Deloitte.



Defending the digital insurer

November 2026

Table of contents

Foreword 04

Executive summary 05

Chapter 1: Emphasizing the growing cyber risk in India 06

Chapter 2: How insurers assess and underwrite customer cyber risks 19

Chapter 3: How insurance companies need to protect themselves against cyberattacks 34

Chapter 4: Regulations: IRDAI guidelines, DPDP Act, IT Act and CERT-In advisories 37

Conclusion: Building a resilient digital insurance ecosystem 42

Endnotes 44

Connect with us 46

Foreword



Debashish Banerjee
Partner, Insurance Sector Leader
Deloitte South Asia



Munjal Kamdar
Partner
Deloitte India

The world of cyberthreats is evolving at a faster pace. Insurers are now exposed to risks far exceeding a simple data compromise or even a single security breach. Underwriters pursuing digital transformation are changing the way they process customer identification, payments and services, and, more crucially, build trust at every touchpoint. Meanwhile, the surge in connectivity and the swift rise of AI are presenting fresh opportunities and introducing a whole new set of intricate risks. Cyber risk, once seen largely as a technology or IT concern, is now a broader business challenge, one that can affect insurers, customers, collaborators and the wider insurance ecosystem.

The effects of this transformation are already visible across the insurance value chain. Digital identity enables near-instant customer onboarding, APIs strengthen connectivity between insurers and financial technology networks, and AI is increasing the sophistication of both fraudulent and legitimate activities. As risks become more dynamic and interconnected, traditional, point-in-time approaches to underwriting and risk management are becoming insufficient.

This publication, "Defending the Digital Insurer," explores how insurers can respond through intelligence-led underwriting, continuous cyber-risk monitoring, adaptive pricing, stronger cyber maturity assessment and sophisticated loss and accumulation modelling. It also highlights the growing importance of alternative cyber datasets, ransomware stress testing, cyber catastrophe modelling, third-party risk assessment and regulatory resilience in developing a more comprehensive view of emerging exposure.

In this environment, insurers have a broader responsibility to strengthen their own cyber resilience while supporting resilience across customers, intermediaries, digital channels and third-party networks.

As custodians of trust and financial stability, insurers can become enablers of ecosystem resilience, helping to reduce systemic exposure while supporting customer confidence and sustainable growth. India stands at an important inflexion point. Insurers that integrate cyber resilience across underwriting, fraud, claims, cybersecurity and enterprise risk management will be better positioned to respond to evolving threats, strengthen portfolio resilience and support the sustainable growth of India's digital insurance ecosystem.

The pages ahead present perspectives on the trends and ideas influencing the evolution of digital insurance providers.

Executive summary

The cyber risk environment is escalating as insurers quickly digitalise their operations, customer journeys and ecosystems. Identity-led attacks, AI-enabled fraud, operational vulnerabilities and interconnected digital ecosystems are converging to create risks that can affect trust, resilience, underwriting, claims and growth. Cyber risk is no longer just a technology issue, but a strategic business priority.

This publication, **Defending the Digital Insurer,** examines insurers' responses to this shifting landscape through the **Deloitte Secure, Vigilant and Resilient (SVR) Framework.** The framework provides a systematic path to building cyber resilience at scale. It is structured around three core elements:

- **Secure:** Strengthens digital foundations through identity-centric security, zero trust, cloud protection and robust controls
- **Vigilant:** Connects cyber, fraud, claims, underwriting and customer signals with AI, behavioural analytics and anomaly detection to enable continuous, intelligence-led detection
- **Resilient:** Embeds cyber risk into enterprise risk management, operational resilience, governance and ecosystem oversight, strengthening insurers' ability to anticipate, respond to and recover from disruption

The publication explores both facets of the cyber risk equation: how insurers can protect themselves from attacks and how they can better understand, underwrite and price cyber risk for policyholders. It outlines the operating model, technology and investment requirements needed to achieve these objectives and explores how leading practices can be tailored for the Indian market.

As the cyber insurance sector evolves, dynamic underwriting and pricing will prove crucial. Insurers will need to assess the likelihood and potential severity of an incident using indicators such as security posture, exposure, behavioural risk, historical incidents, claims experience and real-time cyber signals. Insights drawn from these indicators can support more responsive pricing as incident probability, loss severity and claims frequency evolve.

This publication examines how insurers can lead and participate in creating secure, smart and resilient digital insurance ecosystems that also unlock cyber insurance as a significant growth engine, given the momentum of digital infrastructure and policy reform in India.

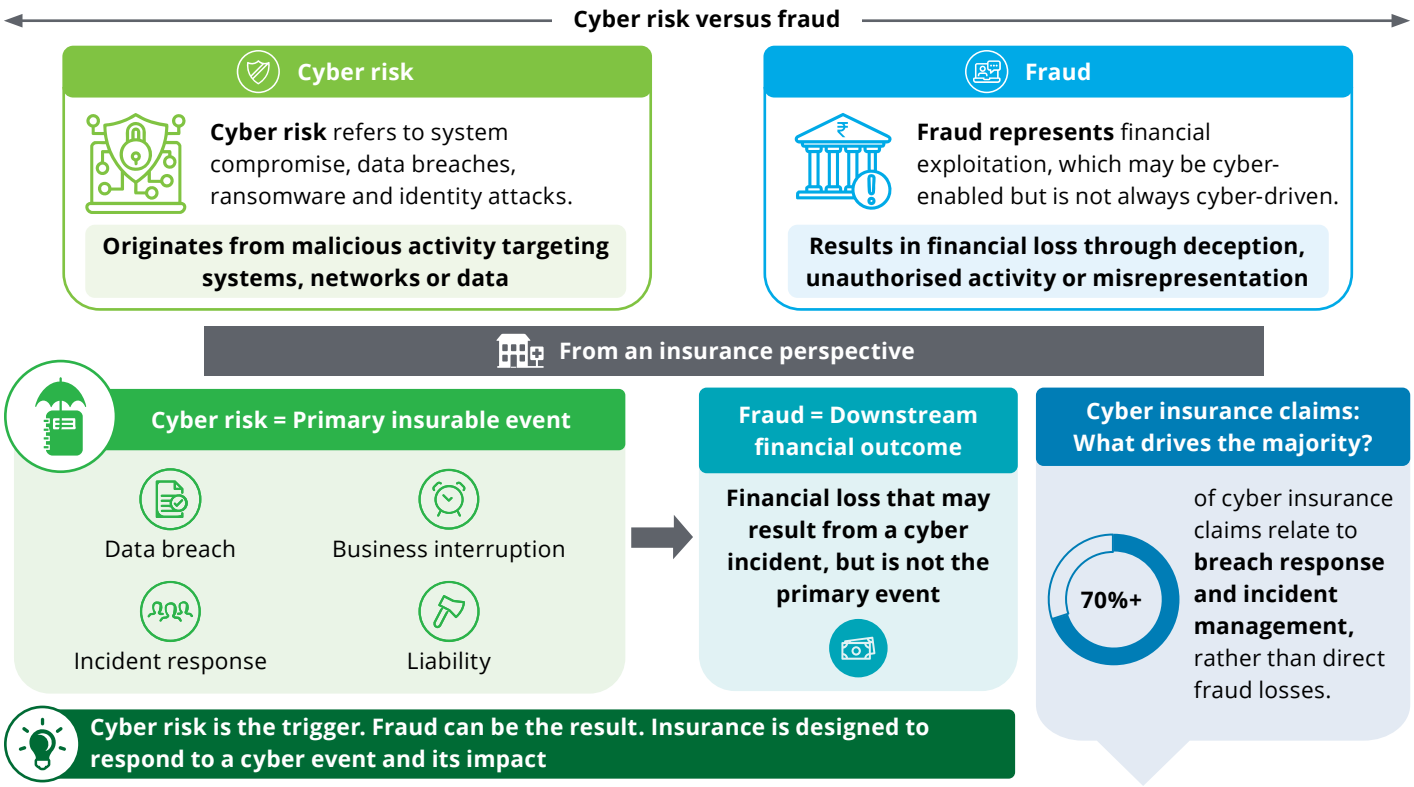


Chapter 1: Emphasizing the growing cyber risk in India

India's rapid digitalisation over the last decade has rewritten the nature of risk for the country. Mobile coverage, smartphones, Digital Public Infrastructure (DPI) and real-time payments systems have enabled digital-native consumer behaviour and have made "digital-first" the de facto approach to many consumer-facing interactions across banks, insurers, e-commerce sites and payment platforms. For insurers, digitalising the customer purchase cycle, underwriting, service, payments and claims increases cyber exposure, making cyber resilience an integral element of their overall business strategy rather than simply a technology problem. This impact is perhaps more profound for the insurance industry, where digital-first customer journeys, Application Programming Interface (API)-powered ecosystems and embedded insurance are rapidly changing how insurance products are distributed and managed.

Digital transformation will play a central role in advancing India's "Insurance for All by 2047" vision. It can help insurers serve a broader customer base across urban and rural India while enabling greater connectivity among insurers, technology providers, brokers and other ecosystem participants. The increased connectivity among actors in a more ecosystem-based world, whether in clouds, through interlinked ecosystems or via real-time payment infrastructures, is exposing the insurance sector to a wider range of more systemic cyberthreats beyond localised failures. As insurers operate across increasingly interconnected digital ecosystems, fraud is also evolving in fundamental ways. Unlike traditional insurance fraud centred on fabricated claims or agent misconduct, cyber-enabled fraud increasingly exploits compromised credentials, synthetic identities, deepfake impersonation, AI-generated artefacts and social engineering to infiltrate digital customer journeys across onboarding, servicing, claims and payments. In many cases, cyber compromise becomes the precursor to financial fraud, underscoring the importance of clearly distinguishing cyber risk from traditional fraud, as illustrated below:

Figure 1: Understanding the difference between cyber risk and fraud



Source: Deloitte analysis, Cyber insurance 2026 statistics

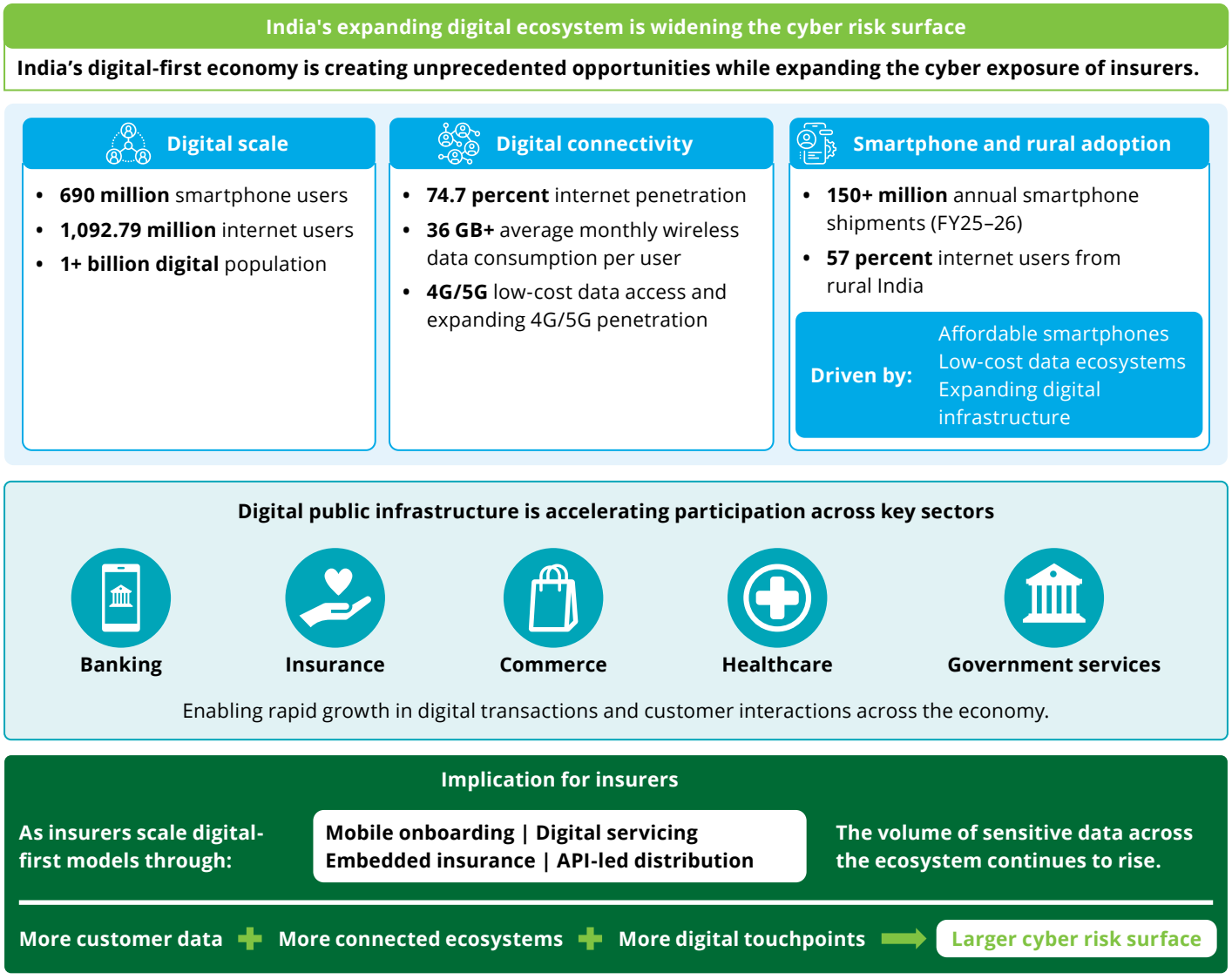
Accordingly, this publication focuses on cyber risk and cyber-enabled fraud as key drivers of financial loss, with particular attention to identity theft, account takeover and synthetic identities. It examines the role of cyber insurance in transferring these risks while excluding traditional insurance fraud, such as fabricated claims and agent misconduct.

This chapter explores how digital adoption, ecosystem interdependencies, AI-enabled threats and regulatory developments are reshaping India's cyber-risk landscape and influencing enterprise resilience.

India's mobile-first digital economy: Expanding the cyber-risk surface

India's mobile-first economy is fuelling its digital transformation. Over the past decade, growing access to affordable smartphones and mobile data, plus expanding internet penetration, has revolutionised the way Indian consumers access financial, commerce, health and insurance services. Across sectors, mobile is the new medium for customer onboarding, payments, services and customer interaction.

Figure 2: India's expanding digital ecosystem and cyber risk surface



Greater digital adoption is accelerating insurance innovation, but also widening the cyberattack surface.

Source: Deloitte analysis; Digital portal; Smartphone market analysis, 2026; Internet and Mobile Association of India, Internet Statistics in India: Usage and Penetration Rate (2026), Smartphone Users In India (2026 Data), Telecom Regulatory Authority of India (TRAI)



For insurers, cyber risk in India is growing due to the following three structural factors.

Figure 3: Reasons for the increase in cyber risk among insurers in India

The pace of digital adoption has outstripped the maturity of cyber resilience capabilities in several areas, including **identity intelligence, real-time monitoring, data integration and ecosystem-wide fraud coordination.**



Insurers are now handling significantly larger volumes of sensitive financial, health and behavioural data through digital channels, making them attractive targets for **ransomware groups, organised fraud networks and identity-focused attackers.**

Insurance ecosystems are becoming highly interconnected through APIs, cloud platforms, embedded insurance models and digital servicing channels, increasing **dependency on external partners and third-party infrastructure.**

Source: Deloitte analysis

India's rapid digital adoption is reshaping the cyberthreat landscape. Cyber risks were once largely infrastructure-led, with attacks focused on malware and isolated system intrusions. Attacks are now increasingly identity-centric, transaction-led and enabled by AI. Cybercriminals use compromised credentials, phishing, synthetic identities, deepfake impersonation and AI-generated content to enter legitimate customer journeys.

This risk is particularly pronounced in India. Mobile-first insurance interactions and high-frequency payments allow transactions to be completed within seconds, leaving limited time for human intervention or real-time security responses. For insurers, expanding digital access must therefore go hand in hand with building trust and security across customer journeys.

Real-time financial ecosystems amplify cyber risk

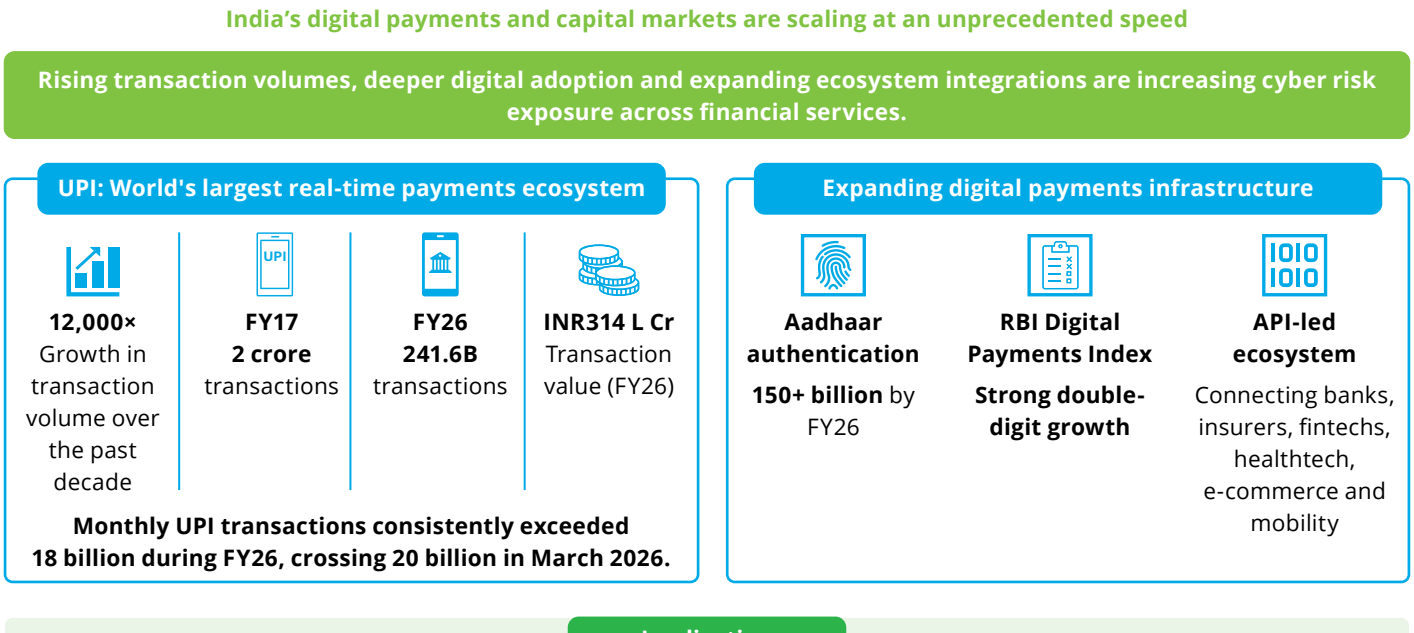
As India's financial ecosystem becomes more digital and interconnected, its exposure to cyber risk is increasing.

The growing use of real-time payments, digital identity systems and high-speed transactions is expanding the potential attack surface for financial institutions, including insurers.

India's insurance sector is facing accelerated cyber risk exposure due to the rapid rise of digital infrastructure, real-time financial ecosystems and interconnected distribution networks. The increasing scale is driven by the rapid deployment of DPI, such as Aadhaar, UPI, Account Aggregator frameworks and API-enabled financial services, which enable insurers to scale policy issuance and servicing quickly.

This growth also makes insurers more dependent on a wider digital ecosystem. Core functions such as policy issuance, premium collection, claims settlement, customer identification and servicing are increasingly connected with banking systems, payment gateways, third-party APIs and fintech services. As these connections increase, so do the potential points of exposure to cyberthreats.

Figure 4: Growth in India's digital financial ecosystem



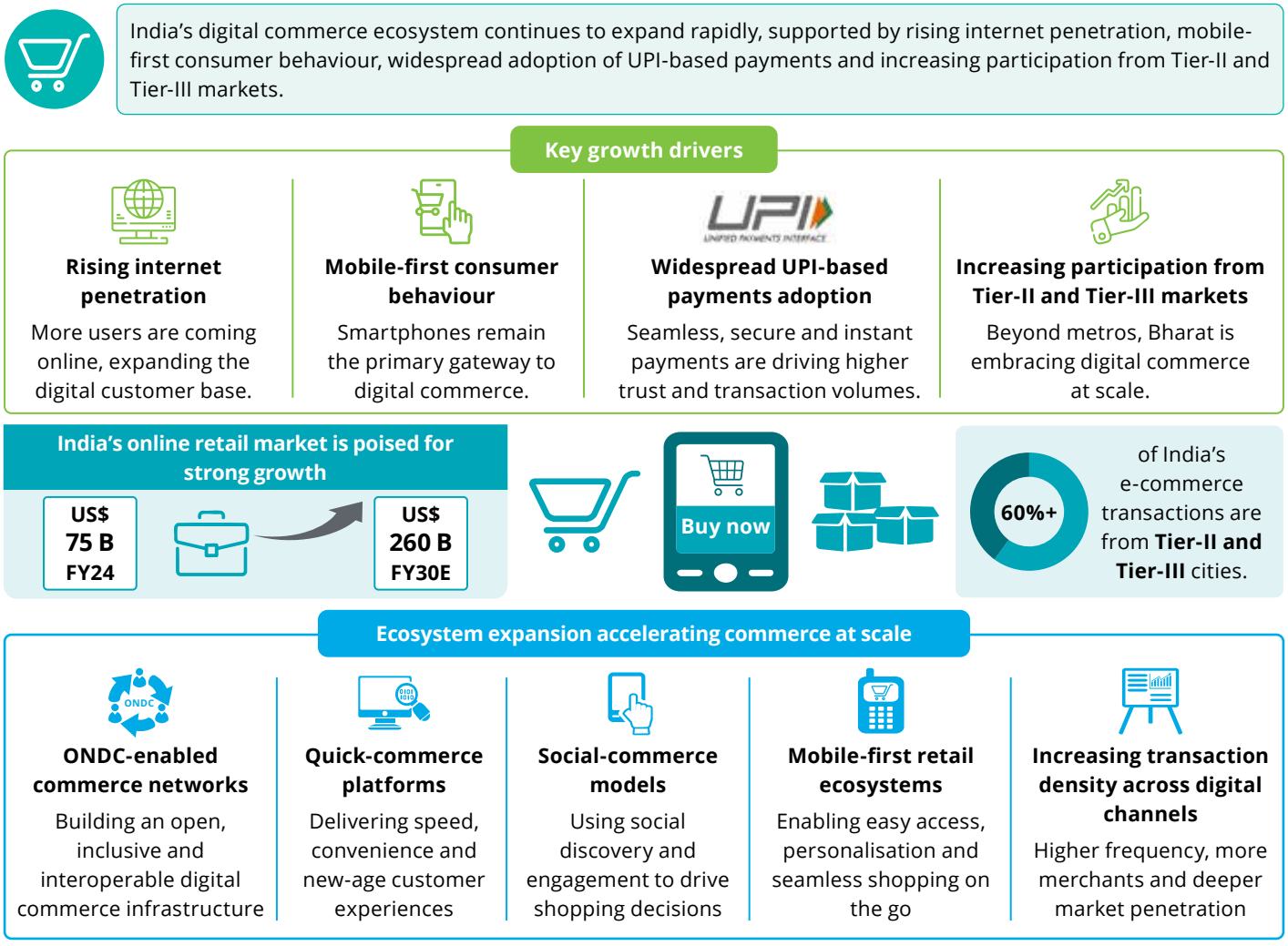
Source: NPCI Monthly Transaction Data, March 2026; RBI; PIB; IBEF; NSE.

As transaction volumes rise across India's digital financial ecosystem, cyber risk is becoming increasingly systemic, with vulnerabilities in identity systems, payment infrastructure, cloud environments and third-party ecosystems that can affect multiple institutions simultaneously. Fraudsters increasingly exploit compromised credentials, phishing, synthetic identities, deepfake impersonation and AI-generated artefacts to infiltrate customer journeys, with cyber compromise often preceding fraud across onboarding, claims and payments. Coupled with fragmented legacy systems and collaborator ecosystems, insurers face growing visibility gaps. As digital insurance expands under the Insurance for All by 2047 vision, cyber resilience has become fundamental to sustaining trust, protecting financial stability and enabling secure digital growth. Among the key drivers of this expanding cyber risk landscape, the rapid growth of digital commerce is emerging as a significant source of new vulnerabilities.

Online shopping is expanding cyber exposure

The rapid growth of India's digital commerce ecosystem is creating new channels of cyber exposure across consumers, merchants, payment systems and insurers. As online shopping, embedded finance and digital servicing ecosystems scale, cyber risks increasingly propagate across interconnected platforms through identity compromise, payment fraud, phishing attacks, account takeover and third-party vulnerabilities.

Figure 5: How e-commerce is reshaping India's cyber risk landscape



Source: Deloitte-FICCI Report: Spotting India's PRIME innovation moment

These trends reinforce India's position as one of the world's fastest-growing digital commerce markets, with digital transaction volumes, merchant participation and platform-based commerce continuing to scale across the economy. The growth of online shopping is expanding consumers' cyber exposure as millions of users store payment credentials, personal information, location data, purchase histories and digital identities across commerce platforms, payment applications and financial ecosystems. As digital engagement deepens, cybercriminals increasingly exploit phishing, credential theft, account takeover, fake merchant websites, payment redirection and AI-enabled social engineering.

Deloitte's analysis highlights that digital commerce growth is increasingly driven by omnichannel retail, platform integrations, AI-enabled consumer engagement and expanding ecosystem collaborations, materially increasing transaction density and interconnectivity across digital channels. Consequently, regulatory expectations are shifting from periodic vendor assessments towards continuous, risk-based third-party resilience monitoring.[1]

As embedded insurance expands across e-commerce, mobility, travel and digital payments, insurers are becoming increasingly dependent on external platforms for customer acquisition, servicing, claims and data exchange, which materially increases systemic cyber exposure across merchants, financial institutions, payment networks and insurers. This reinforces the need for continuous third-party risk monitoring, stronger cyber resilience, identity intelligence and coordinated fraud risk management across interconnected digital value chains.

India's rising cyberattack exposure: A structurally vulnerable digital economy

India's accelerating digital transformation is creating new opportunities while increasing the country's exposure to cyber risk. Growing interdependence across the financial services,



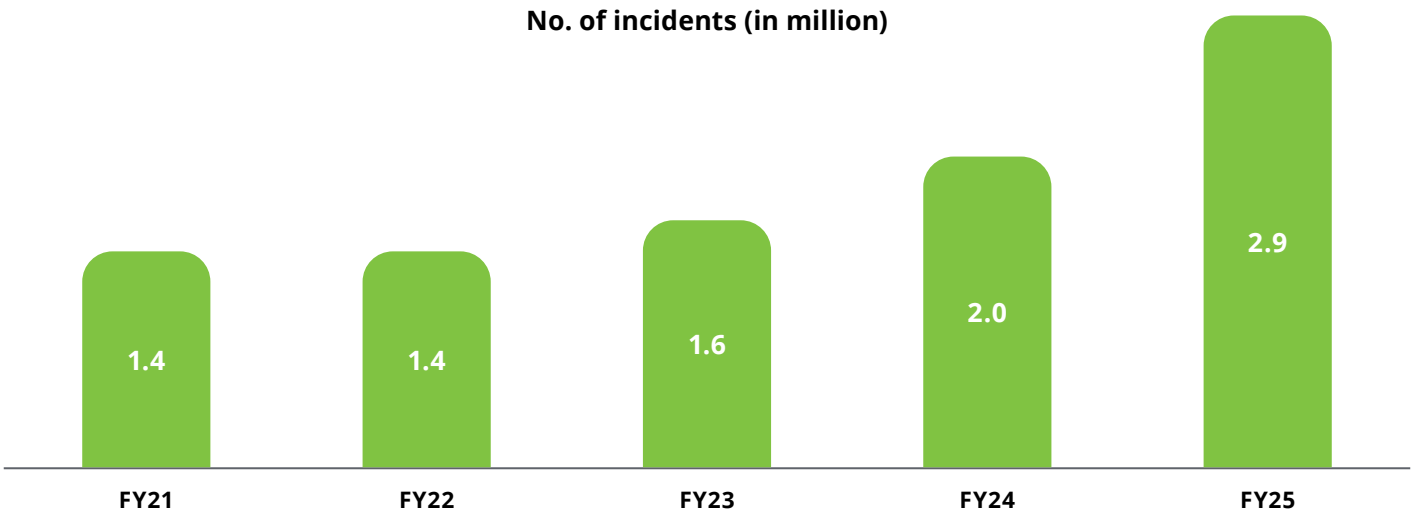
insurance, healthcare, e-commerce and government segments has caused cyberattacks to evolve beyond mere security breaches into sustained, systemic and operational risks. This high transaction volume, fragmented cyber maturity, expanding dependence on third parties and increased reliance on digital identities have firmly positioned India among the most cyber-exposed emerging digital economies.

Insurance is already an indicator of the changing trend due to rapid digitalisation; the number of policyholders is increasing, and financial and health data are moving through cloud platforms, APIs, intermediaries and an expanding ecosystem of collaborators. Several large-scale cyber incidents in FY2024–25 resulted in the breach of millions of customers' records, indicating that cyber risk is an ongoing operational issue rather than an episodic incident.[2]

More recently, several incidents across India's BFSI sector have exposed vulnerabilities in key financial infrastructure. In February 2025, cloud misconfiguration issues at a large retail stock-broking platform exposed the data of hundreds of thousands of customers to the dark web, resulting in a significant loss of market value. The threat environment continued to intensify in FY2026, with at least 116 data-related incidents recorded across India's financial sector in just six months between March and August, including 46 data breaches, 37 data leaks and 33 credit-card-related incidents. In one particularly concerning case, nearly 1 terabyte of data allegedly associated with a major Indian public-sector bank was advertised on the dark web, reportedly including customer records, identification documents, loan information and internet-banking data. These incidents are a testament to the growing vulnerability of cloud providers, shared tech providers and digital asset platforms in India's financial sector. Cyberthreats will continue to intensify and become more technologically sophisticated.[3,4]

According to CERT-In, the organisation tracks over two million cybersecurity incidents each year, ranging from malware infections to credential theft and network breaches. The rise of identity-led attacks, ransomware, API exploitation and attacks on financial institutions has increased the importance of rapid incident response. CERT-In requires specified cyber incidents to be reported within six hours of identification, supporting faster coordination and remediation.

Figure 6: CERT-In cyber incidents have doubled in four years

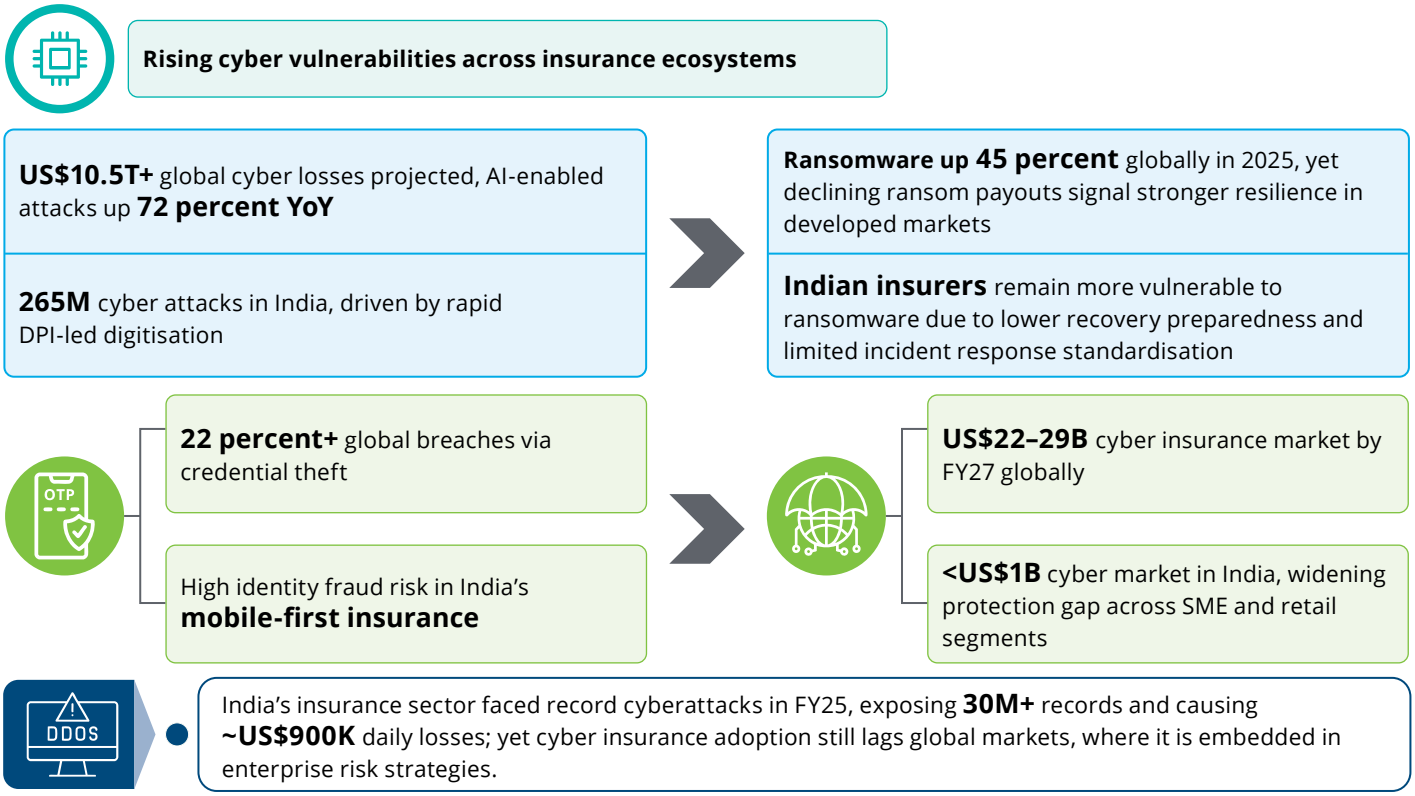


Source: CERT-In annual numbers 2025, CERT-In Annual Reports 2021-24

Attackers now rely more heavily on stolen credentials and compromised identities than on malware to breach enterprise systems. Security reports cite account compromise and software vulnerabilities as the most common forms of breach, and social engineering/human error as major contributors to ransomware attacks. For insurers, whose operating models increasingly depend on digital onboarding, customer authentication and ecosystem integrations, protecting digital identities is becoming as critical as securing network infrastructure.[5]

Geopolitical conflict further increases country-level cyber risk, as state-sponsored actors and hacktivists target government agencies, financial services and critical infrastructure. This was evident following the events of May 2025, when more than 1.5 million cyberattacks reportedly targeted Indian websites within two weeks. At the same time, cybercriminals' technical sophistication and organised scale are continuously increasing, with advancements such as AI-driven malware, automated phishing tools, deepfakes, synthetic identities and large-scale account takeovers that increase operational precision, enabling actors to attack faster and at greater scale. Ransomware, business email compromise, credential theft and identity-led attacks are still growing rapidly, and financial firms appear to be the primary targets because they hold concentrated critical data, digital identities and financial resources, making them a consistent focus for attackers.[6]

Figure 7: Cyber exposure in insurance: From growth to vulnerability



Source: Deloitte analysis, Cybersecurity statistics 2025, AI cybersecurity statistics 2025, Cyber risk: A look ahead to 2026, Cybercrime statistics 2026: Global losses and enterprise signals, Cyber insurance statistics 2026, India cyber insurance market report and forecast FY2026-34, Cyber breaches in Indian insurance sector 2025

The BFSI sector remains significantly vulnerable. RBI data indicates that digital payment fraud is rising, driven by social engineering and account takeover. This trend illustrates how increasingly complex digital systems are creating new attack vectors for sophisticated threat actors. As digital financial services evolve, attacks increasingly seek to disable access to payment credentials, accounts and authentication and onboarding methods rather than disrupt underlying infrastructure.

The financial impact is becoming increasingly significant. Industry estimates suggest cybercrime-related losses in India could exceed US$20 billion annually as digital payments, cloud adoption and interconnected systems continue to expand. At the same time, ransomware groups are intensifying multi-stage extortion campaigns targeting financial institutions, healthcare providers, technology companies and critical infrastructure, with business interruption emerging as one of the largest drivers of financial loss.[7,8]

Many successful attacks continue to exploit fundamental weaknesses rather than advanced technical vulnerabilities. These include misconfigurations in cloud deployment, weak credential management, inadequate third-party visibility and poor access controls. Insurers' reliance on cloud infrastructure, APIs, digital distribution channels and third parties creates systemic cyber exposure, as a vulnerability in one shared service can disrupt multiple functions or organisations. Interconnected dependencies, AI-driven attacks and escalating ransomware threats have therefore fundamentally reshaped the nature of cyber risk. The combination of interlocking dependencies, AI-driven attacks and rapidly escalating ransomware threats has fundamentally transformed the nature of cyber risk.

Cyber resilience is no longer confined to an IT discussion. It has become a strategic business imperative that must encompass the entire extended digital ecosystem of cloud providers, intermediaries and third-party vendors whose operations are critical to the success of the insurance value chain.

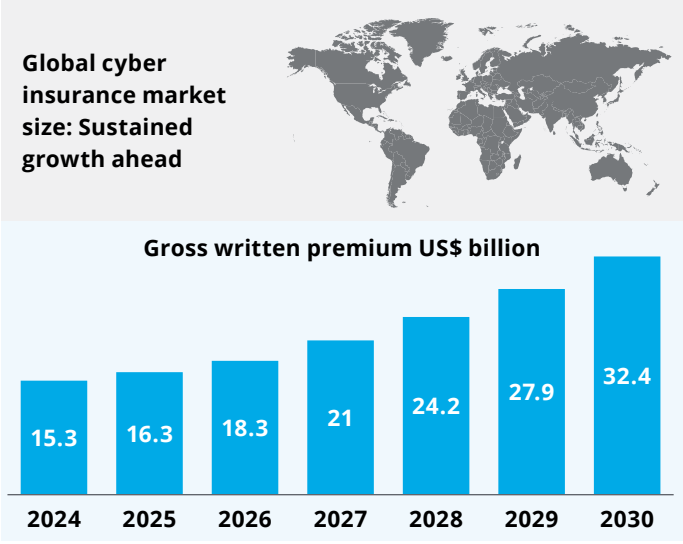
Cyber insurance is gaining prominence amid evolving regulatory expectations

Cyber insurance is becoming an important component of enterprise risk management and operational resilience as India's digital economy expands and regulatory expectations evolve. Greater use of cloud services, real-time payments, digital infrastructure, connected supply chains and data-dependent operating models has increased both cyber exposure and the potential financial consequences of disruption.

Evolving regulations concerning privacy, cybersecurity and operational resilience, particularly in financial services, are expected to further stimulate demand. Cyber insurance can provide financial protection against data breaches, cyber extortion, ransomware, business interruption and third-party liabilities. Cyber policyholders increasingly view coverage as part of a broader cyber-resilience strategy that complements cybersecurity investment, governance, business continuity and incident response.

Cyber insurers are also evolving from pure risk-transfer providers into active risk-management collaborators. In leading international markets, insurers increasingly bundle continuous vulnerability scanning, threat intelligence, ransomware response, digital forensics, legal advice and breach-coaching services with insurance coverage. This reflects a growing recognition that preventing and containing cyber incidents is more sustainable than relying solely on post-event indemnification. The global cyber insurance market is projected to nearly double from US$16.3 billion in 2025 to US$32.4 billion by 2030, representing a CAGR of approximately 14.8 percent. This growth is expected to be supported by wider adoption, increasing insured limits and expansion across emerging markets, although maturing underwriting, greater capacity and competitive pricing may moderate premium-rate growth.[9,10]

Figure 8: Global cyber insurance market growth trajectory



Source: Cyber insurance risks and trends report (2025 edition)

Growth is being driven by ransomware, phishing, data breaches, supply chain disruptions and AI-enabled attacks, including automated phishing and deepfakes. Increasing regulatory and disclosure requirements, along with a greater focus on operational resilience, are also supporting demand.

At the same time, competitive underwriting capacity and softer pricing in some markets may moderate premium growth. Future expansion is therefore likely to rely increasingly on wider adoption, higher insured limits, new geographies and greater policy volumes rather than price increases alone.

Insurers are using machine learning, external risk scoring and continuous monitoring to improve underwriting. They are also refining policy language, tightening exclusions and requiring stronger minimum cybersecurity controls.

Standalone and packaged cyber coverage are likely to coexist. Standalone policies remain important for large policyholders requiring tailored limits, business interruption protection and specialist incident response. Packaged products can widen adoption among mid-market and smaller policyholders by combining cyber protection with property, liability or other commercial insurance. Buyers must nevertheless understand the sublimits and exclusions applying to bundled cover.

India is following a similar trajectory from a smaller base. The domestic cyber insurance market is estimated at approximately US$115–255 million in FY25 and is projected

to reach US$321–594 million by FY30–31, implying a CAGR of about 18 percent–19 percent and expansion of approximately 2.3–2.8 times. Growth will be led by rising cyber incidents, cloud adoption, digital payments, data protection requirements and increasing demand from financial institutions, technology businesses, healthcare providers, digital platforms and MSMEs for modular coverage with incident-response support.[11,12,13]

Distribution through brokers, banks, digital aggregators and embedded collaborations may widen access, although affordability and minimum cybersecurity requirements could constrain adoption among smaller policyholders.

Insured limits are increasing

Demand is evident in growing policy volumes and higher levels of protection.

Aggregate insured limits in India are estimated to have grown by approximately 16–17 percent annually over the past three years. Some large banking policyholders almost doubled their limits between FY2024–25 and FY2025–26, with protection reaching US$50–100 million in certain cases. Compared with five to seven years earlier, limits for some large banking policyholders may be as much as ten times higher. Large technology and IT-enabled services policyholders have purchased limits of approximately US$200–300 million, reflecting exposure to operational disruption, data loss and third-party liabilities. Life sciences and pharmaceutical policyholders are also seeking higher protection against data breaches, privacy liabilities and business interruption. The rise in insured limits indicates that demand is deepening through both new policies and greater protection among digitally exposed sectors. It also reinforces the need to monitor concentration and accumulation risk.[14]

A substantial protection gap persists

Despite this growth, cyber insurance penetration remains below 1 percent of the global property and casualty insurance market, reflecting both supply- and demand-side constraints.[15]

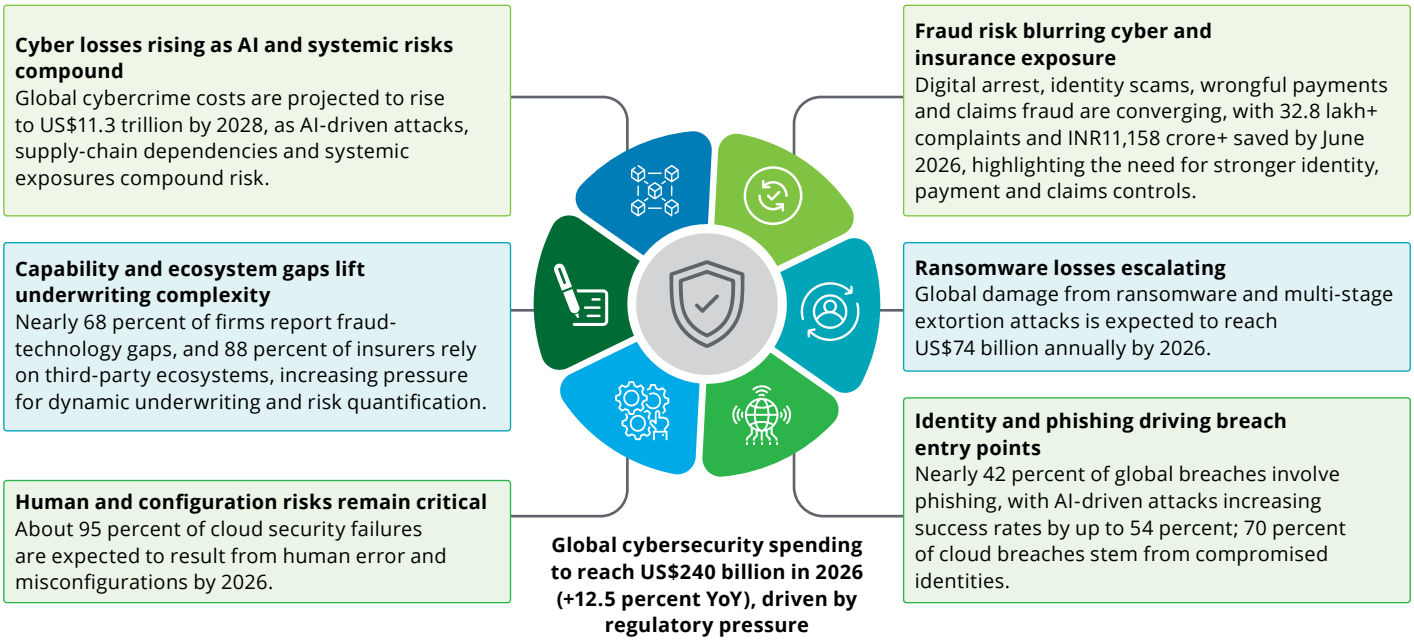
On the supply side, insurers continue to face limited historical loss data, modelling challenges and accumulation-risk concerns. On the demand side, firms, particularly SMEs, remain constrained by limited awareness, pricing concerns and uncertainty about policy coverage. As cyber exposure outpaces insurance capacity, the protection gap continues to widen. Global cyber claims have risen by 30–40 percent in recent years, driven primarily by ransomware, business interruption and data breaches, according to the National Association of Insurance Commissioners (NAIC) report on the cybersecurity insurance market in 2025.[16]

Improved underwriting discipline has helped maintain cyber insurance loss ratios below 50 percent. However, average cyber losses exceeded US$1 million per event in 2025, with business interruption now accounting for more than half of all claims, reinforcing the importance of resilience, business continuity and incident response capabilities in underwriting decisions.[17]

The opportunity lies in developing affordable, clearly worded coverage supported by risk engineering, incident response and effective claims capability.



Figure 9: Global cyber insurance trends

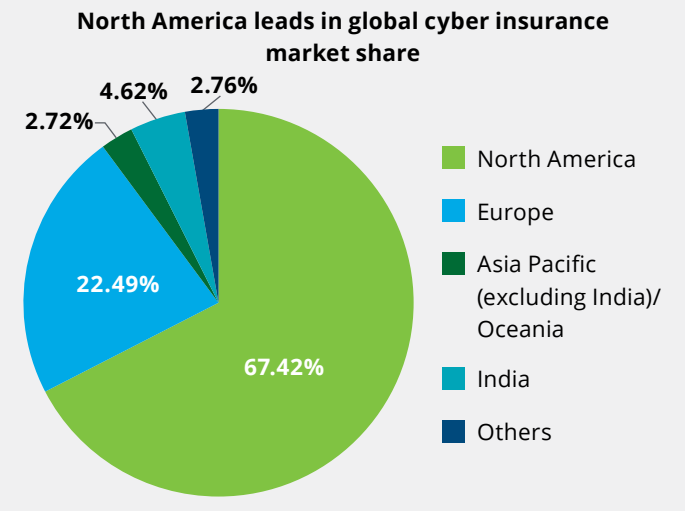


Source: Sentinel One, Experian, Global Cybersecurity Magazine, PIB

Global market concentration and India's emerging role

The global cyber insurance market remains concentrated. North America accounts for the largest share of premiums due to mature regulation, higher litigation exposure and stronger adoption. Europe follows, supported by stringent data-protection regimes, while Asia-Pacific represents a smaller but expanding share as digitalisation outpaces cyber-insurance maturity.[18]

Figure 10: Cyber insurance market: Skewed market structure



Source: Deloitte analysis, Cyber insurance risks and trends 2025, Industry research report based on secondary sources (India cyber insurance market size)

Within this landscape, India represents one of the world's largest long-term growth opportunities. As one of the fastest-growing digital economies and the world's third-largest economy by gross domestic product (GDP), measured at purchasing power parity (PPP), India continues to expand its digital public infrastructure. Yet cyber insurance penetration remains low despite rapid cloud adoption and real-time payments, reflecting a structural mismatch between rising cyber exposure and insurance adoption.[19]

Limited actuarial depth, evolving underwriting standards, low SME awareness and the perception of cyber insurance as a post-incident purchase continue to create a persistent "high exposure–low coverage" gap. This early stage of market maturity presents significant opportunities for intelligence-led underwriting, continuous cyber-risk monitoring and resilience-based insurance models. As cyberthreats become more sophisticated and ecosystem dependencies deepen, insurers face the dual challenge of strengthening their cyber resilience while developing cyber insurance as a sustainable line of business. Advanced cyber-risk analytics, continuous monitoring and more sophisticated underwriting will be critical to scaling the market without compromising profitability.

Time to consider cyber as a distinct reporting category

A review of the IRDAI Handbook on Indian Insurance Statistics 2024–25 and published non-life segment reporting indicates that cyber insurance is not separately reported as a standalone line of business comparable with motor or health. Cyber premiums and claims remain embedded within broader

non-life classifications, limiting visibility into the market's scale, claims experience and performance.[20]

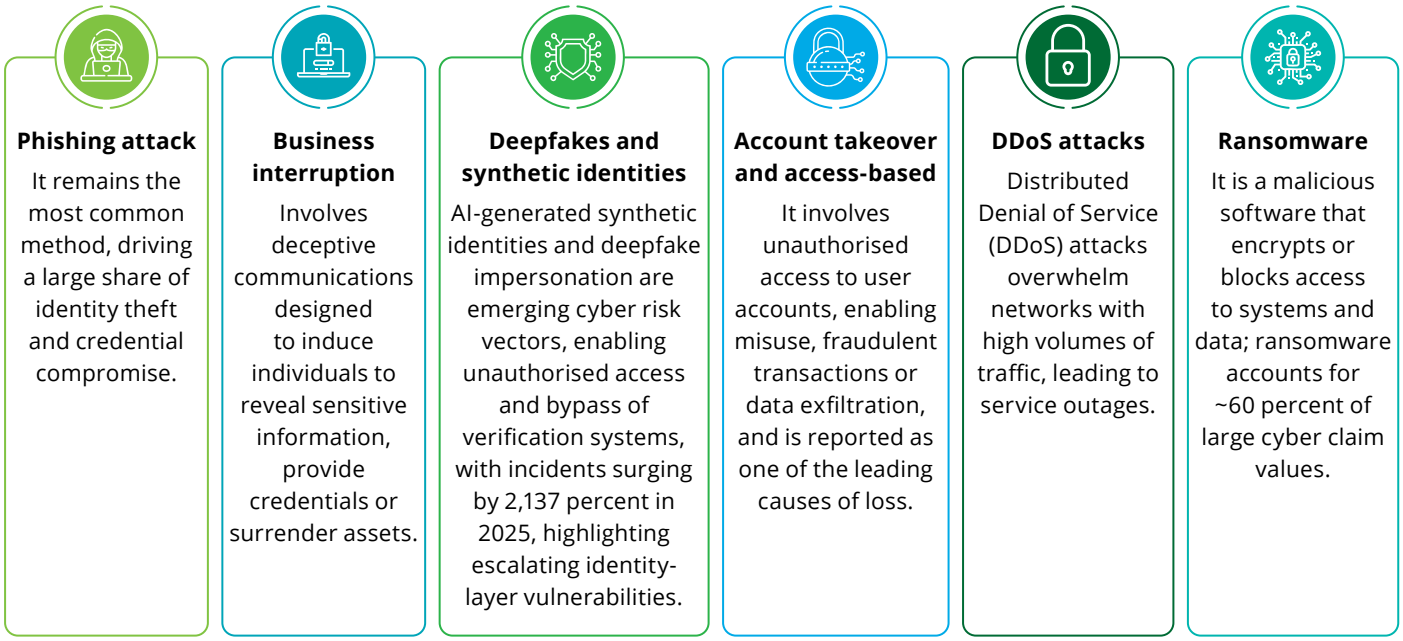
The time may have come to consider cyber insurance as a distinct reporting category, even if it is not immediately established as a separate statutory line of business. Dedicated disclosure of cyber premiums, insured limits, claims, loss ratios, sectoral concentration and accumulation exposure would improve transparency and build actuarial depth. Clearer reporting would help insurers price risks, support reinsurance capacity and develop suitable products for large policyholders and MSMEs. Separate reporting would help policymakers determine whether market growth reflects an increase in the number and diversity of insured businesses or primarily higher coverage limits purchased by a small group of buyers.

Cyber insurance is increasingly relevant to economic resilience because digital disruption can affect business continuity, customers, supply chains and critical services simultaneously. Greater regulatory visibility could support responsible market development while encouraging policyholders to invest in cyber preparedness.

Emerging risks and regulation are reshaping underwriting

Clearer regulatory reporting is only one part of developing a sustainable cyber insurance market. Insurers must also respond to a threat landscape shaped by ransomware, AI-enabled attacks, cloud concentration, supply chain dependencies and changing regulatory obligations. Together, these forces are redefining the risks that require coverage, the controls expected of policyholders and the information needed for effective underwriting.

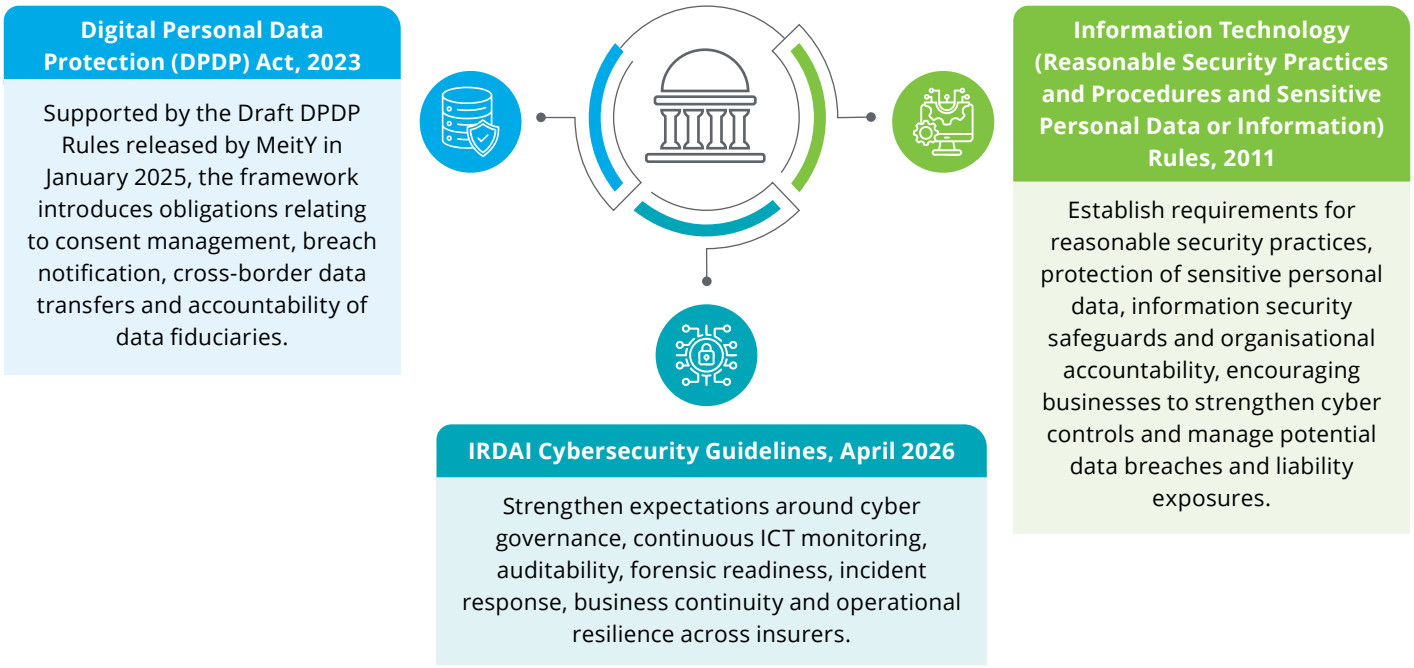
Figure 11: Emerging cyber risks in global insurance



Source: Cyber Insurance risk and trends 2025, Cyber security resilience 2025, Insurance Times, World Economic Forum, Fintech Intel

Evolving regulatory expectations are increasingly shaping demand for cyber insurance. Across major jurisdictions, frameworks such as the EU's Digital Operational Resilience Act (DORA), updated US cyber-incident disclosure requirements and sector-specific financial regulations are encouraging organisations to strengthen cyber governance, third-party risk management and operational resilience, driving greater adoption of cyber insurance alongside broader cybersecurity investments. India is following a similar trajectory through the CERT-In Directions, the Information Technology Rules, 2011 (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information), the Digital Personal Data Protection (DPDP) Act, 2023 and IRDAI's cyber governance expectations, collectively raising standards for incident reporting, data protection and enterprise resilience.

Figure 12: Key regulatory developments accelerating cyber insurance adoption



Source: PIB, IRDAI, Ministry of Communications and Information Technology

These developments are encouraging insurers to incorporate cyber maturity, governance, incident response preparedness and third-party risk into underwriting decisions. As underwriting becomes increasingly resilience-based, pricing and coverage will progressively reflect an insurer's ability to prevent, detect, respond to and recover from cyber incidents. Broader threat intelligence sharing, coordinated cyber exercises and public-private collaboration will further strengthen underwriting confidence while reducing systemic cyber risk.

MYTHOS: Frontier AI reshaping cyberthreats

Frontier AI and autonomous systems are shaping the next phase of cyber risk. AI-native threat models are enabling cybercriminals to automate reconnaissance, generate synthetic identities, deploy adaptive malware, execute large-scale impersonation attacks and orchestrate complex multi-stage cyber operations with unprecedented speed and sophistication. Unlike earlier automation-led attacks, frontier AI introduces autonomous reasoning capabilities that fundamentally change how vulnerabilities are discovered, exploited and weaponised. Industry demonstrations have shown that frontier AI systems can autonomously conduct sophisticated enterprise attack simulations at compute costs measured in tens of dollars. At the same time, smaller open-weight models have replicated exploit-generation capabilities at only a few cents per million tokens. As these capabilities diffuse into open-source ecosystems, advanced offensive cyber techniques are expected to become significantly more accessible.

The emergence of frontier AI models, such as Anthropic's MYTHOS in 2026, has intensified concerns around AI-native cyber risk. Demonstrations showed the ability to autonomously identify previously unknown vulnerabilities, generate exploit pathways and execute complex multi-step cyber operations across software environments. Industry assessments increasingly view this as a structural inflexion point where vulnerability discovery and exploit generation are beginning to operate at machine speed rather than human speed.[21]

This fundamentally changes the economics of cyberattacks. Vulnerabilities that previously required months of specialised research can potentially be identified within hours using AI-assisted systems. Industry estimates suggest that exploit development timelines could shrink by more than 90 percent, while enterprise remediation cycles for critical vulnerabilities still average over 30 days, significantly widening the discovery-to-remediation gap.[22]

At the same time, defenders are adopting AI-assisted threat hunting, code analysis and incident response, while threat actors are using similar capabilities to automate exploit

generation, reverse-engineer patches and compress the time between vulnerability disclosure and active exploitation. For insurers, this expands risk across identity systems, payment rails, customer authentication, onboarding and claims platforms. It also raises the likelihood of coordinated attacks spanning APIs, cloud infrastructure and enterprise networks.

The implications extend beyond cybersecurity operations. Frontier AI is expected to reshape cyber insurance underwriting, pricing, accumulation-risk modelling, incident-severity expectations and business-interruption assumptions. As autonomous cyber agents become more capable, the probability of systemic cyber events affecting multiple organisations through shared cloud infrastructure and software dependencies also increases materially. Open-weight frontier AI models are expected to further democratise advanced offensive cyber capabilities over the next few years, lowering barriers to sophisticated attacks and increasing risks from AI-generated ransomware, synthetic identity fraud, deepfake-enabled financial manipulation, automated account takeover and machine-scale phishing campaigns.

As vulnerability discovery accelerates at machine speed, traditional vulnerability-management approaches are becoming increasingly inadequate. Quarterly remediation cycles, fragmented governance and periodic testing frameworks are unlikely to keep pace. Insurers will increasingly require AI-enabled cyber-resilience architectures that combine continuous attack-surface monitoring, AI-assisted code auditing, real-time threat intelligence, agentic remediation and automated patch management. The next generation of cyber resilience will depend on AI-led detection and vulnerability discovery, agentic remediation and automated response orchestration, as well as continuous governance, validation and operational resilience at machine speed.



Chapter 2: How insurers assess and underwrite customer cyber risks

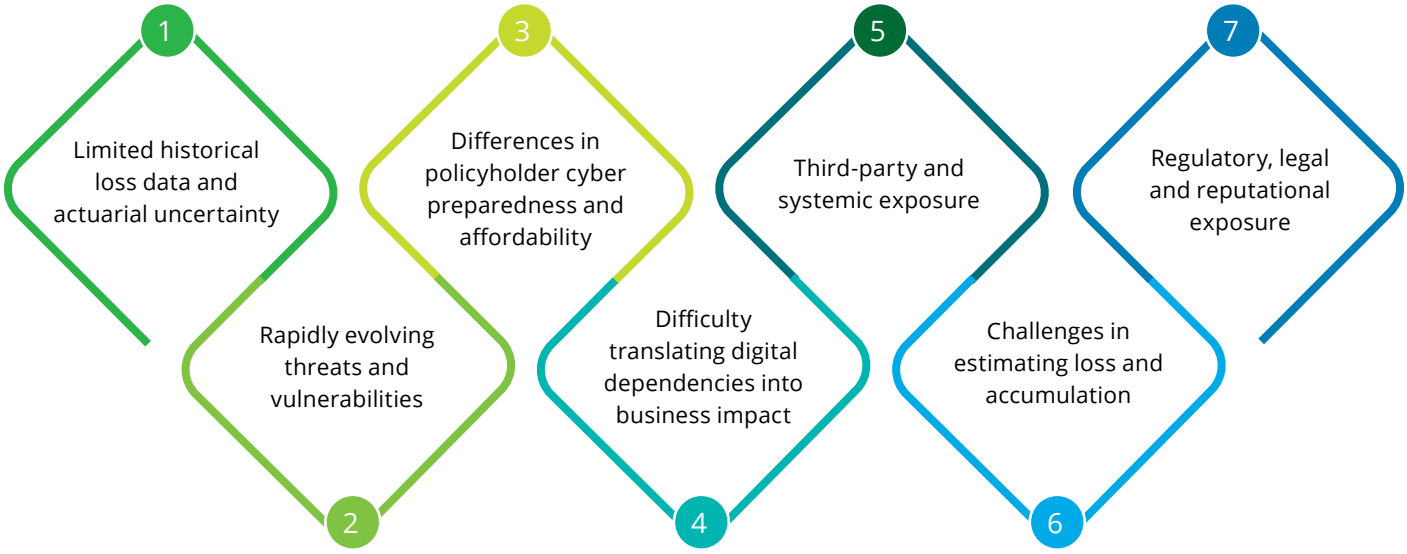
Compared with conventional insurance, cyber underwriting stands apart because cyber risk is constantly changing and inherently interdependent. Unlike physical assets or mortality risks, which have more clearly defined parameters, cyber risks are in constant flux, and a single vulnerability can have widespread implications for businesses across multiple industries. As insurers around the world embrace security-linked underwriting and continuous risk monitoring, the model of traditional underwriting, typically reliant on static, proposal-based assessment, is evolving to intelligence-led, real-time, and dynamic risk evaluation frameworks.

The Indian cyber-underwriting market is still developing. Limited actuarial depth, inconsistent incident-reporting data, varying policyholder cyber maturity and insufficient cyber-risk quantification make underwriting more complex. AI-enabled attacks, ransomware, identity compromise and ecosystem dependencies further increase uncertainty around pricing, coverage and accumulation risk. Indian insurers, therefore, need standardised underwriting frameworks that combine cyber intelligence, operational resilience, behavioural indicators and financial risk analysis.

Cyber insurance challenges and potential solutions

The core structural difficulty of cyber underwriting is quantifying, continuously assessing and accurately pricing a risk that can change materially during the policy period. Cyber exposure is shaped by technology, attacker capabilities, human behaviour, cloud adoption, third-party dependencies, regulatory expectations and the insured's evolving security posture. In India, these challenges are compounded by problems such as a lack of centralised, consolidated claims data, rapidly changing regulations, the infancy of cyber-risk models and a lack of integrated underwriting practices, all of which make it difficult for insurers to measure and accurately price exposure, estimate losses and maintain a viable business model.

These challenges are interconnected but distinct. They can be considered across the following seven areas:



Together, these factors explain why cyber underwriting is moving from predominantly historical, questionnaire-led assessment towards a data-driven, business-impact-oriented and continuously monitored model.

Limited historical data, actuarial depth and systemic accumulation risk

Cyber insurance is still maturing, constrained by limited, comparable and sufficiently granular historical loss data. Unlike mature insurance lines such as motor, property or life, cyber insurance does not yet have a long, stable claims history that can reliably establish loss distributions across sectors, attack types and exposure profiles. Claims experience is often fragmented across insurers, geographies and policy wordings, while the underlying risk itself continues to evolve.[23]

Absence of a comprehensive cyber-loss repository

A particular gap is the absence of a comprehensive, industry-wide repository that consistently captures the frequency, severity and economic impact of cyber incidents, particularly ransomware, business email compromise, data breaches and other high-severity events. Available information may not consistently record the full chain from initial attack vector and root cause through ransom demands or payments, business interruption, recovery costs, legal and regulatory expenses, reputational effects and the ultimate economic loss.

The challenge is compounded because much of this information is not readily shareable. Cyber incidents can involve commercially sensitive information, confidential security configurations, customer or employee data, legal considerations, ongoing investigations and potential reputational consequences. Policyholders may therefore be reluctant to disclose granular incident and loss information, while insurers may have limited ability to pool detailed claims experience across the market. Under-reporting and inconsistent incident reporting can further limit visibility into the causes and characteristics of losses. The result is a fragmented evidence base that makes it difficult to establish sufficiently deep, comparable and representative datasets for actuarial analysis.

Ransomware illustrates the challenge particularly clearly. Loss outcomes can vary significantly depending on the initial access vector, extent of network compromise, data exfiltration, backup resilience, business interruption, recovery time, ransom-related decisions and the involvement of third-party technology providers. Where claims experience is sparse, a small number of severe events can materially influence observed loss experience. At the same time, changes in attacker tactics can make historical ransomware claims less directly comparable with future events.[24]

For Indian insurers, the challenge is compounded by a still-maturing domestic cyber insurance market. Consolidated information on the frequency, severity, characteristics and economic consequences of ransomware and other cyber losses across industries remains limited. The absence of a standardised repository covering incidents, claims, loss components and recovery outcomes can constrain insurers' ability to benchmark risks consistently, establish reliable loss distributions and develop robust assumptions for pricing and reserves. More structured data-sharing mechanisms, supported by appropriate confidentiality, aggregation and governance arrangements, could progressively strengthen the industry's evidence base.

Changing risk environment limits the predictive value of historical data

The challenge arises from the scarcity of historical data and the changing nature of the risk reflected in that data. The past cyber environment cannot necessarily serve as a reliable proxy for the future because technology architectures, attacker capabilities, vulnerabilities and business dependencies evolve rapidly. New attack vectors can emerge within a relatively short period, while the adoption of cloud platforms, APIs, digital identities and interconnected ecosystems can materially alter an insurance company's exposure.

This creates a fundamental actuarial challenge, as even where historical claims data are available, the underlying risk-generating environment may no longer be comparable with the environment being priced.

Historical loss experience, therefore, remains an important foundation, but needs to be interpreted alongside forward-looking indicators of threat, exposure, business dependencies and potential impact.

Interconnectedness increases accumulation and systemic risk

The interconnected nature of cyber risk further strains traditional actuarial techniques. A single ransomware campaign, cloud outage, software vulnerability or supply chain compromise can trigger claims across multiple policyholders simultaneously. This introduces network effects and systemic correlations that are difficult to capture through conventional frequency-severity models.[25]

Unlike many traditional insurance risks, where losses can be modelled as relatively independent events, cyber events can propagate through common technology, infrastructure and service dependencies. The increasing use of AI-driven attacks, data breaches, identity compromise, cloud platforms and software supply chains can therefore create correlated losses across otherwise unrelated policyholders. Insurers need to

consider these network effects and evolving threat pathways alongside individual policyholder risk.

These accumulation effects also create challenges in estimating portfolio-level loss, reserve adequacy and potential catastrophic outcomes. The paucity of data on claims frequency, claim size, loss accumulation and catastrophic losses poses serious challenges to estimating reliable prices, ensuring reserve adequacy and building optimal cyber portfolios.

Moving from historical pricing to multifaceted risk assessment

The implication for pricing is that insurers need to supplement traditional actuarial approaches with forward-looking inputs. Rather than treating historical claims experience as the sole predictor of future losses, underwriting models can combine available loss data with threat intelligence, cyber telemetry, scenario analysis, predictive techniques, policyholder cyber maturity and estimates of potential business impact.

This does not imply replacing actuarial pricing with technology-led scoring. Rather, the objective is to strengthen actuarial models with additional evidence to capture emerging threats, changing exposures and systemic dependencies that historical claims experience may not adequately represent. Hybrid actuarial approaches that combine traditional techniques with machine-learning-based methods can help insurers extract greater predictive value from limited historical datasets, while allowing forward-looking indicators to reflect changes in the cyber-risk environment.[26]

For Indian insurers, this points towards a progressive shift from reliance on limited historical claims experience towards a broader evidence base. Alternative cyber datasets, global market experience, specialist modelling capabilities and structured collaborations with insurers, reinsurers and technology providers can help supplement domestic claims data as India's own cyber-loss repository and reporting practices mature.

Alternative cyber datasets Indian insurers can use

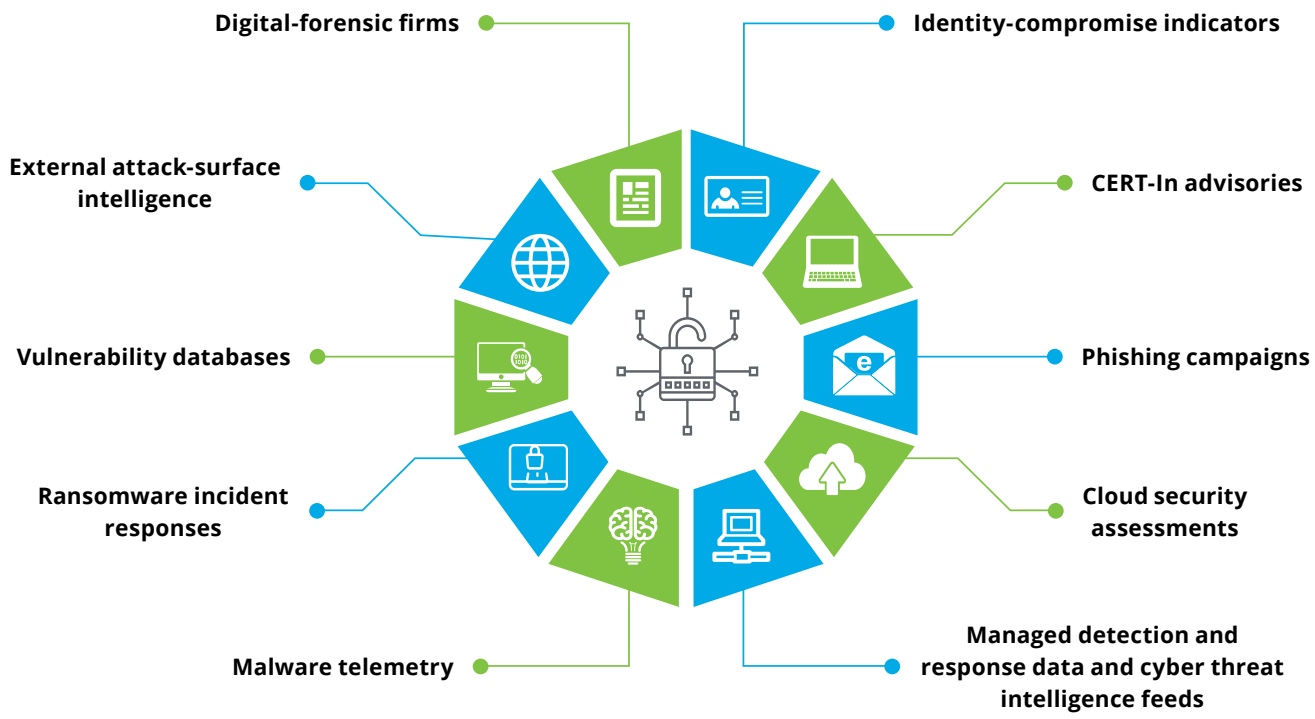
Where historical cyber-claims data are limited, Indian insurers can supplement available loss experience with alternative cyber datasets that provide more current visibility into policyholder exposure, threat behaviour and control effectiveness. International cyber-insurance markets provide useful examples of how insurers can combine claims experience with threat intelligence, security telemetry, external risk indicators and specialist cybersecurity data to strengthen underwriting. Indian insurers can draw on these approaches, data collaborations and analytical capabilities while adapting them to the availability, quality and regulatory requirements of the Indian market.

Relevant inputs can include data from Managed Detection and Response (MDR) providers, security operations centres, digital forensics and incident response firms, CERT-In advisories, vulnerability disclosure databases, cyber risk rating platforms and external attack surface intelligence. MDR and security operations data can provide particularly valuable evidence of changes in threat activity, endpoint exposure, identity compromise, suspicious behaviour and control effectiveness. Phishing and credential-compromise intelligence can further indicate changes in an organisation's exposure to social engineering and identity-based attacks. In contrast, evidence from phishing simulations or security-awareness assessments



can provide additional insight into human-related vulnerabilities where such information is available. These datasets are illustrated below:

Figure 13: Compensating for limited actuarial history



Source: Deloitte analysis

Forensic and incident-response data can provide insight into attack vectors, root causes, recovery periods and loss drivers, while vulnerability and external attack-surface data can help identify exposures that may not yet have resulted in claims. Cloud security telemetry can provide visibility into configuration weaknesses and changes in cloud exposure, while ransomware intelligence can help insurers understand emerging attack techniques, extortion patterns and sector-specific threats. These datasets can therefore complement, rather than replace, traditional claims experience and policyholder disclosures.

Global insurers and specialist cyber-risk providers can also provide a useful source of capability development for the Indian market. Their experience in integrating alternative datasets, developing cyber-risk scoring approaches, using external attack-surface monitoring and incorporating threat intelligence into underwriting can help Indian insurers identify relevant data sources and build more structured assessment models. Collaborations with global insurers, reinsurers, cybersecurity firms and technology providers could further enable access to international threat intelligence, benchmarking and analytical capabilities, while Indian insurers contribute local claims experience, sector knowledge and India-specific threat intelligence.

For Indian insurers, progressively integrating CERT-In advisories, sectoral incident reporting, cloud security telemetry, ransomware intelligence, cyber forensic findings, vulnerability disclosures, phishing and identity risk indicators, MDR data, and cyber risk intelligence platforms into underwriting and actuarial models could strengthen loss estimation and improve pricing consistency across industries. The use of such datasets should remain proportionate to the policyholder's size, sector and risk profile, with appropriate attention to data quality, consistency, privacy and validation before they are incorporated into pricing or coverage decisions.

Taken together, historical claims, forward-looking threat intelligence, policyholder maturity, business-impact analysis and portfolio-level accumulation modelling can provide a more robust basis for cyber pricing. This allows insurers to retain actuarial discipline while recognising that cyber risk is evolving faster than the historical datasets on which traditional actuarial models depend.

Parametric cyber frameworks relevant for Indian markets

Parametric cyber insurance represents an emerging risk-transfer approach that can complement conventional indemnity-based cyber cover, particularly for events where the occurrence, duration or severity of disruption can be measured objectively. Unlike conventional indemnity-based policies, which generally reimburse the policyholder for covered losses subject to the policy's terms and conditions, parametric structures provide a predefined payout when an agreed-upon and independently verifiable trigger is met. Potential triggers could include a prolonged cloud service failure, specified operational downtime, a defined denial-of-service event, widespread disruption to critical digital infrastructure or another objectively measurable cyber event.[27]

The approach is gaining attention in global cyber-insurance markets, particularly for business-interruption exposures. The Geneva Association notes that cyber insurers are increasingly exploring parametric and agreed-value solutions to speed up payouts for business-interruption losses, including structures linked to measurable events such as major cloud outages. At the same time, cyber-specific reference indices and standardised triggers remain relatively nascent, making reliable trigger design and benchmarking an important challenge.[28]

The model can reduce the need to establish and quantify every component of an actual loss, potentially enabling faster settlement and reducing claims-assessment complexity. This can be particularly relevant when a cyber incident causes significant operational disruption, but the resulting financial loss is difficult to measure promptly or to attribute precisely. At the same time, parametric structures introduce basis risk, as the predefined payout may not correspond exactly to the policyholder's actual economic loss. Trigger design, data quality, measurement methodology and independent verification are therefore critical to ensuring that the payout remains transparent and appropriately aligned with the exposure being transferred.

For India, the global experience provides a potential pathway to develop parametric solutions for exposures that can be measured with greater certainty. Initial applications could complement conventional cyber policies by covering objectively measurable events such as major cloud service disruptions, payment infrastructure outages, prolonged technology downtime, or defined interruptions affecting digitally dependent sectors. Hybrid structures could combine parametric protection for clearly measurable disruptions with conventional indemnity cover for losses requiring detailed assessment.

For Indian insurers, the opportunity is therefore not to replicate global parametric products directly, but to identify cyber exposures for which India has sufficiently reliable data, observable triggers and appropriate verification mechanisms. As the market develops, stronger incident reporting, cyber-loss repositories, threat intelligence and scenario-based modelling could improve the quality of triggers and benchmarks, while collaborations with global insurers, reinsurers and technology providers could provide access to international experience in product design and risk modelling. Parametric structures can consequently broaden the cyber risk-transfer toolkit, but should complement, not substitute for, stronger actuarial data, risk assessment and conventional cyber coverage.

Challenges in assessing threats and vulnerabilities

Cyberthreats are evolving faster than traditional underwriting methods. These include a rise in AI-driven attacks, Ransomware-as-a-Service (RaaS), markets for stolen credentials, deepfake impersonations and software supply-chain vulnerabilities, which continue to change the nature and scale of the cyber risk environment.

As these threats grow and become more complex, insurers are finding it increasingly challenging to accurately assess the likelihood and potential impact of a cyber incident. Cyber risk has transformed from a standalone concern into a pervasive issue across the entire insurance value chain, with interconnected digital systems amplifying risks such as identity theft, third-party dependence and AI-driven threat vectors.

The underwriting challenge involves identifying vulnerabilities, assessing their likelihood of exploitation and determining whether successful exploitation could cause a financially material event. Cyber risk is pervasive across the insurance value chain, with interconnected systems amplifying exposure to identity theft, third-party compromise, operational disruption and AI-enabled threat vectors. This makes it difficult for insurers to rely solely on proposal questionnaires and periodic reviews. External intelligence on vulnerabilities, exploitability, attack surfaces, identity risk and ecosystem dependencies is increasingly relevant to underwriting decisions.

From the viewpoint of a Chief Information Security Officer (CISO) and within the realm of enterprise risk management, cyber risk in insurance companies is complex and ever-changing. At the enterprise level, insurers face four primary categories of cyber risk, as outlined below:

Figure 14: Four pillars of enterprise cyber risk

Data compromise risk

Breach of sensitive personal, financial and health data, leading to regulatory penalties and reputational damage



Operational disruption risk

Attacks on policy administration, claims and other core systems resulting in business interruption

Identity-driven risk

Account takeover, credential theft and synthetic identities now among the primary attack vectors

Ecosystem risk

Third-party and vendor compromises across APIs, cloud environments and partner networks

Source: Deloitte analysis

The interconnected nature of these risks means that a compromise in one area can result in data theft, fraud, business interruption or broader operational disruption. Underwriting, therefore, needs to translate technical exposure into a measurable potential loss, considering the threat vector, the effectiveness of controls, the criticality of affected assets and the resulting financial consequences. In practice, threat assessment should bring together three perspectives covering existing vulnerabilities, their active exploitation and the potential business consequences of successful exploitation. This creates a stronger bridge between cyber intelligence and pricing decisions, reducing reliance on point-in-time technical assessments.

Gaps in assessing policyholder cyber preparedness

Cyber preparedness represents a separate underwriting consideration from the availability of historical loss data. Even when insurers have access to sufficient external threat intelligence, differences in policyholders' security maturity can materially affect the likelihood and potential severity of a cyber loss.

The underwriting process, therefore, needs to assess the prospective policyholder's ability to prevent, detect, respond to and recover from cyber incidents. This expands cyber underwriting beyond financial assessment to include operational robustness, governance capability, cyber hygiene and security architecture. Pricing, coverage limits and policy conditions can be influenced by the effectiveness of controls such as identity and access management, endpoint protection, privileged access management, vulnerability management, incident-response and ransomware preparedness. Prospective policyholders with similar revenues or technology investments may present markedly different cyber-risk profiles depending on governance maturity, third-party risk management, employee awareness, business continuity planning and cyber resilience.

A key underwriting question is therefore not simply whether a policyholder has security controls, but whether those controls are sufficiently effective and consistently implemented to reduce the probability and potential impact of a cyber event. The maturity of a business across ransomware preparedness, identity protection, external third-party risk and cloud security posture can provide important inputs for estimating potential business impact and determining appropriate underwriting terms. These factors should, however, be assessed alongside asset criticality, threat exposure and financial consequences rather than treated as standalone proxies for loss.[29]

The central challenge is translating these technical and operational capabilities into objective and measurable underwriting variables. Static proposal questionnaires generally provide only a point-in-time view and may not capture changes in controls, vulnerabilities or threat exposure during the policy period. A more mature underwriting approach may therefore combine initial assessments with updated risk information, control validation and evidence of resilience throughout the policy lifecycle.

Figure 15: Continuous underwriting and intelligence-led monitoring

From changing exposure to underwriting action

A four-step operating model for cyber risk telemetry

1. Detect
Identify material changes in exposure, including new vulnerabilities, exposed credentials, cloud-security gaps and third-party threats.

2. Assess
Determine relevance to the policyholder and portfolio, including exploitability.

3. Evaluate
Assess potential business impact, loss severity and portfolio accumulation.

4. Respond
Apply mitigation, risk engineering, enhanced monitoring or review coverage, terms and pricing during the policy term or at renewal, where appropriate.

Interpret telemetry through three questions
What changed? → Is it relevant and exploitable? → What could the consequences be?

By evaluating what has changed, its exploitability and its potential consequences, insurers can better understand business impact, loss severity and portfolio accumulation risk.

Source: Deloitte analysis

Continuous underwriting models relevant for Indian insurers

From periodic assessment to responsive underwriting

A phased, intelligence-led cycle that strengthens decisions without replacing underwriting judgement

Monitor risks
Track vulnerabilities, exposed credentials, cloud-security gaps and third-party threats using security data and external intelligence. Use these signals alongside policyholder disclosures and security assessments.

Prioritise exposures
Use AI and threat intelligence to identify material changes and critical hygiene gaps, with validation and underwriting oversight.

Leverage partnerships
Collaborate with cybersecurity providers for threat intelligence, security telemetry, incident insights and risk analytics. Insurers retain underwriting accountability.

Progress in phases
Begin with periodic reassessments across ransomware readiness, vulnerabilities, identity maturity, cloud security and third-party dependencies. Move towards more responsive coverage and pricing as capabilities mature.

Continuous learning
Feed incident, claims and remediation insights into future risk assessments.

Telemetry complements policyholder disclosures and underwriting judgement. Fully dynamic pricing remains a developing approach, dependent on data quality and cyber-data infrastructure maturity.

Global cyber-risk assessment frameworks relevant for India

Structured and repeatable assessment frameworks can provide insurers with a consistent reference for evaluating policyholder preparedness and control effectiveness.

The NIST Cybersecurity Framework (CSF) 2.0, CIS Controls and ISO/IEC 27001 can support assessment across governance, asset management, identity security, vulnerability management, threat detection, incident response, recovery, third-party risk and continuous improvement. NIST describes CSF 2.0 as a taxonomy of cybersecurity outcomes that can be used by insurance firms of different sizes and maturity levels, giving confidence in their overall cybersecurity strategy.[30]

Where greater maturity-level differentiation is required, insurers may also draw on CMMI-based cybersecurity maturity models as an additional reference. Such models can help distinguish between controls that exist only as documented practices and those that are consistently implemented, measured and improved.

These frameworks should be positioned within the underwriting process as reference standards rather than as separate underwriting methodologies. They primarily support the assessment of cyber maturity and control effectiveness, helping insurers establish a more consistent basis for evaluating policyholder preparedness. For Indian insurers, these international benchmarks can be supplemented by relevant Indian regulatory and sectoral expectations, including those of IRDAI and CERT-In. IRDAI's Information and Cyber Security Guidelines establish information and cybersecurity expectations for insurers while subsequent guidance addresses insurance intermediaries.

The frameworks can then be complemented by the Factor Analysis of Information Risk (FAIR), which provides a methodology for quantifying potential cyber losses and linking technical risk assessments to financial impact. The distinction is important because NIST CSF, CIS Controls and ISO/IEC 27001 help insurers understand the strength and consistency of controls, while FAIR helps connect those exposures to potential financial impact. These should remain complementary inputs rather than being presented as a single prescribed underwriting model.

For Indian insurers, the longer-term opportunity is to connect cybersecurity audits, maturity assessments and operational resilience indicators more directly to underwriting decisions. Instead of relying on a single maturity score, insurers can combine evidence of control effectiveness, resilience testing, incident-response preparedness and business continuity with the policyholder's threat exposure, asset criticality and digital dependencies. This provides a more rounded basis for differentiating risk without allowing any individual control, certification or benchmark to determine price or coverage independently.

The MSME preparedness and affordability loop

The challenge is particularly relevant for smaller businesses. MSMEs may have fewer resources to invest in specialised cybersecurity capabilities, dedicated information-security teams, advanced monitoring or resilience infrastructure. This can result in lower cyber maturity and greater underwriting uncertainty, which may translate into higher premiums, tighter coverage terms or additional risk-mitigation requirements. At the same time, higher insurance costs may reduce the willingness or ability of smaller businesses to purchase cyber cover or invest further in cybersecurity.

This creates a preparedness–affordability loop in which limited cybersecurity investment can increase exposure and underwriting costs, while higher insurance costs can constrain uptake and further investment in security, leaving the underlying risk insufficiently addressed. Breaking this loop may require insurers to combine maturity-based underwriting with practical remediation guidance, scalable coverage, risk-engineering support and security-linked incentives rather than relying primarily on higher premiums or tighter coverage.

Security-linked pricing

Evidence of stronger cyber maturity can increasingly serve as an input to differentiated underwriting terms. Cyber-risk engineering, independent security assessments and quantitative risk analysis can help insurers identify material control weaknesses and assess whether remediation measures have reduced the policyholder's risk profile.

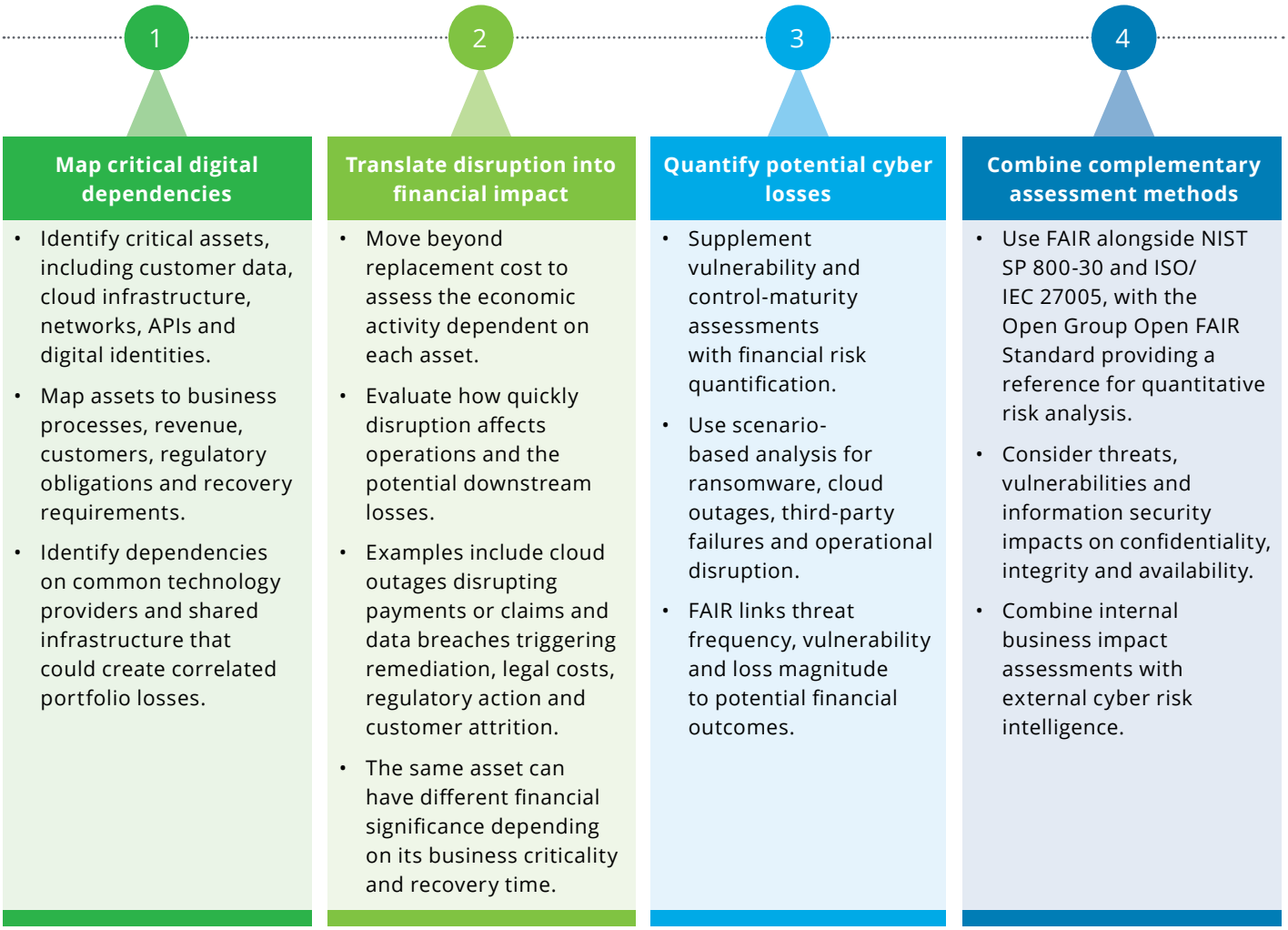
Global cyber-insurance practice is increasingly moving beyond self-declared compliance towards evidence-based assessment. Underwriting may incorporate validated information on privileged-access management, multifactor authentication, endpoint detection, ransomware resilience, incident-response testing and remediation progress. This enables underwriting terms to reflect demonstrated control effectiveness rather than the stated existence of a policy or technology alone.

For Indian insurers, demonstrable improvements in cyber maturity, independent assessments and operational resilience indicators could be progressively incorporated into underwriting decisions. Although India's cyber-insurance market remains at a relatively early stage, the progressive use of maturity assessments and independently validated security information can improve underwriting consistency while giving policyholders clearer incentives to invest in risk reduction. Depending on the broader risk assessment, such evidence may inform premiums, deductibles, coverage limits, sub-limits and policy conditions.

This can create a clearer relationship between measurable risk reduction and underwriting terms, while encouraging policyholders to strengthen their security posture. Security-linked pricing should therefore be viewed as an outcome of the broader maturity assessment rather than a separate assessment methodology. The objective is to translate evidence of stronger controls and improved resilience into more differentiated underwriting decisions, without treating any single control or framework as a standalone determinant of price or coverage.

Figure 16: Complexity in estimating the value of digital assets and business dependencies

From identifying critical dependencies to estimating financial losses



Source: Deloitte analysis

Underwriting implication

Estimate the financial consequences of compromise, unavailability or disruption rather than assigning a conventional value to every digital asset. Incorporate these loss scenarios into coverage terms, limits and pricing based on the asset's business criticality, recovery requirements and potential operational, financial and regulatory impact.

From traditional underwriting to intelligence-led cyber underwriting

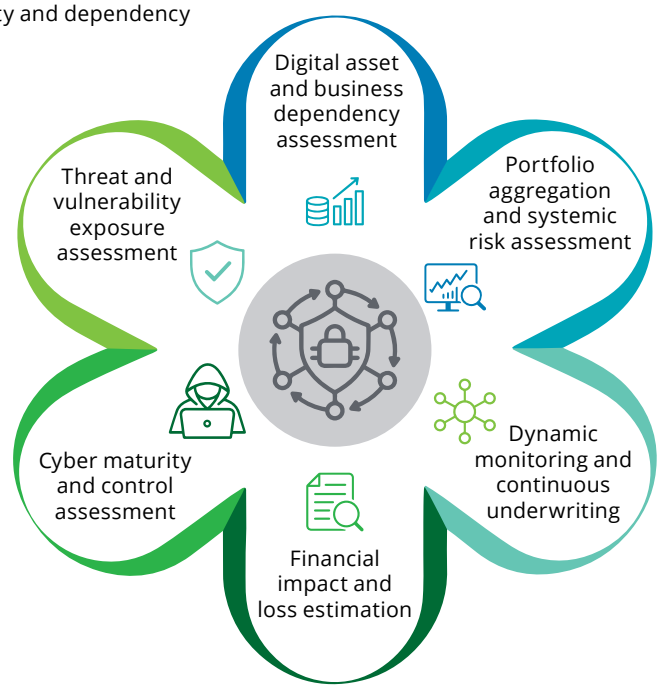
The challenges above can be brought together through an intelligence-led underwriting framework that integrates business dependency, threat exposure, cyber maturity, financial impact, continuous monitoring and portfolio accumulation to inform pricing, coverage, risk mitigation and portfolio decisions.

Figure 17: Building intelligence-led cyber underwriting frameworks

Understand what matters most to business
- Identify critical digital assets, systems and processes
- Map cloud, API, software and third-party dependencies
- Assess potential business interruption from technology disruption
- Classify assets by business criticality and dependency

Understand how the business could be attacked
- Assess ransomware, identity compromise and attack surface exposure
- Monitor exploited vulnerabilities and external exposure
- Evaluate cloud, third-party and software supply-chain risks
- Incorporate evolving threat intelligence into underwriting

Assess the strength of the insured's defences
- Evaluate governance and security-control maturity
- Assess identity security, vulnerability management and privileged access
- Review detection, response, backup and recovery capabilities
- Benchmark against NIST CSF, CIS controls and ISO/IEC 27001



Translate cyber exposure into potential loss
- Estimate ransomware, business interruption and recovery losses
- Assess legal, regulatory and reputational impacts
- Apply FAIR-based quantitative analysis and scenario modelling
- Evaluate potential severity and accumulation of losses

Understand how risks can accumulate across the book
- Identify concentration across cloud, software and technology providers
- Map common third-party and ecosystem dependencies
- Assess correlated exposure across sectors and policyholders
- Incorporate systemic and accumulation risk into portfolio decisions

Track how risk changes during the policy lifecycle
- Monitor changes in vulnerabilities, exposure and cyber posture
- Use cyber telemetry, threat intelligence and external risk signals
- Identify material deterioration or improvement in risk
- Enable responsive pricing, coverage and mitigation recommendations

Source: Deloitte analysis

The framework begins with an understanding of the business's critical digital assets and dependencies, followed by an assessment of external threat exposure and the effectiveness of cyber controls. These assessments can then be translated into potential financial, operational, legal and regulatory impacts. Continuous intelligence can refresh the assessment as exposure changes, while portfolio-level analysis can identify common dependencies and correlated loss scenarios.

The resulting assessment can feed directly into pricing, coverage, risk mitigation, claims preparedness and portfolio management throughout the policy lifecycle. The framework adds value by connecting technical exposure with business consequences and portfolio-level accumulation rather than assessing each dimension separately.

Global actuarial models adaptable for Indian cyber insurance

Traditional frequency-severity models remain useful for estimating how often cyber incidents occur and how severe the resulting losses may be, but they are insufficient on their own. Insurers increasingly combine these models with complementary techniques: Bayesian updating revises loss estimates as new evidence emerges; Monte Carlo simulations model thousands of possible loss scenarios to estimate potential outcomes; and network dependency analysis assesses how an incident affecting one organisation or cloud provider could spread across interconnected businesses. Machine-learning models and threat intelligence further help insurers adapt estimates to evolving ransomware tactics, cloud service disruptions and newly disclosed vulnerabilities. Recent actuarial research also supports combining conventional loss modelling with AI-based exposure assessment to improve cyber insurance pricing.[31,32]

For Indian insurers, the opportunity lies in building hybrid models that combine the limited historical claims data with alternative cyber-risk data and forward-looking scenarios. This can help reduce dependence on historical averages while maintaining actuarial discipline and making pricing more responsive to the current threat environment.

Difficulty in estimating cyber losses

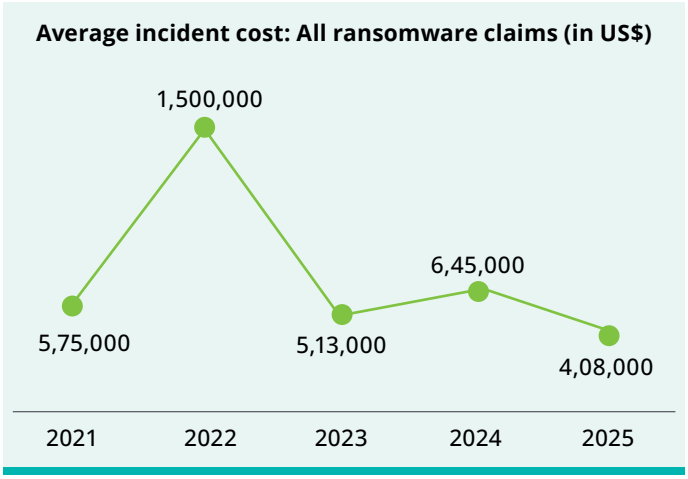
Cyber losses are multidimensional and can extend well beyond the immediate cost of technical remediation. A single incident can generate business-interruption losses, ransom or extortion costs, data-restoration expenses, forensic costs, regulatory investigations, litigation, customer compensation and third-party liabilities.

The sequence of loss can also extend over time. Initial operational disruption may be followed by identity compromise or fraud, legal and regulatory action, reputational damage and prolonged business interruption. The resulting loss depends on the initial event, the speed of detection, containment and recovery, the criticality of the affected systems and the organisation's ability to maintain or restore business operations.

Cloud providers, managed service providers and software supply chains can further create correlated losses across multiple organisations. A single disruption or vulnerability affecting a common technology provider may therefore generate simultaneous claims across policyholders, making Maximum Probable Loss (MPL), tail exposure and portfolio accumulation particularly difficult to estimate.

Ransomware illustrates the volatility of cyber losses particularly well. NetDiligence's 2026 Cyber Claims Study analyses 10,309 cyber-insurance claims from incidents occurring between 2021 and 2025. The study highlights the wide distribution of cyber losses, with large companies accounting for only 3 percent of claims but 56 percent of total incident costs, while ransomware and business email compromise together accounted for more than half of SME claims over the five-year period. Ransom demands reached as high as US$500 million and payments as high as US$90 million.[33]

Figure 18: Ransomware average incident costs trend in the last five years



Source: Cyber claims study 2026

The dataset should be viewed as an illustration of claims volatility rather than as a representation of the entire global cyber-insurance market. Other claims datasets report varying levels of ransomware frequency and severity, reflecting differences in policyholder populations, revenue segments, coverage and loss definitions. This variation itself reinforces the need for insurers to supplement historical claims experience with scenario analysis and forward-looking cyber-risk indicators.

Long-tail cyber losses also need to be incorporated into underwriting. The very large ransom demands and payments reported in the NetDiligence's 2026 Cyber Claims study illustrate the importance of modelling tail risk alongside expected losses, particularly where a single event can generate significant business interruption or correlated claims.

The implication for insurers is that claims experience should inform, but not determine, cyber pricing. Loss models need to combine historical claims with policyholder maturity, threat exposure, business impact assessment, recovery capability and systemic risk scenarios to estimate both expected loss and potential tail exposure.

Global cyber catastrophe models relevant for India

As cyber insurance portfolios expand, insurers are increasingly adopting cyber catastrophe (cyber-CAT) models to estimate potential losses arising from large-scale cyber events. Cyber catastrophe models adapt catastrophe-modelling principles to systemic digital events. They simulate scenarios such as widespread ransomware campaigns, cloud outages, software supply-chain compromises and attacks on critical infrastructure that may generate correlated losses across multiple policyholders.

Such models estimate losses using claims history, threat and vulnerability data, technological interdependencies, shared-provider concentrations and sector-level exposure. They can simulate major events such as ransomware attacks, cloud outages, software supply chain compromises and attacks on critical infrastructure.

The value of cyber-CAT modelling, therefore, extends beyond estimating the severity of an individual claim. It helps insurers understand accumulation and correlation risk, particularly where multiple insureds depend on the same technology providers, infrastructure or digital ecosystems. Current cyber-risk modelling approaches explicitly assess shared technology dependencies and portfolio concentration alongside event frequency, severity and tail risk.

For Indian insurers, catastrophe modelling can progressively incorporate sector-specific digital dependencies,

CERT-In information, cloud adoption, financial services interconnectedness and exposure to critical infrastructure. These inputs can help insurers identify concentration and accumulation risk, strengthen capital management and inform portfolio construction.

Global ransomware stress-testing models applicable to Indian underwriting

Ransomware stress testing provides a more targeted complement to catastrophe modelling by testing how individual policyholders and the wider portfolio could respond to severe but plausible ransomware scenarios.

A robust stress test can incorporate Probable Maximum Loss (PML), business interruption, recovery timelines, ransom-demand scenarios, operational effectiveness of backups, robustness of the incident-response plan, control over privileged access and the organisation's broader technology architecture and governance. Such exercises can also highlight portfolio concentrations in sensitive sectors such as healthcare, banking and finance, manufacturing and transportation, where a ransomware event could result in correlated losses across multiple insureds.

Security controls such as multi-factor authentication, privileged access management, Endpoint Detection and Response (EDR), an immutable backup strategy and tested disaster recovery plans can be incorporated as scenario variables. These variables test how differences in cyber preparedness could change loss outcomes under defined scenarios without duplicating the earlier maturity assessment.[34]

Cloud and technology aggregation represents a related portfolio-level challenge. Businesses may rely on the same cloud service providers, global software platforms, managed service providers and interconnected networks, creating the potential for a single disruption or software supply chain compromise to generate losses across multiple policyholders.

This portfolio perspective is particularly relevant where a common provider supports critical operations across multiple insureds. Understanding the concentration of such dependencies can help insurers assess correlated exposure, diversify risk and incorporate technology-driven accumulation into portfolio construction and capital management.

Faster containment and recovery are also important to limiting downstream financial losses. A shorter disruption period can reduce business-interruption losses and may also limit secondary consequences such as fraud, customer disruption and reputational damage. Ransomware stress testing can therefore connect technical preparedness and recovery capability with the potential financial severity of a portfolio loss.

For Indian insurers, these international practices provide a practical roadmap for strengthening cyber underwriting. Integrating ransomware preparedness, recovery maturity, backup validation, CERT-In intelligence, cloud security evaluations, cyber maturity indicators and operational resilience measures into scenario analysis can improve the assessment of both individual- and portfolio-level exposure.[35]

International reputational loss frameworks relevant for Indian insurers

Estimating cyber losses requires insurers to recognise that a cyber event can impose costs well beyond technical recovery expenses. Reputational damage, customer attrition, future revenue impact and declining stakeholder confidence can become significant components of total cyber losses, particularly for businesses whose revenues depend heavily on customer trust and uninterrupted digital services.

Consequently, loss-estimation approaches are increasingly expanding beyond direct technical and financial costs to consider the wider business consequences of a cyber event. Assessments can consider customer dependency, brand sensitivity, the policyholder's digitally enabled business model, contractual obligations and potential regulatory outcomes when evaluating the longer-term economic consequences of an incident.

Scenario modelling should therefore consider reputational impact alongside direct financial and operational losses, including extended business interruption, media attention, regulatory scrutiny, customer attrition and potential erosion of future revenues. The objective is to understand how reputational effects may translate into measurable economic consequences following a cyber event rather than assigning reputation a standalone monetary value.

This is particularly relevant for Indian policyholders across financial services, technology, insurance, healthcare and other digital industries, where customer trust and service continuity are increasingly central to business models. For insurers, incorporating these downstream effects into loss scenarios can provide a more complete view of an event's potential severity and reduce the risk of underestimating losses that emerge after the initial technical disruption.

Evolving approaches to cyber-loss estimation

The challenge of estimating cyber losses is therefore increasingly being addressed through a combination of historical claims, business impact assessment, scenario modelling, cyber catastrophe analysis, ransomware stress testing and forward-looking intelligence. These approaches

address different dimensions of the problem rather than representing competing methodologies. The price trends shown below provide a relatively practical proxy for the evolution of cyber risk exposure and loss intensity:

Figure 19: Why global cyber losses are becoming harder to underwrite

Growing complexity of cyber losses



- Small businesses globally pay ~**US$1,000** annually for US$1 million cyber coverage.
- Mid-sized firms pay **US$10,000–25,000** annually, reflecting risk exposure and security maturity.



- Ransomware remains one of the most expensive cyber claims, with average losses **~US$269,000** per incident in 2025.

Source: Blog-Cyber insurance costs

With a renewed focus on estimating and pricing risks related to business interruption, data leaks and accumulation, the industry is also shifting to scenario-based business interruption modelling, analysis of cloud exposure, identification of risk related to identity and data management and utilisation of AI. These approaches can improve the estimation of potential loss severity and support more informed pricing and reserve assumptions, while helping insurers identify systemic risks arising from interconnected policyholders.

The Indian cyber insurance market remains in an early stage of maturity, with underwriting and pricing significantly below those in mature global markets due to lower coverage limits, limited actuarial depth and evolving risk assessment capabilities, as indicated below:

Figure 20: Indian cyber insurance benchmarks

India's cyber insurance indicators



Indian SMEs typically pay between **INR18,000 and INR2 lakh annually** for cyber insurance coverage, depending on the insured businesses' sector exposure, turnover, digital dependency and cyber maturity levels.



Insurers are gradually beginning to differentiate pricing based on controls such as **multi-factor authentication, endpoint security, incident response readiness and cloud security posture,** signalling an early shift towards more dynamic, security-linked underwriting models.



Ransomware demands against Indian SMEs are now estimated to average between **INR15 lakh and INR80 lakh per incident,** alongside nearly **16 days of operational downtime** in many cases, making cyber insurance relevant as a business continuity and resilience mechanism across digitally dependent sectors.

Source: Deloitte analysis, Blog-Cyber insurance for Indian buyers

For India, the next stage of market development will require insurers to strengthen the underlying data, modelling and governance capabilities needed to support this evolution. Indian insurers will need to strengthen cyber-incident reporting, expand industry-wide cyber-loss repositories and develop more mature actuarial, catastrophe-modelling and cyber-risk quantification capabilities. These aspects will necessitate close collaboration among underwriting, claims, cyber forensics, threat intelligence and operational resilience departments to achieve more consistent pricing models and enable all risk managers to have visibility into the entire book of business.

Systemic cyber-risk accumulation will also require cooperation beyond individual insurers. Insurers, regulators, cloud service providers, cybersecurity providers and other ecosystem stakeholders will play an important role in improving visibility into common dependencies, incident patterns and emerging threats.

As the Indian market matures, integrating cyber-CAT modelling, ransomware stress testing and business impact assessment can provide a more comprehensive view of potential losses. Reputational and other downstream effects can then be incorporated into these scenarios where they have a measurable economic impact, rather than being treated as separate qualitative risks.

This integrated approach can help Indian insurers improve loss estimation, strengthen portfolio resilience and develop more consistent underwriting practices while supporting the sustainable expansion of cyber insurance.

Regulatory uncertainty and legal exposure

Cyber risks and the number of resultant security regulatory and legal events continue to rise. Cyber risk events no longer carry only technological recovery implications, as a growing percentage also have regulatory and legal dimensions that can far exceed mere technical losses. This extends to a wide range of privacy, mandatory reporting and legal issues, sector-specific compliance and inter-company, inter-state and inter-country disputes.

A single cyber incident can carry multiple regulatory and legal implications, and the legal regime surrounding cybersecurity is extremely dynamic and can also change frequently during an underwriting year.

The regulatory landscape has also expanded beyond data protection. Regulators now place increasing emphasis on operational resilience, cyber governance, third-party risk management, digital operational continuity, fraud prevention and timely incident reporting to avoid higher fines and penalties. As a result, insurers must assess a firm's cybersecurity controls and its ability to comply with evolving regulatory requirements throughout the policy period.

Global privacy-law underwriting models relevant for Indian insurers

The expansion of privacy and cyber regulation across major markets is making regulatory exposure increasingly relevant to cyber underwriting.

Global privacy regimes such as the EU General Data Protection Regulation (GDPR), California's CCPA/CPRA, Brazil's LGPD and Singapore's PDPA have established requirements regarding data governance, individual rights, accountability, breach management, and, in several cases, cross-border data transfers. Australia has also progressed privacy reforms, including the Privacy and Other Legislation Amendment Act 2024. Alongside privacy regulation, the EU's DORA, applicable to financial entities from January 2025, and the Network and Information Security (NIS2) Directive have broadened the regulatory focus towards ICT resilience, third-party dependencies, governance and incident reporting.[36, 37,38,39,40,41,42]

For Indian insurers, the regulatory landscape is similarly expanding. The DPDP Act, 2023 and the DPDP Rules, 2025, establish a new framework for digital personal data governance, with implementation phased across different provisions. CERT-In's directions require specified cyber incidents to be reported within prescribed timelines, while sectoral regulators have established additional requirements for cybersecurity, technology risk and resilience. IRDAI's Information and Cyber Security Guidelines set out requirements for insurers and insurance intermediaries. At the same time, RBI and SEBI have established corresponding IT, cyber resilience, outsourcing and cybersecurity requirements for entities within their respective regulatory frameworks.

This regulatory convergence is important for cyber underwriting because the same underlying cyber event can create different obligations depending on the policyholder's sector, the nature of the information involved and the jurisdictions in which it operates. Insurers, therefore, need to distinguish between enterprise-wide cyber controls and regulatory obligations specific to financial services, insurance, capital markets, payments or other regulated activities.

Cross-border cyber liability

Cross-border operations add another layer of complexity. Businesses increasingly rely on international cloud infrastructure, technology vendors and outsourced processing arrangements while serving customers across multiple jurisdictions. Following a cyber incident, legal

responsibility may therefore depend on where the data is stored, where affected individuals are located, which entity determines the purpose and means of processing, what contractual obligations apply and which regulators have enforcement jurisdiction.

Underwriting should consequently assess international data transfers, cloud-hosting locations, outsourced processing, contractual indemnities, notification requirements, allocation of liability among group entities and third parties and the organisation's ability to coordinate incident response across jurisdictions. The assessment should identify circumstances in which overlapping or conflicting regulatory requirements could materially increase the cost, duration or complexity of a cyber claim, without attempting to model every possible legal outcome.

Cross-border liability becomes particularly relevant when Indian insurers cover organisations that store or process personal data in multiple jurisdictions, use overseas cloud or technology providers, serve customers abroad or transfer data between group entities. Cross-border legal exposure can therefore feed into policy wording, coverage interpretation, claims preparedness, reserve assumptions and the assessment of potential regulatory and litigation costs.

Regulatory exposure modelling practices India can adopt

Regulatory and legal exposure can be incorporated into the broader loss-estimation process rather than treated as a standalone compliance checklist. Insurers can assess indicators such as privacy governance, regulatory reporting readiness, contractual risk allocation, third-party compliance oversight, data management practices, incident response governance and board-level accountability. Inputs from these will help insurance firms estimate the potential financial consequences of investigations, litigation, remediation, customer compensation and enforcement.

This approach can be strengthened through scenario-based regulatory stress testing. Scenarios could include a significant personal data breach, a prolonged disruption of a regulated service, a third-party incident affecting critical operations, a cross-border breach involving multiple notification regimes or an investigation following delayed or incomplete reporting. Assessing these scenarios can help insurers understand how technical, operational and regulatory factors interact to influence the ultimate loss, rather than relying primarily on point-in-time proposal questionnaires.

Regulatory intelligence is therefore becoming an important complement to technical cyber-risk intelligence. Changes in privacy requirements, reporting expectations, enforcement approaches, contractual arrangements or technology dependencies can alter the potential regulatory and legal exposure during the policy period. For insurers, maintaining visibility into these changes can support more responsive coverage decisions, loss assumptions and renewal assessments.

The underwriting response is also extending beyond pre-loss questionnaires to greater integration among insurers, policyholders, legal advisers, forensic specialists, incident responders and other ecosystem collaborators. Pre-loss support can include privacy and regulatory readiness assessments, contractual reviews, incident response planning and preparedness exercises. At the same time, post-incident engagements can provide information on legal costs, notification requirements, regulatory interactions and claims outcomes that can improve future loss assumptions.

For Indian insurers, the immediate opportunity is to build a structured regulatory-risk lens around the requirements most relevant to their policyholders. This could include DPDP compliance readiness, CERT-In reporting preparedness, sector-specific cyber and resilience requirements, third-party governance, contractual liability mapping, cross-border data exposure and broader regulatory maturity. These indicators should complement and not replace the technical cyber-maturity assessment.

Chapter 3: How insurance companies need to protect themselves against cyberattacks

With growing digitalisation and the convergence of insurance into an ever-expanding network of interdependent ecosystems, cyber risk has transitioned from a primarily technological challenge to an enterprise-level business risk. Insurance companies face an expanding attack surface due to the sensitive financial, medical and personal data they hold, their reliance on cloud infrastructure and APIs, and their growing networks of digital distribution collaborators, financial institutions, health networks and third-party suppliers. This increases their exposure to ransomware, identity fraud and API-based attacks. Synthetic identities and AI-based attacks have become more frequent and sophisticated, making cyber resilience for insurers critical to underwriting certainty, consumer trust, operational continuity and fraud prevention.

Cyberthreats and fraud have become inextricably linked, evolving into a new interconnected universe of fraud and cyber risk. In 2025–26, the global insurance and financial sector groups faced highly coordinated credential stuffing, ransomware and phishing attacks, as well as increasingly sophisticated AI-powered attacks that used deepfakes to target customer logins, service portals and payment systems. These incidents show that a cyberattack rarely remains a technology issue; it can quickly trigger fraud, identity misuse, financial loss and operational disruption across the insurance value chain.[43]

India is seeing a similar shift as digital onboarding, embedded insurance, instant servicing, cashless claims and digital payments expand. Government advisories during FY2025 also pointed to rising incidents of phishing, ransomware, credential theft and synthetic identity misuse across financial services. As insurers move towards near-real-time servicing and claims, cyber and fraud monitoring must work continuously across onboarding, underwriting, servicing, payments and claims, rather than as isolated controls.

Insurance fraud is increasingly cyber-enabled. Traditional fraud, such as fabricated claims, inflated medical bills, premium diversion and intermediary misconduct, is now facilitated by stolen credentials, breached customer data, deepfakes and AI-generated synthetic identities. Cyber compromise is often the entry point, with financial fraud as the downstream consequence. This exposes fragmented controls and underscores the need for integrated, intelligence-led models that combine cybersecurity, fraud, underwriting, claims and operational resilience within a unified enterprise risk architecture.

Best practices and frameworks: ISO and global cyber resilience standards

Many of the world's leading insurance companies are increasing the use of international cybersecurity standards and best practices to improve business governance, operational resilience and cybersecurity risk management across all operational segments. Compliance, rather than being seen as the goal itself, increasingly drives the embedding of cyber resilience across the board.

ISO/IEC 27001

It provides a structured framework for establishing Information Security Management Systems (ISMS), helping insurers strengthen governance over data protection, identity management, encryption, incident response, vendor oversight, business continuity and continuous monitoring. As insurers expand API-driven and cloud-based operating models, ISO-led governance increasingly supports consistent cyber controls, audit readiness and operational resilience across interconnected environments.[44]

ISO/IEC 42001: AI management systems

The growing adoption of AI across underwriting, claims management, fraud detection, customer service and decision-making calls for a framework to manage the resulting opportunities and risks. ISO/IEC 42001 provides a risk-based, objective-based management system approach to governing AI-related risks and opportunities. It supports insurers in formulating policies, processes and controls for the responsible development and use of AI, with emphasis placed on transparency, traceability, reliability and continued monitoring. ISO/IEC 42001 can complement existing information-security controls by strengthening transparency, traceability and accountability across the AI lifecycle, including the governance of AI models and AI-enabled agents.[45]

ISO 22301: Business continuity management systems

Cyber resilience also depends on an insurer's ability to maintain critical services and recover quickly when disruption occurs. ISO 22301 provides a structured Business Continuity Management System (BCMS) for identifying risks, preparing for disruptive incidents, maintaining continuity of critical insurance operations and supporting effective response and recovery. For insurers, this is particularly relevant to claims, payments, policy servicing and other customer-critical processes that increasingly depend on interconnected digital infrastructure and third-party ecosystems. Applying ISO 22301 alongside cybersecurity controls can help insurers move from preventing disruption alone towards broader operational resilience and recovery capability.[46]

ITIL: IT service management and operational resilience

Provides a structured approach to IT service management, helping insurers establish consistent practices for incident management, change enablement, service continuity, configuration management and continual improvement. For insurers operating increasingly through cloud platforms, APIs and interconnected third-party ecosystems, ITIL can complement cybersecurity standards by embedding resilience and control into day-to-day technology operations. Its practices can help strengthen incident response, minimise service disruption and support faster recovery, complementing frameworks such as ISO/IEC 27001, ISO 22301 and NIST CSF.[47]

NIST Cybersecurity Framework

The NIST Cybersecurity Framework is increasingly being used globally to build operational cyber resilience through five integrated functions comprising Identify, Protect, Detect, Respond and Recover. For insurers, this framework aligns closely with real-time fraud detection, cyber underwriting risk assessment, cloud and API security, ransomware preparedness, business continuity and the integration of security operations. Global insurers increasingly use NIST-aligned models to integrate cyber-risk intelligence directly into enterprise risk management and underwriting functions as cyber exposure becomes more systemic and interconnected across customer journeys and third-party ecosystems.

Zero-trust security architecture

Leading insurers are replacing perimeter-based security with zero-trust architectures, in which every user, device, application and API must be continuously verified. This approach reduces identity-related risks, limits lateral movement following compromise and strengthens protection across cloud-native, third-party and embedded insurance ecosystems.

AI-driven cyber defence frameworks

Insurers are increasingly deploying AI-led behavioural analytics, graph analytics, computer vision, voice analytics and anomaly detection to identify account takeover, synthetic identity fraud, document manipulation and coordinated fraud networks in real time. These capabilities enable continuous learning, improve fraud-detection accuracy and reduce investigation costs while supporting faster underwriting and claims decisions. Industry research increasingly highlights that AI-native fraud platforms significantly improve fraud-detection accuracy while reducing investigation costs, response times and operational leakage. They also enable insurers to process large volumes of transactional, behavioural, claims and identity-related data continuously across onboarding, servicing, underwriting, payments and claims ecosystems.[48]

Operational resilience and ecosystem security

Insurers rely heavily on third-party systems and data to deliver efficient real-time services, particularly for health insurance claims, keep pricing affordable and broaden the range and quality of their services to meet evolving customer needs. Consequently, insurers are strengthening cloud infrastructure security, API governance, application architecture, third-party risk management, ransomware protection and the integration of threat intelligence into day-to-day operations to manage systemic cyber exposure.[49] Leading insurers in India are increasingly investing in dedicated Security Operations Centres (SOCs), either in-house or through managed security service providers. As insurers expand their digital channels, cloud adoption, interconnected customer journeys and reliance on third-party ecosystems, a well-managed SOC is essential for providing 24/7 monitoring, threat detection, incident response and cyber-fraud intelligence. Strong SOC governance, skilled teams, clearly defined processes and continuous improvement enable insurers to identify and contain threats early, strengthen regulatory and operational resilience and prevent cyber incidents from escalating into business disruption, customer harm or financial loss.

Global investment priorities and India's rebalancing challenge

Worldwide, insurers are scaling up investment into AI-based fraud detection, cybersecurity solutions, behavioural authentication, identity intelligence, real-time threat surveillance and integrated analytics to gain a clearer, enterprise-wide overview of cyber risk. There is also a clear and rapid industry shift from simply detecting threats to predicting, containing and responding to them much more quickly. Those insurers that are adopting advanced detection, automation and response capabilities are observing faster threat identification, reduced breach costs and increased operational resilience.

While Indian insurers have embraced digital KYC, secure onboarding and claims analytics, their enterprise-level gaps include cross-business-unit integration, real-time cyber monitoring, user identity intelligence, continuous underwriting, AI governance and visibility into their supply chain and third-party risk. To close these gaps, the investment will need to shift from standalone technology to a connected approach to cyber risk capabilities, in which underwriting, servicing, claims, fraud management and cybersecurity are linked through a common intelligence layer. Given how rapidly contactless claims, embedded insurance and digital services are moving, this will be more important than ever. For health insurance, constant monitoring of behaviour and the use of AI-driven fraud analytics will become extremely important in the short- to medium-term to detect suspicious billing, identity fraud and coordinated attacks almost in real time. The gap illustrated below, comparing global maturity and India's current state, is therefore less about awareness and more about the depth of execution, integration and scale.

Figure 21: Urgent investment priorities: Global momentum versus India gap



Global cybercrime costs could reach **US$15.6T** by FY28–29, up from **US$10.5T** in FY24–25, driving proactive insurer investment; Indian insurers remain cost-sensitive, focusing on selective, high-ROI use cases such as claims analytics.

Cyber insurance claims frequency and severity are **surging** globally, improving pricing sophistication; India's limited claims history constrains actuarial depth and underwriting precision.

Global insurers are investing heavily in **cloud-native security and API protection;** Indian insurers face elevated exposure due to rapid digital expansion without equivalent runtime monitoring capabilities.

Investment focus is shifting towards identity security globally, with organisations prioritising **zero-trust models,** while Indian insurers continue to rely heavily on perimeter-based security, creating gaps in protecting distributed digital insurance journeys.

AI-driven cybersecurity tools are becoming mainstream, with phishing attacks increasing **over 1,200 percent** due to automation, pushing insurers globally towards real-time detection systems, while Indian firms are still transitioning from rule-based to adaptive AI systems.

Source: Deloitte analysis, 205 cybersecurity stats and facts for 2026, 64 cyber insurance claims statistics 2026, cyberinsurance market size and outlook, AI cyber security statistics 2025, Cyber risk: A look ahead to 2026

Cyber resilience is truly transitioning from a technology-based capability to a strategic one. With cyberthreats becoming more intertwined, complex and AI-driven, insurers must integrate cybersecurity across underwriting, fraud management, claims, operations and Enterprise Risk Management by migrating from isolated controls to connected security capabilities underpinned by AI-powered vigilance, unified data architectures and ongoing cyber intelligence.

Insurers that make this transition can mitigate risks more effectively, build customer trust, improve underwriting decisions and strengthen resilience across their operations and the broader insurance value chain.

Chapter 4: Regulations: IRDAI guidelines, DPDP Act, IT Act and CERT-In advisories

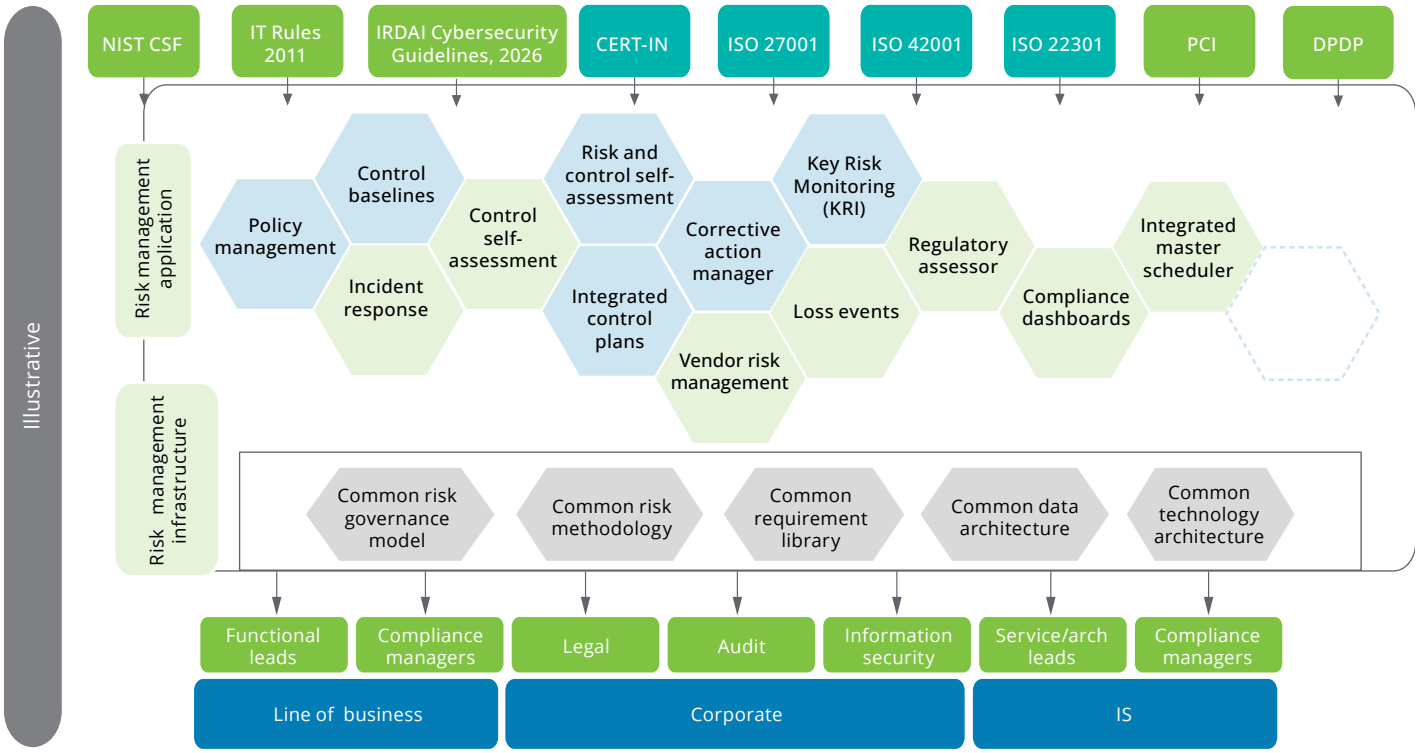
Regulatory expectations in the insurance sector are expanding across cybersecurity, data protection, operational resilience, AI governance, third-party risk and incident reporting to promote cyber resilience. In India, the regulatory landscape has shifted its focus from compliance controls towards accountability, continuous monitoring, faster incident reporting and measurable operational resilience. Globally, regulators from Europe to the US are similarly embedding cyber resilience into financial stability, operational continuity and customer protection.

As insurers navigate a growing number of regulatory obligations, compliance is increasingly becoming about integrating a range of mandates, not just following dictates set by specific legislation. It is shaped by a combination of regulations, industry standards and internal governance requirements, creating increasingly diverse compliance obligations across the enterprise. Many insurers managing compliance obligations independently face duplicated controls, fragmented governance and inconsistent risk oversight.

To address this complexity, insurers require a holistic approach that simplifies compliance while strengthening enterprise-wide governance. Deloitte's Integrated Compliance and Risk Management (ICRM) Framework, therefore, provides this foundation by enabling insurers to align regulatory obligations, industry standards and internal compliance requirements through a common governance and risk management structure. By integrating regulations, industry best practices and the insurer's internal policies and procedures through a centralised framework, insurers can manage compliance as a cohesive unit rather than as independent obligations, thereby lowering costs, optimising governance and ensuring a centralised approach to risk.

Figure 22: Integrated Compliance and Risk Management (ICRM) Framework

Diverse compliance requirements are a result of regulations, industry standards and internal compliance requirements. A holistic approach is needed that simplifies compliance with these diverse requirements.



Source: Deloitte analysis

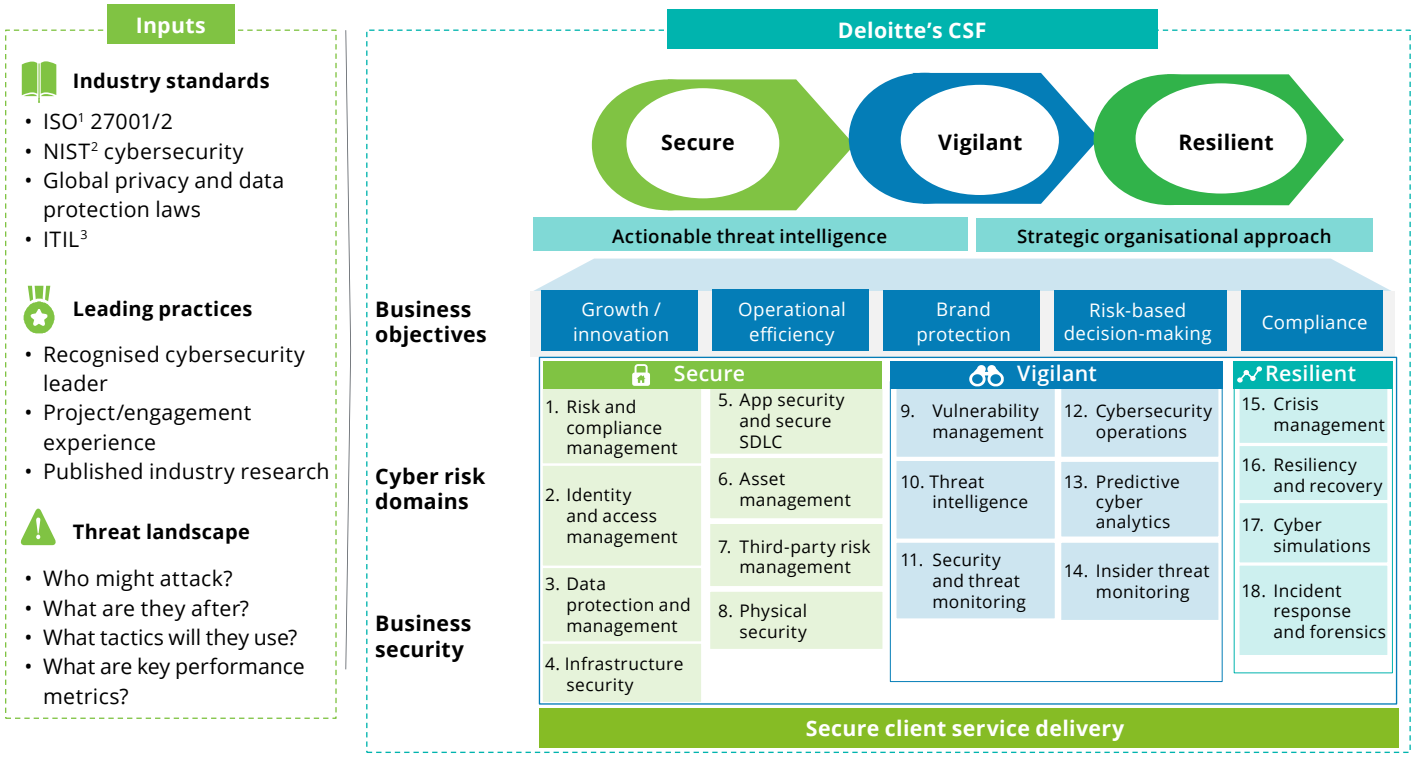


Building on this governance layer, insurers need a clear operational framework to translate regulatory and risk obligations into on-demand cybersecurity and resilience capabilities. Deloitte's Secure-Vigilant-Resilient (SVR) framework connects preventive controls, continuous monitoring and operational resilience into an overarching cybersecurity infrastructure.

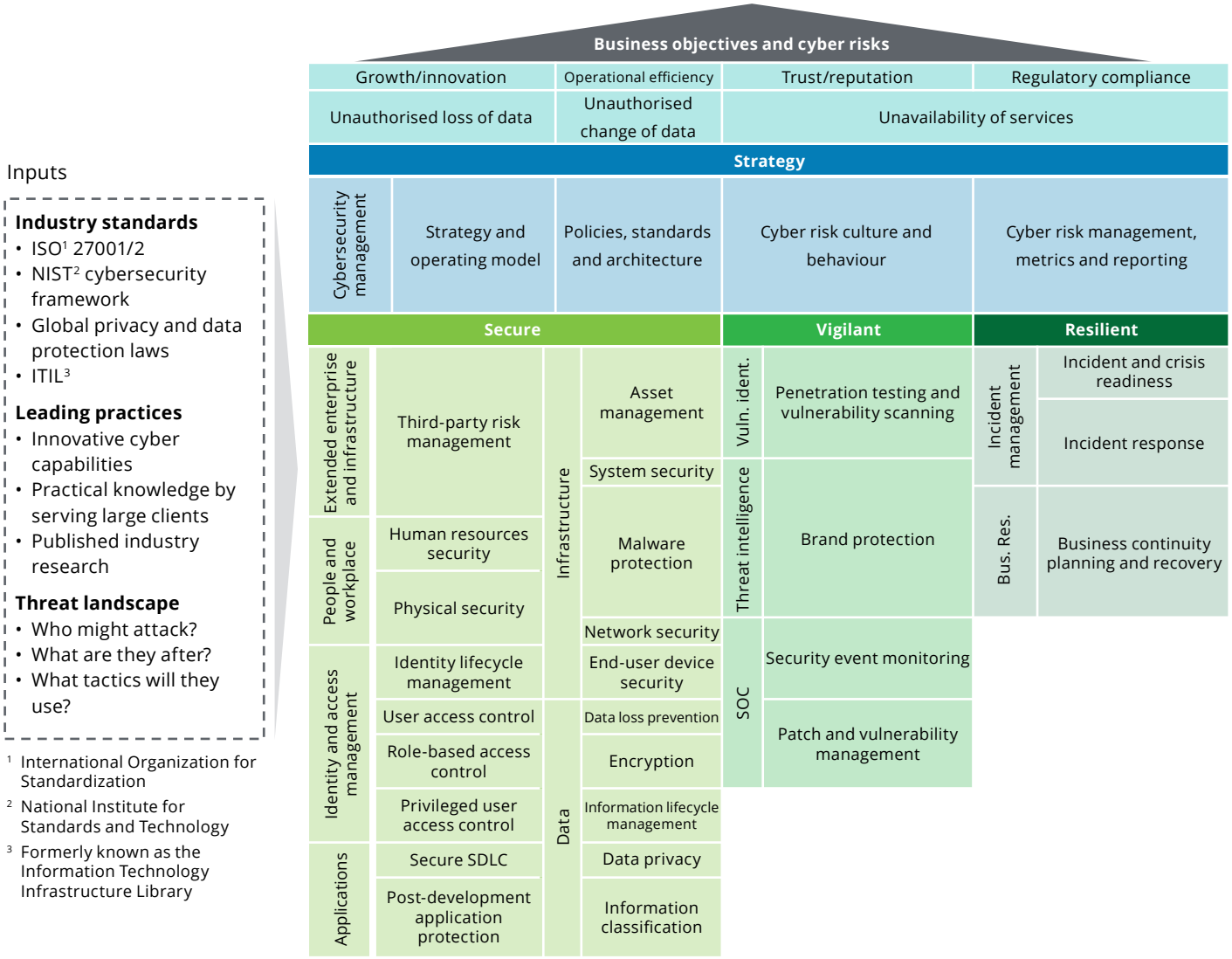
The combination of the ICRM and SVR frameworks helps insurers meet diverse regulatory obligations and strengthen cyber resilience through a unified and scalable operating model.

Figure 23: Deloitte's Cyber Security Framework (CSF)

Deloitte's cyber risk framework incorporates key cybersecurity areas and is built on industry-leading practices and regulatory expectations.



Source: Deloitte analysis



[1] International Organization for Standardization

[2] National Institute for Standards and Technology

[3] Formerly known as the Information Technology Infrastructure Library

Source: Deloitte analysis

Together, these frameworks provide the foundation for responding to today's evolving regulatory landscape. While the Deloitte ICRM Framework integrates heterogeneous compliance obligations into a unified, comprehensive framework to support effective governance and compliance management, the Deloitte SVR Framework operationalises those regulatory requirements through integrated cyber resilience capability components of the operating model. Against this backdrop, insurers must align their operating models with the key regulatory and supervisory expectations shaping the sector.

IRDAI cyber insurance and cybersecurity guidelines

Notified by the IRDAI on 24 March 2025 and updated in April 2026, the guidelines mark an important step towards improved cybersecurity governance within the Indian insurance sector.[50]

The guidelines treat cybersecurity as a strategic business priority rather than an IT or compliance issue, demanding board-level governance, enterprise-wide accountability and the integration of risk management, thereby contributing to greater resilience and security. The updated regulatory framework strengthens governance and establishes more structured operational requirements for data classification, secure system development, cloud governance, remote work security, continuous monitoring, independent auditing, external oversight and cyber resilience. Security has become a major component throughout the technology life cycle, comprising system design, access controls, incident response, recovery and continual improvement processes, illustrating a shift towards a more proactive, risk-oriented regulatory paradigm. In addition, increased emphasis is placed on consistent monitoring of cyber risk, prompt incident reporting, business continuity planning and safeguarding policyholder data.

As insurers increasingly rely on cloud providers, APIs, Third-Party Administrators (TPAs), healthcare providers and digital collaborators, cyber risk is no longer confined within organisational boundaries. Consequently, regulatory expectations extend beyond domestic technology controls to include governance of the entire insurance ecosystem.

The guidelines also recognise the growing intersection between cyber resilience and fraud management, driven by the increasing overlap among identity compromise, ransomware, cyber-enabled fraud and operational outages stemming from common vulnerabilities. This direction aligns closely with global regulatory trends. Established frameworks such as the U.K. Prudential Regulation Authority's Operational Resilience regime require financial institutions to maintain critical services even amid cyber incidents or operational outages. Likewise, the IRDAI is positioning cybersecurity as a vital element of integrated enterprise risk management, operational resilience and board-level governance, rather than a solitary IT issue. These trends suggest a broad shift from compliance-driven cybersecurity to a resilience-focused approach, encouraging insurers to integrate cyber resilience, continuous monitoring, third-party oversight and an enterprise-wide governance strategy to enhance operational resilience and protect policyholder data in today's interconnected digital environments.[51]

Digital Personal Data Protection Act (DPDP Act), 2023

The DPDP Rules, 2025, notified on 14 November 2025, implement the DPDP Act, 2023, which lays down a comprehensive regulatory framework encompassing consent management, security safeguards, breach notification, cross-border data transfers and organisational accountability. In the insurance industry, the DPDP Rules have a direct impact on digital onboarding processes, underwriting standards (which must comply with the Act), the claims management process, the collection and use of health data, the operation of AI systems and the management of third-party data-sharing arrangements. As AI becomes embedded across underwriting, claims and other core insurance processes, governance must extend beyond privacy compliance to encompass trusted data, explainable AI, model accountability, enterprise-wide oversight, security and fraud monitoring. By incorporating the capabilities prescribed under the DPDP Rules into their operating models, insurers will be better positioned to expand their use of AI securely, thereby improving customer trust, regulatory confidence and cyber resilience.[52]

Information Technology Rules, 2011

The Information Technology Act, 2000, laid the foundation for India's legal framework governing electronic transactions, cyber offences and protection of digital information. Building on this foundation, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, issued under Section 43A, introduced more specific requirements for handling sensitive personal information, including financial, health and biometric data. These include obtaining consent for collection, stating the purpose and manner of use, maintaining a privacy policy, enabling individuals to review and correct their information, restricting disclosure and transfer subject to specified conditions and implementing documented reasonable security practices to protect information from unauthorised access, use or disclosure. For insurers, these requirements are particularly relevant given the volume and sensitivity of customer and health information handled across digital platforms, intermediaries and third parties. As cyber risks increasingly extend across insurers, intermediaries, technology providers and customers, the Act and associated Rules provide an important legal foundation for data security, accountability, incident management and evidence management across the wider insurance value chain.[53]

PCI DSS – Payment card security

The Payment Card Industry Data Security Standard (PCI DSS) provides a baseline of technical and operational controls for protecting payment-card data. For insurers, its relevance is increasing as premium payments, renewals and other customer transactions move through digital channels and involve payment gateways, banks and third-party service providers. PCI DSS covers areas such as access controls, protection of cardholder data, secure transmission, vulnerability management, monitoring and incident response. It also extends to service providers that can affect the security of payment-card environments, making third-party oversight an important part of the control framework. For insurers, applying PCI DSS where cardholder data is within scope can strengthen payment security, reduce exposure to payment-related cyber incidents and complement broader cybersecurity and fraud controls across digital insurance journeys.[54]

CERT-In advisories and incident-reporting expectations

In alignment with CERT-In's efforts, regulatory expectations for the timely reporting of cyber incidents, threat intel sharing, ransomware preparedness, security monitoring, log retention and coordinated response are becoming increasingly rigorous. Recent advisories focus on emerging threats from phishing, compromised credentials, ransomware, cloud infrastructure vulnerabilities, AI-powered social engineering and supply chain attacks. These expectations require insurers to implement integrated monitoring capabilities and employ cyber-fraud intelligence across all stages of underwriting, claims, customer service and payment processes, as well as in relation to third-party engagements. Rather than relying on disparate security monitoring functions, insurers will need to develop agile, interconnected operating models to identify and respond to cyberthreats in near real time.[55]

Governance, accountability and operational resilience

Globally, cyber regulation is moving beyond policy documentation towards demonstrable operational resilience. Regulatory bodies are placing greater emphasis on board-level accountability, continuous security monitoring, AI governance, incident readiness, third-party oversight, ecosystem resilience and the integration of cyber risk within overall enterprise risk management. Illustrative examples of this evolving paradigm include the EU's DORA and the US Securities and Exchange Commission's (SEC) requirements for cyber incident disclosure. DORA signals a move from compliance to demonstrable resilience, requiring insurers to strengthen their ability to withstand, respond to and recover from cyber disruptions while managing risks arising from critical technology and third-party providers.[56] The US SEC's four-day cyber-incident disclosure requirement similarly reinforces greater transparency, executive accountability and timely reporting of material cyber events.[57]

For Indian insurers, the current landscape is increasingly defined by operational rather than regulatory challenges. The ability to achieve sustained compliance will hinge upon the integrated functionality of cyber governance, fraud management, operational resilience and enterprise risk management, supported by continuous monitoring, shared intel and dynamic controls. The incorporation of these capabilities into their business operations will enable insurers to meet ongoing regulatory expectations and cultivate customer trust and long-term business sustainability.

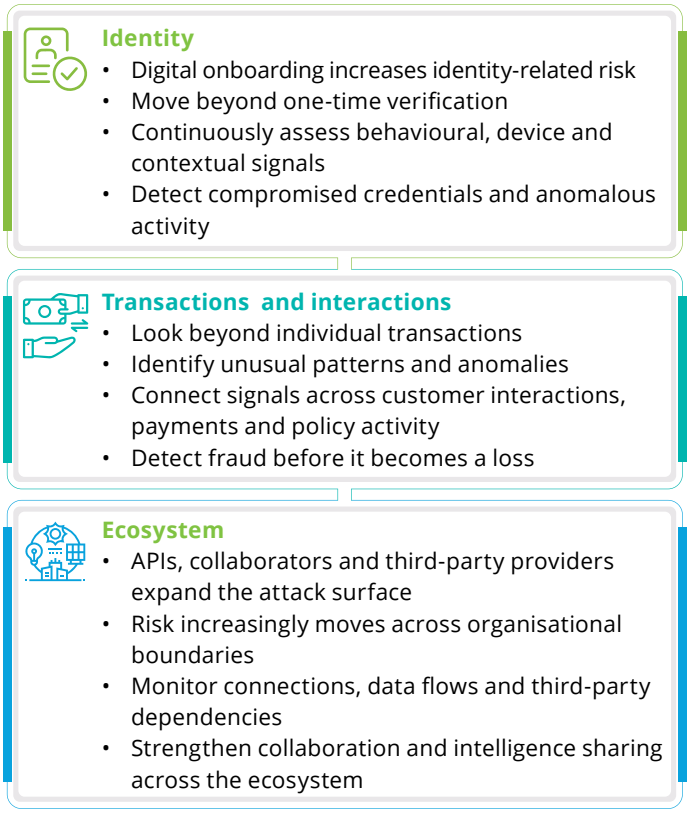


Conclusion: Building a resilient digital insurance ecosystem

As insurers digitalise operations, expand API-driven ecosystems and accelerate digital servicing, the relationship between cyber risk and fraud is undergoing a significant transformation. Cyber compromise often opens the door, while fraud typically occurs at the data, account or policy level through impersonation, identity misuse, financial account manipulation, policy abuse or unauthorised transactions. Defending the digital insurer requires multilayered approaches to secure identities, continuously monitor the customer lifecycle and build resilience amid the converging web of cyberthreats and fraud in interconnected insurance ecosystems.

As cyber and fraud risks increasingly cut across the insurance lifecycle and extend beyond individual systems, addressing them in isolated pockets is becoming less effective. A more joined-up approach is needed, bringing together three interconnected layers of resilience comprising identity, transactions and interactions and the broader ecosystem.

Figure 24: Three layers of cyber resilience for the digital insurer



Source: Deloitte analysis

To establish durable digital insurance, an insurer must broaden its perspective beyond specific control measures and encompass the accumulation of risk across a client lifecycle. Identity resilience involves establishing trustworthiness when presented with a given identity and recognising those moments when confidence may begin to wane. This is now more pertinent given increasingly digitalised customer journeys, in which security tokens can be stolen and/or shared with or utilised by actors other than true customers, implying a paradigm shift towards dynamically managing trust through multiple signals to avoid repeated inconvenience for the end customer.

Focusing on what is plausible, an insurer using transaction and interaction resilience would evaluate whether a given activity seems in context rather than viewing an action as an isolated incident. A payment, policy change or service request may appear legitimate on its own but become suspicious when viewed alongside changes in behaviour, timing, channel, device or account activity. Tracking these distinct indicators helps insurers distinguish genuine customer activity from emerging fraud patterns, enables them to intervene proactively with customers throughout the insurance lifecycle and helps them progress towards securing customer trust in digital spaces.

When it comes to ecosystem resilience, an insurer must move beyond the confines of its direct boundaries. As insurance becomes increasingly dependent on platforms, APIs, healthcare providers, intermediaries and other third parties, vulnerabilities or control gaps at one point can have implications elsewhere in the value chain. Resilience therefore requires stronger internal controls, visibility into dependencies, clearer accountability across collaborators and secure intelligence sharing across the ecosystem.

Taken together, these layers suggest a shift from individual fraud-defence tactics and other sporadic controls to a unified process in which trustworthiness, behaviour and an interconnected network of risks are consistently reviewed. The goal, therefore, shifts to detecting small vulnerabilities earlier and identifying how risks propagate and how to respond to them before they affect customers, insurers or ecosystem collaborators.

Europe, already a leader with an increased number of requirements emphasizing explainability, privacy and ethical and responsible AI practices, has taken great strides in

developing AI governance mechanisms by strengthening the protection of sensitive customer data, where information can be shared amongst insurers and business collaborators to prevent future fraud schemes from impacting customers, which tends to permeate numerous stakeholders in the insurance value chain.[58]

India is just beginning this transformation with rapid progress in digital insurance via mobile-first interfaces, real-time payments and easy onboarding processes that present both risk-mitigation opportunities and new risks.

As AI becomes more embedded in insurance, the role of human and digital agents is also likely to evolve. This raises new questions about accountability when an AI-enabled or digital agent makes an incorrect recommendation, misrepresents an insurance product, executes an incorrect insurance transaction or contributes to a fraudulent instance. Establishing how accountability is assessed and where responsibility ultimately lies among the individual insurer, the intermediation collaborator, the technology company providing the service, the human agent involved and the end-customer will become more crucial over time.

The issue could become more complex as digital assets and digital insurance converge. As customers increasingly use AI agents to transact, manage digital assets or access insurance, the industry may need clearer frameworks for establishing liability when decisions or transactions go wrong. Questions around who authorised an action, who controlled the agent, whether the customer understood the implications and how responsibility is shared across the digital ecosystem are likely to remain open areas of regulatory and industry development. As insurance becomes increasingly agentic and ecosystem-driven, cyber resilience will need to address system security and accountability for harm arising from autonomous digital actions.

These emerging forms of digital interaction also reinforce the need for stronger, connected fraud controls across the insurance lifecycle. Fraud beyond insurance claims is likely to become more common across the customer lifecycle, including onboarding and customer management, as the insurance sector becomes increasingly digitalised. While disconnected systems and fragmented customer data can create opportunities for fraud, real-time claim settlement (for example, a cashless health-insurance framework requires insurers to decide on pre-authorisation requests within one hour of receipt and provide final authorisation within three hours) requires insurers to act immediately upon of receiving a hospital's discharge request. Meeting these timelines necessitates connected ecosystems capable of accessing and analysing data immediately, while generating timely fraud alerts.[59]

Against this backdrop, the proposed Deloitte Cyber Framework aims to build on a shift from isolated, reactive control and fraud defence systems to continuously monitored models for cyber resilience that include cyber governance, fraud intelligence, underwriter decision-making, ecosystem cooperation, business resilience and the crucial component of customer trust. Looking ahead, a key competitive differentiator for insurers will be building trust in the digital consumer experience. The focus of fraud defence will shift from cost and control towards enabling business value. An insurer that delivers a seamless, secure and trusted digital consumer experience will be better equipped to accelerate its customer base growth, ensure loyalty and maximise long-term profit. At the same time, cyber insurance is expected to undergo a transformation. Conventional risk-based underwriting and pricing may become untenable as attack surfaces continually evolve and incidents spread rapidly across connected ecosystems. Future insureds can expect insurers to use real-time cyber risk intelligence, behavioural indicators and threat data from both external and internal sources to estimate losses accurately. A gradual shift will be seen from static underwriting models towards intelligence-led, adaptive cyber insurance models.

Insurance companies that achieve robust digital resilience (for example, have strong cyber hygiene and controls, along with the capability for instant incident response) will optimise pricing and coverage. However, cyber insurance will evolve beyond risk transfer alone to actively encourage better security practices across the entire value chain of clients and business collaborators. If India's vision to provide insurance for all citizens by 2047 is to be realised, defending the broader digital insurance ecosystem, not just individual insurance companies, must be prioritised in the long term. Insurers can support India's Insurance for All by 2047 vision by strengthening their own cyber resilience, helping policyholders improve preparedness and expanding access to appropriately designed cyber cover. Closer collaboration across insurers, intermediaries, technology providers, regulators and cybersecurity specialists can improve threat visibility, reduce systemic exposure and support the sustainable growth of India's digital insurance ecosystem.

Endnotes

1. https://www.deloitte.com/us/en/insights/industry/retail-distribution/retail-distribution-industry-outlook-2025.html?utm
2. https://www.moneycontrol.com/banking/india-s-insurance-sector-faced-maximum-cyber-onslaught-in-fy25-article-13131547.html
3. https://www.business-standard.com/companies/news/india-s-angel-one-says-investigating-security-breach-assessing-impact-125022800434_1.html
4. https://www.cyfirma.com/research/cyber-threat-landscape-report-india-bfsi-2026/
5. https://www.verizon.com/business/resources/Tea/reports/2025-dbir-data-breach-investigations-report.pdf?msockid=174309ae2dc46a7a13ad1c422c156bd6
6. https://timesofindia.indiatimes.com/technology/tech-news/pakistani-hackers-attacked-1-5-million-plus-indian-websites-after-operation-sindoor-failure-rate-names-of-7-pakistani-hacker-groups-techniques-used-and-more/articleshow/121128592.cms
7. https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/
8. https://economictimes.indiatimes.com/industry/banking/finance/indian-entities-may-lose-rs-20000-cr-to-cyber-crimes-in-2025-cloudsek-report/articleshow/118651127.cms?from=mdr
9. https://commercial.allianz.com/news-and-insights/reports/cyber-risk-trends.html
10. https://deepstrike.io/blog/cyber-insurance-statistics-2025
11. https://www.kenresearch.com/india-cyber-insurance-market
12. https://www.marketsandmarkets.com/Market-Reports/geography/cyber-insurance-market/india
13. https://www.imarcgroup.com/india-cyber-insurance-market
14. https://askfuzz.ai/discover/news/banking/banks-double-cyber-insurance-cover-to-100mn-amid-rising-threats
15. https://www.munichre.com/en/insights/cyber/cyber-insurance-risks-and-trends-2025.html
16. https://content.naic.org/sites/default/files/inline-files/2025_Cybersecurity_Insurance%20Report.pdf
17. https://deepstrike.io/blog/cyber-insurance-statistics-2025
18. https://industrialcyber.co/reports/munich-re-sees-untapped-potential-in-15-3b-cyber-insurance-market-amid-rising-threats-and-evolving-risks/
19. https://www.linkedin.com/pulse/india-cyber-insurance-market-size-growth-trends-share-aryan-rawat-eflse
20. https://irdai.gov.in/handbook-of-indian-insurance
21. https://www.weforum.org/stories/2026/04/anthropic-mythos-ai-cybersecurity/?utm
22. https://www.weforum.org/stories/2026/05/cyber-resilience-goal-frontier-ai-makes-it-urgent//?utm
23. https://www.genevaassociation.org/publication/cyber/strengthening-cyber-resilience-through-insurance?utm
24. https://actuary.info/insights/cyber-insurance-2026?utm
25. https://onlinelibrary.wiley.com/doi/10.1002/ijfe.70166?af=R&utm
26. https://link.springer.com/article/10.1007/s10207-026-01275-5?utm
27. https://www.genevaassociation.org/publication/cyber/strengthening-cyber-resilience-through-insurance?utm
28. https://www.genevaassociation.org/sites/default/files/2026-05/cyber_resilience_080526_digital_final.pdf
29. https://www.helpnetsecurity.com/2026/04/23/cyber-insurance-claims-report/?utm
30. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1347.pdf

31. https://onlinelibrary.wiley.com/doi/10.1002/ijfe.70166
32. https://www.cambridge.org/core/journals/british-actuarial-journal/article/cyberinsurance-pricing-models/81A761007ADE929C4E81AFB9ADB054B0?utm
33. https://www.prnewswire.com/news-releases/netdiligence-releases-fifteenth-annual-2025-cyber-claims-study-302558642.html
34. https://www.theinsurer.com/cyber-risk/news/ransomware-activity-hits-record-levels-in-q4-travelers-2026-03-23/?utm
35. https://www.munichre.com/en/insights/cyber/cyber-insurance-risks-and-trends-2026.html?utm
36. https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng
37. https://www.oag.ca.gov/privacy/ccpa
38. https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm
39. https://www.pdpc.gov.sg/about/the-legislation/pdpa-overview
40. https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en
41. https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng
42. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
43. https://cpl.thalesgroup.com/financial-services-data-threat-report
44. https://www.tcsa.in/frameworks/iso-27001/for-irdai
45. https://sprinto.com/blog/iso-42001-vs-iso-27001/
46. https://ucstoolkit.store/blogs/blog/iso-standards-guide-27001-22301-42001-implementation
47. https://www.itil.org.uk/blog/what-is-itil
48. https://www.techradar.com/pro/security/businesses-are-finally-taking-action-to-crack-down-on-ai-security-risks?utm
49. https://www.itpro.com/security/supply-chain-and-ai-security-in-the-spotlight-for-cyber-leaders-in-2026?utm
50. https://caalley.com/acts_reg/irdaacts/guidelines/IRDAI_Information_and_Cybersecurity_Guidelines_2026.pdf
51. https://www.bankofengland.co.uk/prudential-regulation/publication/2026/june/pra-annual-report-2025-26
52. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2190655&lang=1&reg=3
53. https://consentos.in/learn/dpdp-vs-it-act/
54. https://www.pcisecuritystandards.org/standards/pci-dss/
55. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2217537&lang=1&reg=3
56. https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en
57. https://www.crowdstrike.com/en-us/resources/crowdcasts/sec-readiness-demystifying-the-four-day-breach-disclosure-requirement/
58. https://finance.ec.europa.eu/document/download/bd5b4871-2bb6-4681-a982-b3bebad46b00_en?filename=260310-report-eu-financial-sector-preparedness_en.pdf
59. https://www.moneycontrol.com/news/business/personal-finance/health-insurance-claims-5-irdai-rules-that-can-make-a-difference-when-you-need-to-claim-14036208.html

Connect with us

Debashish Banerjee
Partner, Insurance Sector Leader,
Deloitte South Asia
debashishb@deloitte.com

Munjal Kamdar
Partner
Deloitte India
mkamdar@deloitte.com

Jignesh Oza
Partner
Deloitte India
jigneshoza@deloitte.com

Contributors

Alpa Talwar

Astha Bhadauria

Acknowledgements

Deepa PS

Neha Kumari

Pavleen Segue

Richa Sharma

Rishav Raj

Rishi Malhotra

Sreya Abraham

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which is a separate and independent legal entity, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Bengaluru, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Mumbai, New Delhi, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

This communication contains general information only, and none of DTTL, its global network of member firms or their related entities is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication.

© 2026 Deloitte Touche Tohmatsu India LLP. Member of Deloitte Touche Tohmatsu Limited