

## Insurance

## Are You Cyber Secure?

Your bank accounts, and details of credit and debit cards can be up for sale on the dark web. Run for cover, quickly

By **Nirmala Konjengbam**

**P**ersonal details of 20 million customers of a leading Indian e-commerce portal was allegedly leaked and made available for sale on the dark web last month. In August, almost 3,69,000 banking records of Indian account holders were up for grabs. In September, Prime Minister Narendra Modi's Twitter account was allegedly hacked.

In a world that is online 24x7, the dangers of cyber-attack—a word to describe unauthorised access to private online data—have never been more prominent than today. A recent study indicates that seven out of 10 Indian companies were victims of data breaches and cyber-attacks. The country witnessed close to 10,000 coronavirus-themed attacks between February and May. According to National Cyber Security Coordinator, Lt. Gen. (Retd) Rajesh Pant, cyber-attacks in India have “gone up multi-fold” with four lakh malware being found every day. Data indicates that cyber-attacks witnessed a sharp jump during the lockdown when a large section of the country's population was forced to work from home.

Our dependency on digital platforms has only increased over the years. Apart from being part of our work, digital platforms are also our gateway for shopping, entertainment and social interactions. Increased cyber-attacks make us more vulnerable to crimes like digital identity theft and hacking that takes away sensitive, personal and financial information.

Do not be surprised if your bank account and credit or debit card details are available for sale on this notorious

dark web. Take cover in time.

Online insurance does not act as a firewall every time you are online, neither does it repel an attack like anti-virus software, but it certainly reduces your financial vulnerability.

### SANJAY DATTA

ICICI Lombard's Chief of Underwriting, Claims and Reinsurance



**WFH has increased the risk of exposure to various cyber-threat vectors. Insurers have seen a rise in inquiries**

The cover gets activated after privacy or data breach and personal information theft. It helps you recover any monetary loss that you may have suffered. Today, however, only four insurers offer individual cyber cover and compensations; depending on the losses these can range from ₹50,000 to ₹2 crore.

### Need For Protection

What adds to the woes is the lack of technical knowledge about anti-malware and firewalls among a large section of people. The extra layer of protection that we enjoyed from our employers' well-secured IT infrastructure is also out of the equation, as a large part of the population has been working from home.

Cyber insurance has witnessed a steep rise in demand amid an uncertain environment. For example, Bajaj Allianz General Insurance reported a 20 per cent increase in inquiries for individual cyber insurance covers in the first half of 2020-21. Future Generali India

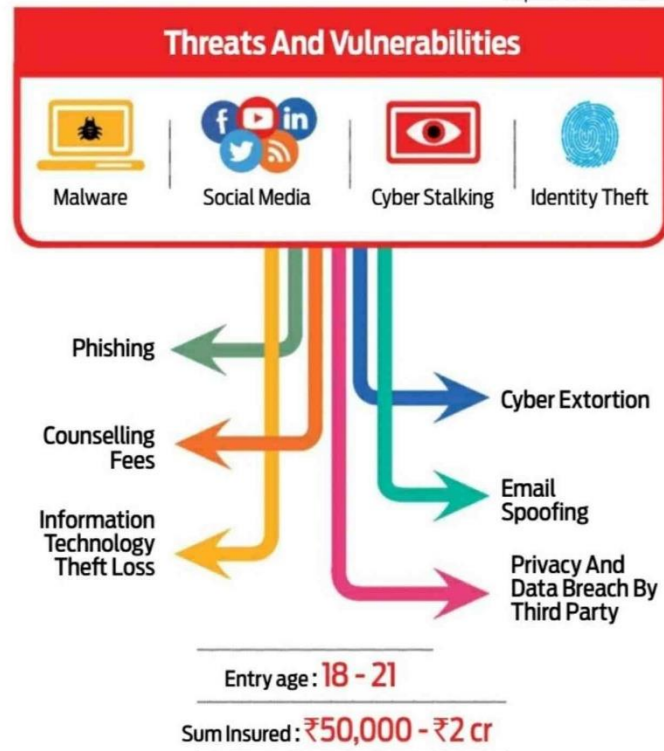


Insurance reported a 30-40 per cent increase in demand. At the same time, ICICI Lombard witnessed similar trends for its corporate plan.

"Cyber insurance does not protect you from potential cyber attacks but offers coverage if you fall prey to various attacks and threats protecting your reputation and losses in case any vital, financial or sensitive information is stolen or misused," explains TA Ramalingam, Chief Technical Officer of Bajaj Allianz General Insurance.

### Right Cover

It insures expenses related to legal defence and prosecution following identity theft and cyberstalking. Transport costs for attending court summons are also covered. The cover pays for restoration, retrieval and reinstallation of data or computer programs damaged by malware. It provides coverage for expenses incurred in counselling services that may be necessary after an attack. Claims for damages to third parties following privacy and



data breach are paid. "During the pandemic, most organisations are adapting the work-from-home model. It has increased cyber attack risk as organisations have moved their IT applications services and databases to cloud platforms. Employees are working from home through networks that are not fully secured. The trend has increased the risk of exposure to various cyber-threat vectors and insurers have seen a 30 per cent rise in inquiries in recent quarters," says Sanjay Datta, ICICI Lombard's Chief of Underwriting, Claims and Reinsurance.

### Things To Remember

Everything so far sounds good about cyber insurance, but merely buying a policy would never prove to be an elixir. It is vital that we evaluate our risks and accordingly choose the cover and add-ons to be best

protected against any threat.

"While evaluating the need for this plan, an individual must consider the exposure risk, or how much private data like financial transactions are being put out on the internet. Suppose one frequently opts for internet banking, card payments, e-wallets, then cyber insurance must move up in consideration set," adds Dr Shreeraj Deshpande, Chief Operating Officer, Future Generali India Insurance Company.

Essentials to keep in mind while buying such a policy would be:

**Evaluating Risks:** It is essential to identify your online vulnerability. It will be a factor of necessary protection required. You need to figure out the frequency of your digital activities, financial transactions, social media interactions and use of digital data lockers.





**Accurate Sum Assured:** After identifying the degree of risk, you must choose the right sum based on vulnerability. Cyber insurance policies offer covers ranging from ₹50,000 to ₹2 crore.

**Right Insurer:** Apart from choosing a policy that provides cover for all your requirements, it is also essential to check an insurer's claim settlement ratio. A low ratio could lead to trouble while making a claim.

**Right Add-ons:** You must look at the add-ons while buying cyber insurance. Your policy may be comprehensive but not exhaustive.

### Claims Procedure

Claims filing procedure for cyber cover is very much like other general insurance policies. A policy-holder is required to fill in a claim form along with a copy of the First Information Report (FIR) with police or cyber cell along with other necessary documents, such as transactional details in case of correspondence with a financial institution.

Policyholders are strongly advised to intimate the insurer about the fraud through telephone calls, emails, or the website as early as possible to expedite the process.

According to Datta, "ICICI

Lombard's claims procedure is simple and user-friendly. Customers can register their claims on the company's website or inform our customer care department. Designated claims manager, along with empaneled cyber experts, help customers contain an attack and guide them through their entire claims journey."

### Everything's Not Covered

A deliberate, criminal, fraudulent, dishonest, or malicious act or omission will not be covered. Cyber insurance policies do not protect you from any actual or alleged bodily injury or sickness, mental anguish, emotional distress or disturbance, or death of any person howsoever

#### Dr. SHREERAJ DESHPANDE

Chief Operating Officer, Future Generali India Insurance Company



**In evaluating the need for a plan, consider the exposure risk, or how much data is put out on the Net**

caused, except as provided in the costs related to counselling services. Damage to computers or any gadgets may not be covered. However, terms and conditions may vary from insurer to insurer.

### Tips To Stay Safe

Apart from purchasing cyber insurance, there is a lot that you can do to secure against cyber attacks. Some of the easiest and effective methods are:

**Securing Computer:** One of the first steps should be securing the system used to access the internet. Activate firewalls and use efficient anti-virus software, and update them regularly.

**Strong Passwords:** Always keep changing passwords regularly and make it as complicated as possible by adding numbers and special characters.

**Social Media Protections:** Opt for private accounts on social media platforms that only your friends and family can access. Most social media websites provide the option of making your account private.

**Don't Click On Phishing Emails:** Phishing emails keep evolving and sometimes appear like government information. It is necessary to evaluate every mail and link before clicking on it. Also, resist clicking on links that offer big prizes. Most of them are scams.

**Data Protection:** It is advised to use encryption for crucial files such as financial records. You must also always keep backups.

**Mobile Phone Protection:** It is also important to secure your mobile devices and protect your laptops or personal computers. The latest anti-malware software on phones is the best option.

While cyber insurance may compensate your monetary losses and pay your counseling fees, it will not protect you from intangible losses like reputation. It is not a safe ground out there, so be cautious. □

nirmala@outlookindia.com