Deloitte.

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.[1]

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.[2]

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.

[1] https://www.ibef.org/industry/insurance-sector-india

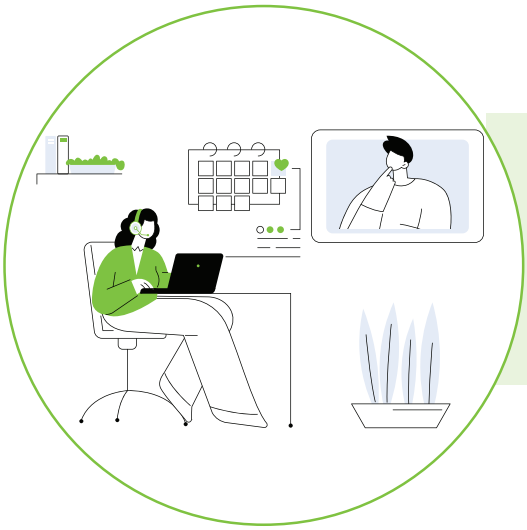
[2] https://www.dsci.in/resource/content/india-cyber-threat-report-2025

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.

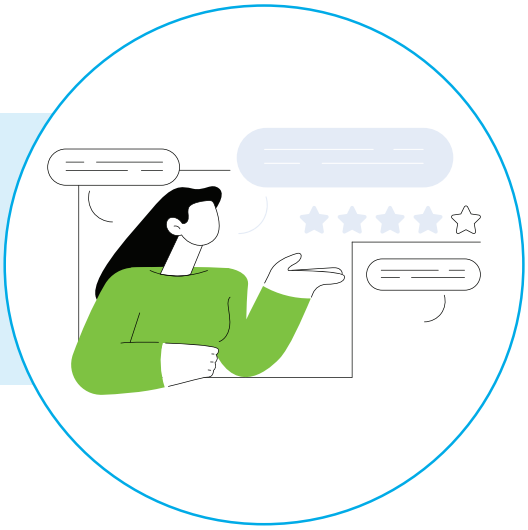
Enhanced monitoring requirements: The new regulation also mandates continuous vigilance over all Information and Communication Technology (ICT) systems. Insurers are expected to ensure end-to-end monitoring and retention of ICT and application log data for a rolling period of 180 days. This enhances 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.

People

- **Governance and board oversight**
  - Ensure cyber risk is a regular board agenda item and that the board receives qualitative information to monitor for possible fraud incidents.
- **Training and awareness**
  - Conduct cybersecurity training for all employees.
- **Culture**
  - Foster a culture of ethics and integrity through strong leadership.

Process

- **Incident response and crisis preparedness**
  - Align with IRDAI's 6-hour incident reporting norms.
  - Define roles and responsibilities, establish communication protocols and conduct periodic training sessions to test the effectiveness of the incident response plan.
  - Establish and validate an 'Operational Resilience' framework that is aligned with business objectives, IT strategy and cybersecurity controls.
- **Enhance the reporting and monitoring mechanism**
  - Increase coverage of monitoring to cover cloud services, third-party integrations, APIs and mobile platforms.
  - Define advanced threat detection use cases and anomaly detection algorithms.
  - Identify critical services, systems and assets for priority monitoring and alerts.
  - Enable 24/7 SOC surveillance.
  - Periodically review, assess and update monitoring strategy.

Technology

- **Ensure time-synchronised systems**
  - Implement an internal NTP server that synchronises with trusted external NTP sources, permitted by CERT-In.
  - Ensure time synchronisation across security monitoring and logging tools.

Connect with us

Nikhil Bedi
Partner and Leader - Risk, Regulatory & Forensic
Strategy, Risk & Transactions
Deloitte India
nikhilbedi@deloitte.com

K.V. Karthik
Partner and Leader - Forensic & Financial Crime
Strategy, Risk & Transactions
Deloitte India
kvkarthik@deloitte.com

Vishal Jain
Partner and Leader – Enterprise Risk
Strategy, Risk & Transactions
Deloitte India
jainvishal@deloitte.com

Sachin Yadav
Partner, Forensic & Financial Crime
Strategy, Risk & Transactions
Deloitte India
sachyadav@deloitte.com

Deloitte.