity Threat Trends Report 2024, Page 6, https://www2.deloitte.com/us/en/pages/risk/articles/cybersecurity-threat-trends-report-2024.html
4. Mandiant M-Trends Report 2025, https://cloud.google.com/security/resources/m-trends
5. Verizon DBIR 2025, Figure 15, Page 20, https://www.verizon.com/business/resources/Tea/reports/2025-dbir-data-breach-investigations-report.pdf
6. Verizon DBIR 2025, Figure 5, Page 10, https://www.verizon.com/business/resources/Tea/reports/2025-dbir-data-breach-investigations-report.pdf
7. https://www.techrepublic.com/article/snowflake-data-theft-extortion/
8. Deloitte TLPT, https://www.deloitte.com/lu/en/services/risk-advisory/services/threat-led-penetration-testing.html
9. Gartner Market Guide for Adversarial Exposure Validation, https://gcom.pdo.aws.gartner.com/en/documents/6255151
10. Deloitte CIR3 services, https://www.deloitte.com/global/en/services/consulting-risk/services/cyber-incident-response.html
11. Gartner on AI-backed threat hunting, https://www.gartner.com/en/documents/5656423
12. SANS Detection and Response Survey 2024, https://www.sans.org/white-papers/sans-2024-detection-response-survey/
13. SANS 2024 AI Survey, https://www.sans.org/white-papers/sans-2024-ai-survey-ai-growing-role-cybersecurity-lessons-learned-path-forward
14. Gartner prediction on AI agents, https://www.gartner.com/en/newsroom/press-releases/2025-03-18-gartner-predicts-ai-agents-will-reduce-the-time-it-takes-to-exploit-account-exposures-by-50-percent-by-2027
15. Deloitte "Global Future of Cyber" survey, https://www.deloitte.com/global/en/services/consulting-risk/research/global-future-of-cyber.html
16. Deloitte "Cybersecurity meets AI and GenAI" report, https://www.deloitte.com/global/en/services/consulting-risk/perspectives/cybersecurity-meets-ai-genai.html
17. Deloitte CMAQ, https://www2.deloitte.com/us/en/pages/risk/solutions/cyber-risk-quantification-CMAQ.html
18. Gartner on outcome-driven metrics, https://www.gartner.com/en/cybersecurity/research/cybersecurity-business-value-benchmark
19. NIST CSF 2.0 and DVMS / IDC Whitepaper, https://www.hpe.com/psnow/doc/a00142134enw
20. Deloitte "Global Future of Cyber" survey, https://www.deloitte.com/global/en/services/consulting-risk/research/global-future-of-cyber.html



Connect with us

Sathish Gopalaiah
President, Technology and Transformation,
Deloitte South Asia
sathishtg@deloitte.com

Gaurav Shukla
Partner and Leader – Cyber,
Deloitte South Asia
shuklagaurav@deloitte.com

Anand Tiwari
Partner
Deloitte India
anandtiwari@deloitte.com

Sanjeev Singh
Partner
Deloitte India
sanjeevs@deloitte.com

Contributors

Piyush Baranwal

Nixon Matharu

Krishna Sanapala

Sunita Kumari

Arnav Agarwal

Deloitte.