Article Date	Headline / Summary	Publication
09 Nov 2026	Under Attack, Banks Bolster Cyber Covers	The Economic Times

GOOD OPPORTUNITY FOR INSURERS, BUT COMPETITION COULD CAP PREMIUMS

Under Attack, Banks Bolster Cyber Covers

Opt for higher sum assured to protect against disruptions, financial hit



Risk Assumption

SBI may claim under ₹**1,425 cr** **Oriental Insurance** cover

Bank of Baroda holds ₹**750 cr** cyber policy; may have filed preliminary data breach claim

AU Bank holds ₹**100 cr** cover

Spandana Sphoorty holds ₹**12 cr HDFC Ergo** policy

Shilpy Sinha

Mumbai: Large financial services companies are seeking to expand their cyber insurance cover amid rising frequency of cyberattacks and increasing cost of business disruption, even as competition among insurers keeps premiums under pressure.

A large non-bank financial company plans to buy a cyber insurance policy of ₹2,000 crore next month, up from ₹1,400 crore last year, according to an insurance industry executive familiar with the placement. The increase reflects concerns that even a temporary disruption to technology systems could result in a substantial financial loss.

"We are seeing increasing interest in higher cyber insurance limits, particularly among large banks, NBFCs and financial institutions," said Najm Bilgrami, head of Casualty and Financial Lines Product at Tata AIG.

Growing digital dependence and interconnected systems are prompting companies to reassess their covers, he said. "Cyber risk is now viewed as a board-level risk, resulting in greater focus on balance sheet protection against severe cyber events," said Amarnath Saxena, chief technical officer, commercial, at Bajaj General Insurance.

BUSINESS INTERRUPTION

For large financial institutions, the biggest impact often is the loss arising from systems remaining unavailable after an attack, rather than the immediate cost of the breach.

Besides business interruption, ransomware, data theft, cyber extortion and third-party liabilities are among the key risks.

Ambiguity in Wordings ▸▸ 9

Ambiguity in Wordings

▸▸ From Page 1

In one of the largest cyber insurance claims, amounting to about ₹700 crore, forensic and legal expenses accounted for nearly 30% of the total cost, Bilgrami said.

For institutions handling large transaction volumes, even a brief disruption can lead to significant losses and costs related to system restoration, forensic investigations, technology consultants, customer communication and the replacement of compromised debit cards. "Ransomware attacks, bricking, privacy and data breaches, as well as direct theft of money through cyberattacks, are the major drivers for NBFCs to seek increased cover," Saxena said.

Recent cyber incidents involving Bank of Baroda, State Bank of India, Central Bank of India and AU Small Finance Bank have brought the vulnerability of financial institutions into focus. Insurers have reported several attacks on financial services and manufacturing companies over the past three to four months. Investigations into some incidents are ongoing.

Insurers are increasingly concerned about hackers using artificial intelligence to identify vulnerabilities and breach IT systems. A deeper breach could expose customer KYC documents and financial records, increasing liabilities as well as the cost of notifying affected customers and monitoring compromised data.

LITTLE CHANGE IN POLICY TERMS

Despite the growing use of AI in cyberattacks, insurance policy wordings have not changed significantly. Policies generally cover the financial consequences of an incident, irrespective of whether it involves AI, a rogue employee or compromised data, subject to policy terms and exclusions. "Only a handful of insurers are currently asking specific questions and evaluating clients' AI exposure," Tata AIG's Bilgrami said, adding that underwriting discipline would be important as new risks emerge.



Policy wording itself remains a concern, with gaps between different sections of cover potentially complicating claims. While the Digital Personal Data Protection Act, expected to be implemented in May 2027, could increase financial consequences of data breaches, it has not yet triggered a significant rise in cyber insurance purchases, an industry executive said.

COMPETITION KEEPS PREMIUMS IN CHECK

Despite rising threats and demand for higher limits, cyber insurance premiums have not increased, remaining around 0.75%-1.5% of the sum assured. A company buying ₹2,000 crore of cyber insurance cover would typically pay annual premium of about ₹15 crore-₹30 crore, depending on its risk profile, claims history and cybersecurity controls.