Date: 14.6.2022	**Publication:** Mint
Page no: 13	**Edition:** Kolkata | Ahmedabad | Bangalore |Chennai|Hyderabad |Mumbai |New Delhi

Firms ramp up compliance, premiums for cyber insurance after covid

Moumita Deb Choudhury
moumita.choudhury@livemint.com
BENGALURU

TECHCIRCLE

Insurance companies, wary of growing cybersecurity attacks on Indian organizations, are raising the cost of cyber insurance and stepping up compliance norms.

According to industry stakeholders and experts, insurers have seen record increases in the number of cyber insurance claims made by companies hit by ransomware attacks and more.

A year ago, ICICI Lombard witnessed an industrywide increase of 40-60% in the cost of premium since the outbreak of covid-19, said Sanjay Datta, the insurer's chief of underwriting and claims.

A spokesperson for another insurance firm said unlike insurance claims for vehicle accidents, which usually range in the hundreds of thousands of rupees, cyber insurance claims can run up to $2-3 million at a time.

The number of cyber policy claims and reporting has soared more than 220% between 2020 and 2021, said Surya Narayan Saha, research manager, financial insights at market research firm International Data Corporation (IDC). This April, IDC projected to spend above $20 million in 2022 on cyber risk management.

T.A. Ramalingam, chief technical officer at Bajaj Allianz General Insurance, said the company has seen a near doubling of the number of cyber insurance claims filed by corporates in the "last few years". He added that increased focus on digitalization and remote work following the pandemic, geopolitical tensions and increasing activity from ransomware groups have contributed to these.

Ransomware is a type of malware that encrypts firm's data, and asks to make payments in exchange for decryption key. GETTYIMAGES

Ransomware is a type of malware that encrypts a company's data, and asks it to make payments in exchange for the decryption key. Groups running such attacks have evolved dramatically since the pandemic, with criminal groups even providing ransomware-as-a-service to others, he added. Ransomware is the most common kind of cyber threat claims are filed for.

In February, security firm Crowdstrike identified a criminal group called Pinchy Spider, which provided services using a ransomware called Revil, which was responsible for attacks worth $10 million at the time. Revil, which originated in Russia, counts companies like Apple-supplier Qanta Computer among its victims.

For users of cyber insurance, this means that it's getting more difficult to get insured. The chief information security officer of a domestic automaker said getting cyber insurance presently requires much more negotiation for premiums. Earlier security reviews used to include a macro-level assessment of the applicant, whereas now, it's micro-level.

RISE IN CLAIMS

NUMBER of cyber policy claims increased by over 220% between 2020 and 2021

INSURERS are projected to spend over $20 million in 2022 on cyber risk management

"It's not like if you just tell them we have implemented certain measures they will believe it. Now they come physically to check whether all controls are in place," he said requesting anonymity.

According to ICICI's Datta, with increasing loss ratios, underwriters who assess exposure faced by clients are repositioning how they evaluate firms' security postures before approving any insurance proposal.

The insurance firm spokesperson cited above said even the policy form that companies have to fill in currently has grown from two to five pages.

Datta said insurance firms evaluate risk by taking note of everything from a firm's infrastructure to the data they handle. They do this by considering three major pillars—human firewall, process and technology.

This means that companies can't just have software firewalls in place, but will need employees dedicated to fighting cyberattacks in order to qualify for insurance. In addition, reviews are conducted of factors such as information security policies, business continuity plans, the kind of data a company handles, and its geographical presence.