



# IRDAI tightens cyber net: Wake-up call for insurers

May 2025



India's insurance sector has grown at a CAGR of 17 percent over the past two decades, reflecting substantial expansion and development. This growth has been driven by increased awareness, favourable regulatory changes and greater participation from the private sector. The increased Foreign Direct Investment (FDI) limit in insurance companies from 74 percent to 100 percent has attracted greater foreign investments in this sector.<sup>1</sup>

Despite the growth rate, the sector has witnessed a surge in cyber incidents in the last five years. According to a latest report published in 2025, India faced nearly 370 million malware attacks in 2024, with the banking, financial services and insurance sector among the top targets.<sup>2</sup>

In today's digital age, any cyber incident poses significant threats to organisations. Therefore, it is crucial to be prepared to respond effectively to prevent or minimise damage to assets, protect customer data and ensure business continuity.

To enhance cybersecurity in the insurance sector, the Insurance Regulatory and Development Authority of India (IRDAI) introduced provisions in its 'Information and Cyber Security Guidelines, 2023' on 24 March 2025. These provisions address cyber incidents and crisis preparedness for insurance companies and intermediaries in India.

The move aims to minimise the potential damage caused by cyberthreats.

<sup>1</sup> <https://www.ibef.org/industry/insurance-sector-india>

<sup>2</sup> <https://www.dsci.in/resource/content/india-cyber-threat-report-2025>



## Breakdown of IRDAI's 2025 cybersecurity guidelines



**Reporting of cyber incidents within six hours of identification:** Per the new guideline, insurance companies and licensed intermediaries such as brokers, corporate agents, insurance marketing firms and web aggregators must notify IRDAI and the Indian Computer Emergency Response Team (CERT-In) within six hours of any cyber incident. This ensures rapid response mechanisms and mitigates financial, operational and reputational risks posed by cyberthreats.

**Enhanced monitoring requirements:** The new regulation also mandates continuous vigilance over all Information and Communication Technology (ICT) systems. Insurers are expected to ensure end-to-end monitoring and retention of ICT and application log data for a rolling period of 180 days. This enhances cybersecurity resilience by ensuring insurers proactively detect and respond to potential threats, reducing the risks of data breaches and system vulnerabilities.

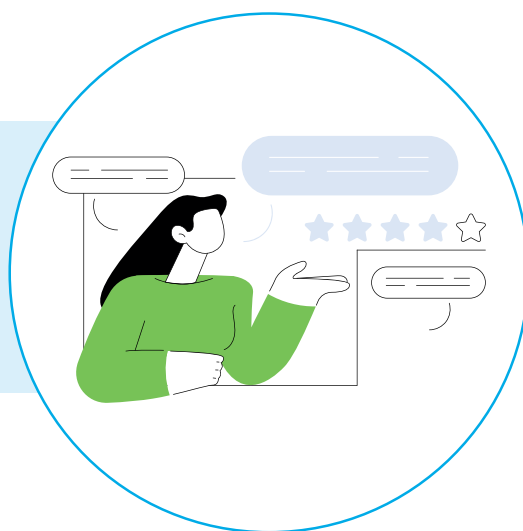


**Time-synchronised systems:** All ICT systems must align with India's official Network Time Protocol (NTP) to ensure consistency in event logging and forensic analysis.



**Implementation of a Cyber Crisis Preparedness Plan (CCMP):** The mandate obligates insurers to have a structured response mechanism in place, enabling swift action in case of a cyberattack or data breach. This proactive approach ensures business continuity and minimal disruption in case of a cyber incident.

**Onboarding certified forensic experts:** Additionally, insurers need to empanel forensic experts in advance to investigate any cybersecurity incident immediately. This approach can eliminate delays in forensic investigations and ensure faster resolution of security breaches.



**Avoiding conflicts of interest:** Companies involved in identifying cyber risks must not be the same as those conducting the investigation. This separation of duties ensures objectivity and transparency and prevents potential conflicts of interest.

**Mandatory board-level oversight:** Insurers and intermediaries must report their compliance status to their respective Board of Directors and submit the minutes-of-meeting to IRDAI as evidence of adherence. This promotes stronger governance and accountability at the board level.

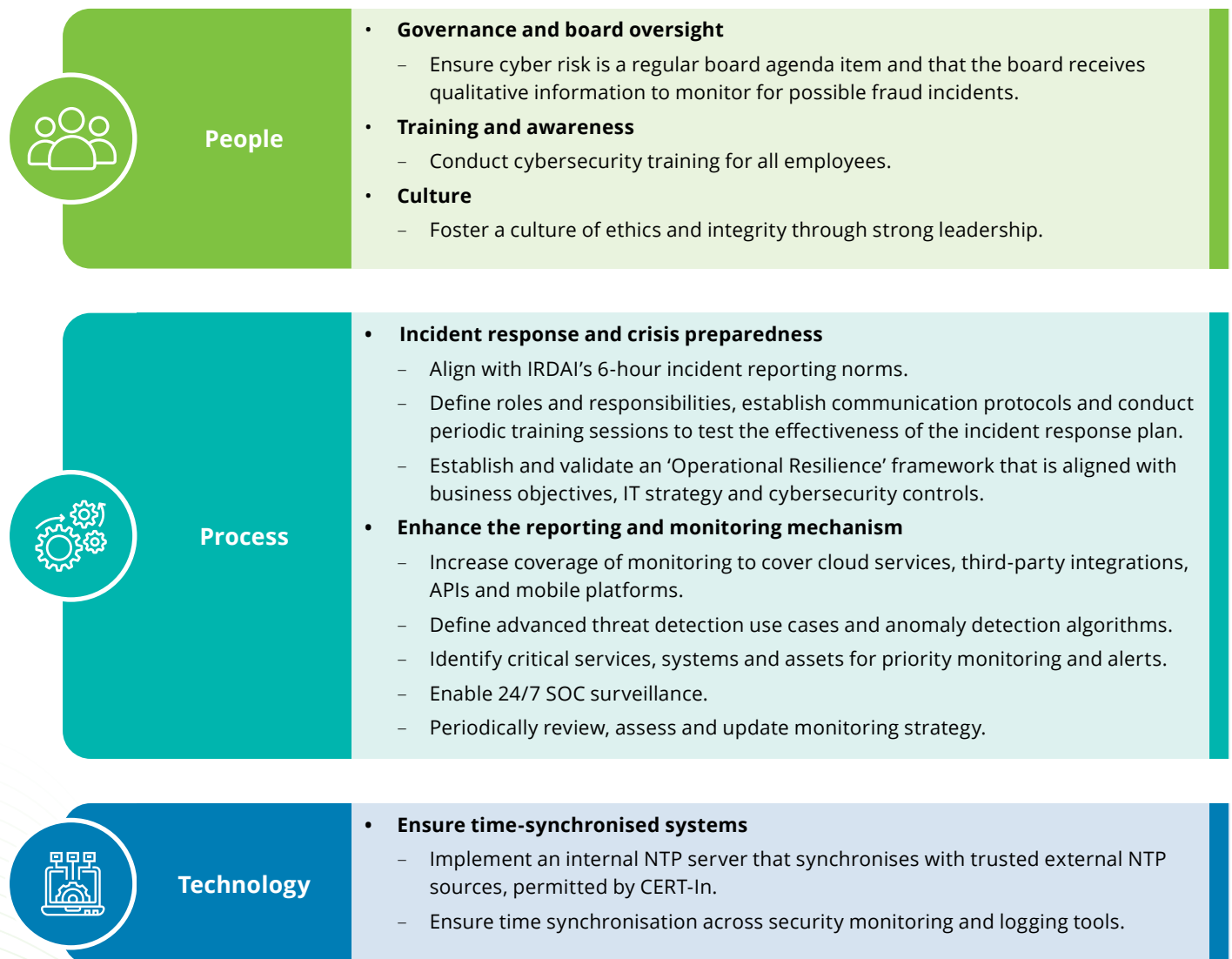




## Key actions for insurers

Insurance firms must be equipped to manage cyber incidents in a responsive and regulatory-compliant manner. This encompasses both proactive and reactive measures for prevention, detection and response to cyberthreats and vulnerabilities.

To comply with the reporting requirements and avoid any regulatory scrutiny, insurers must focus on actionable strategies across people, process and technology, while also building long-term resilience.



# Connect with us

**Nikhil Bedi**

Partner and Leader - Risk, Regulatory & Forensic  
Strategy, Risk & Transactions  
Deloitte India  
[nikhilbedi@deloitte.com](mailto:nikhilbedi@deloitte.com)

**K.V. Karthik**

Partner and Leader - Forensic & Financial Crime  
Strategy, Risk & Transactions  
Deloitte India  
[kvkarthik@deloitte.com](mailto:kvkarthik@deloitte.com)

**Vishal Jain**

Partner and Leader – Enterprise Risk  
Strategy, Risk & Transactions  
Deloitte India  
[jainvishal@deloitte.com](mailto:jainvishal@deloitte.com)

**Sachin Yadav**

Partner, Forensic & Financial Crime  
Strategy, Risk & Transactions  
Deloitte India  
[sachiyadav@deloitte.com](mailto:sachiyadav@deloitte.com)

## Contributors

**Krunal Joshi****Shailesh Kand**

# 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](http://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.

© 2025 Deloitte Touche Tohmatsu India LLP. Member of Deloitte Touche Tohmatsu Limited