

Cybersecurity Insurance Cos Run into a Data Smog

Lack of actuarial data, murky disclosures & speed at which breach may spread have firms in a bind


Megha.Mandavia
@timesgroup.com

Bengaluru: Cybersecurity insurance, a new buzzword among Indian insurers, has crucial hurdles to overcome before it can live up to the potential promised by the companies. Lack of actuarial data on cyberattacks, murky disclosures by corporate victims and the incredible speed at which a breach may spread globally have companies in a bind.

Actuarial data help insurers evaluate financial implications of risk and uncertainty by applying mathematical and statistical methods, while devising solutions to reduce chances of any future risks and occurrence of any undesirable events. In case of cybersecurity insurance, actuarial data are scarce as it is a new line of business. And the little data that insurance companies have lose relevance because cyberthreat keeps getting deadlier.

Earlier this year, Warren Buffett said cybersecurity incidents will rise, and with them the potential to significantly harm the insurance industry. He said he doesn't want much underwriting exposure to cybersecurity threats for Berkshire Hathaway's insurance businesses and expressed scepticism that any insurance company can assess the risk for cybersecurity events. "While the insurers are confident about how cyber risk affects different businesses, they currently face a challenge of lack of enough actuarial data in this new space. Hence, insurance companies rely on qualitative underwriting as-

SPANNER IN THE WORKS



CHALLENGES

- **Cyber insurance** is evolving and actuarial data is scarce as it is a new line of business
- **Cyber risk** is evolving every day and every change leads to increased vulnerability
- **Although attacks** are increasing, majority go unreported

ASSESSING RISK IN ABSENCE OF RICH DATA

<p>1. RISKY INDUSTRIES Finance, insurance & ecomm</p> <p>2. SCALE Larger revenue size, geographic reach etc</p>	<p>3. CURRENT HEALTH Cyber security controls in place, past breaches & awareness level among staff</p>
---	---

sessments to evaluate the risk exposures of each client and their security posture," said Sushant Sarin, executive vice-president — commercial lines & reinsurance, Tata AIG General Insurance. The cybersecurity insurance segment is growing anywhere between 50 and 100% annually, according to aggressive growth projected by various insurance companies and brokers. However, with the growth has come some caution on how to assess a cyber risk. Bajaj Allianz, HDFC Ergo, ICICI Lombard, and Tata AIG are seeking help from either cyber experts or global reinsurance companies.

Cyberattacks not only cause financial losses to companies that are hurt by shutdowns or slowdown in opera-

tions, but also expose them to risks of irreparable reputational damage, regulatory fines, and legal liabilities in case of customer data breach. In cyber extortion cases, it is even tougher to quantify the adequacy and requirement of cover.

"In privacy and data breaches, the losses could be financially devastating and with increasingly stringent guidelines and laws imposing stricter than ever penalties, it is not easy to quantify the potential losses," said Sasikumar Adidamu, chief technical officer, Bajaj Allianz General Insurance. He added that due to the increasing use of cloud computing services and platforms, cyberattacks may lead to breaches on multitudes of connected devices, which leads to accumulation — a term used for the domino effect in the insurance industry. "There is reason for concern. The risk is new and the effects are global. Cyber risk can affect different entities of one company across the globe or different companies at one go. Underwriting cyber insurance is a challenge because there aren't too many models for risk assessment," said Sanjay Datta — chief underwriting, claims and reinsurance, ICICI Lombard.

One of the reasons for the general lack of data, apart from the newness of the segment, is the inadequacy of public disclosures. Although the number of cyberattacks is increasing, a majority go unreported. Unlike in India, in the US, the SEC has mandated the disclosure of cyber security risks and breaches, including potential weaknesses that have not yet been targeted by hackers.

SASIKUMAR ADIDAMU
CTO, Bajaj Allianz

In privacy and data breaches, the losses could be financially devastating and with increasingly stringent guidelines and laws imposing stricter than ever penalties, it is not easy to quantify the potential losses

WALTER TANDY MURCH / The Clock