Taking cover from cyberattacks

Insurers have come up with products for both individuals and business enterprises at attractive premium rates

GURUNATHAN V

As enterprises, the government and public rely increasingly on digitalisation, cybersecurity has become pivotal to their basic functioning nowadays.

Cyberattacks have been on the rise over the past 12-18 months, affecting businesses of all nature and sizes, where the reliability of the data network is a prerequisite to their operations. As a result, cybersecurity has come to occupy a prime position in a company's list of governance priorities.

As more companies shifted to work from home, there were database breaches and hackings, leading to loss of revenue opportunity across industries. Even systems believed to be highly secure could be breached in cyberattacks. Reports say almost 26,000 Indian websites were hacked in the 10-month period ended October. The hackers had been operating from different parts of the world with hidden identities.

While weak passwords are the common cause for such attacks, systems with unprotected or unchanged passwords are highly vulnerable. Second, different types of malware take advantage of expired antivirus software. Third, working in unsecured environments such as a common Wi-Fi network to access private emails and USB drives may prove risky.

The onus is on the organisation to take steps to prevent and counter potential threats. They should educate their employees to create strong passwords, follow proper protocols in keeping passwords secure and ensure firewalls are equipped to resist any malware attack, by installing regular software updates. This is also why virtual private networks are being insisted upon in organisations.

Types of threats

Internal threats could be a result of employee negligence or ignorance, while external threats could be from former employees, competitors, and hackers who steal corporate data and money through spoofing and phishing. These would obviously lead to reputational damage, financial loss, litigation, regulatory probes, and above all, loss of clients and thereby revenue.

Ransomware attacks continue to evolve in the market, with the past 8-10 months witnessing the highest number of threats of sensitive data exposure. A leading social network platform suffered a data breach, wherein millions of profiles containing email addresses, names, dates of birth, and phone numbers were sold on the dark Web. In another incident, a large foreign bank was hacked, causing financial loss. Ransom attackers can expose employees' HR files or clients' vulnerable data.

Insurers also add crime policies to cover collusion by staff.

There are cyber insurance solutions available in the market to protect against losses caused by cyberattacks, including first-party and third-party losses, and cyber extortion.

First-party insurance covers loss caused due to electronic theft, loss of electronic communication, e-vandalism, business interruption (income loss due to fraudulent access causing impairment of operations), and the like.

Third-party loss covers disclosure liability (any customer claim due to system security failures resulting in unauthorised access), content liability (for alleged copyright infringement), reputational liability, and conduit liability. An expenses cover includes privacy notification expenses, crisis expenses and reward expenses.

A few insurers even provide cover for proactive forensic services in a possible threat situation. Companies should first understand the need for cyber insurance solutions, rather than just getting a cyber insurance cover. Cyber insurance helps cover legal expenses stemming from damages due to a cyberattack. It should be part of the company's overall business continuity strategy, as it helps quickly recover post an incident.

The ability to identify an attack and quickly shield against it are a few underwriting principles of the insurers.

Insurers conduct meticulous due diligence via proposal forms, interaction, network diagrams and reviews of cyber strategies of a firm before providing cyber insurance covers.

As part of their review, insurers check the processes of MFA (multi-factor authentication), tested backups, network monitoring, and whether the users are employees and/or vendors.

Buying a cyber insurance policy alone will not suffice; the company should ensure that protocols are followed strictly and train employees in digital hygiene.

Digital discipline

Proactive risk management strategies that include ensuring the use of strong passwords, ensuring that passwords are not freely shared among employees, multi-factor authentication, proper firewall usage and access controls over servers and routers are all examples of good digital behaviour. These are also important underwriting points to obtain cyber insurance from the insurers.

Due to hefty ransomware exposure, whether or how much cover insurers can provide to a company depends on the sector, profile and digital behaviour of the company.

To provide cover, insurers consider factors such as the turnover of the company, individual IT devices, personal identifiable information, whether the system or network management is outsourced, frequency of regular system audits, and use of encryption.

Thanks to work-from-home situations, insurers have come up with products for individuals too at reasonable premium levels, apart from business enterprise solutions.

While the cost of the cover for companies may be obtained approximately at about 4-5% of the limit applied for, retail cyber products come with individual cover and add-ons like family cover and protection of digital assets from malware, with limits of liability ranging from ₹50,000-₹1 crore, at premium prices ranging from ₹1,500 to ₹15,000.

This can be useful in the event of any retail cyber breach. More insurers are coming up with attractive premiums.

Exclusions include deliberate fraudulent or wilful violation, unlawfully collected data and unsolicited correspondence, to name a few.

Insurance cover is always meant to ensure prevention of loss. That said, clear, written incidence-planning and testing drills are crucial for protection against attacks.

A capsuled cyber insurance and the maturity of the company are both important because companies using the best of practices with impeccable technical solutions and systems may still be vulnerable in these modern-day cyber environments.

(The writer is director and CEO, TVS Insurance Broking Ltd.)