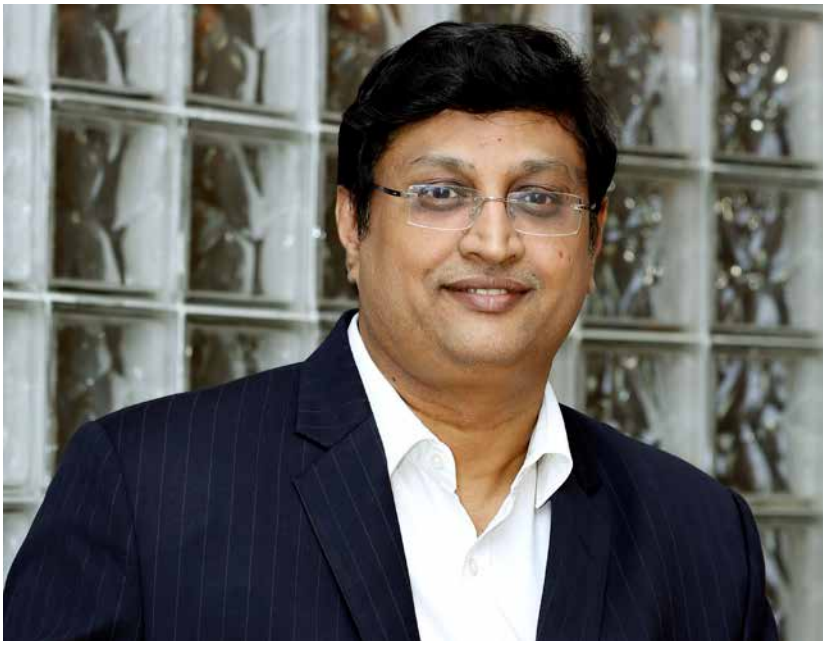
Who will win, cybercrime or cyber insurance?



Rapid digitalisation and growth of 'online' culture in India has also brought in sophisticated cybercrime. *Asia Insurance Review* speaks to **Mr Sasikumar Adidamu**, Chief Technical Officer, **Bajaj Allianz General Insurance**, to understand how insurers can play an important role in developing a comprehensive cybersecurity framework, including cyber-insurance, to tackle cybercrime.

By Anoop Khanna

India has 500 million active internet users and boasts of wireless tele-density of 91.56 with 1.02 billion active mobile subscribers. It speaks a lot about our digital connectivity and the exponential amount of data being generated, transmitted and stored online. Today India is the second largest online market globally after China. This also exposes the entire online system to threats of sophisticated cybercrime.

Cybercrimes in India

According to Indian Computer Emergency Response Team, of the Indian Ministry of Electronics and Information Technology, one cybercrime was committed every 10 minutes in India in the first six months of 2017.

The latest report of National Crime Records Bureau of India records 12,187 cases of cybercrime in India in 2016. According to cyber-experts, however, this is just 10% of the actual number of cybercrimes that take place in India annually.

According to the Federation of Indian Chambers of Commerce and Industry (FICCI) – Pinkerton India Risk Survey 2017, it ranks 'Information & Cyber Insecurity' as the biggest risk across sectors and geographies. There has been a shift in how cyber risks are perceived and from being considered a high impact but moderate probability risk earlier, it is now perceived as a high frequency and high impact risk.

Awareness about cyber insurance

Mr Sasikumar Adidamu said: "We live in an increasingly connected digital world where people use Internet throughout the day on their digital devices. Thus, there is an immense need to protect people against these new age internet risks and cyber threats."

Cyber cover falls under the category of liability insurance which is a very niche line of business that is growing rapidly in India. However, the portion of the same is relatively small as compared to other lines like motor, health or property.

Liability insurance forms around 2% (US$310 million) of the total general insurance business in India. It will be difficult to put a number to cyber insurance business in India as it is still at a nascent stage and the demand is picking up. The awareness and understanding of protecting oneself against cyber risks is however, widely recognised in India.

"In the light of recent incidents like WannaCry, people are realising the importance of having a cyber-cover to protect themselves and their companies as well. We are seeing increase in the number of inquiries for our cyber insurance policies both from corporates and individuals," said Mr Adidamu.

Growth of cyber-insurance portfolio

Speaking about the inherent need for cyber insurance covers given that cyber-crime poses serious threat to Indian corporations, Mr Adidamu said: "Earlier we would receive requests for cyber policies from large corporates and MNCs especially the one's involved in IT related services, but in the last year, we have also received inquiries from SMEs, start-ups and smaller businesses across sectors. The conversions have not been so high from smaller entities, but they are increasing."

Cyber insurance for individuals

He said: "For this category of users and the growing numbers of smartphone users who use mobile internet, Bajaj Allianz General Insurance has come up with Bajaj Allianz Individual Cyber Safe policy."

The very basic and the first line of defence in cyber protection is the use of genuine and updated software, whether anti-virus or operating systems. Quite a few individuals and even smaller businesses, however, still use pirated versions of anti-virus and OS software.

"We understand that in the market we are catering to, pirated versions of anti-virus and OS software pose a major challenge. Therefore, while we have a warranty requirement on the use of the genuine software, we have also built in a mechanism which ensures that if the claim doesn't arise due to use of pirated anti-virus or software then the claim shall be payable," he said.

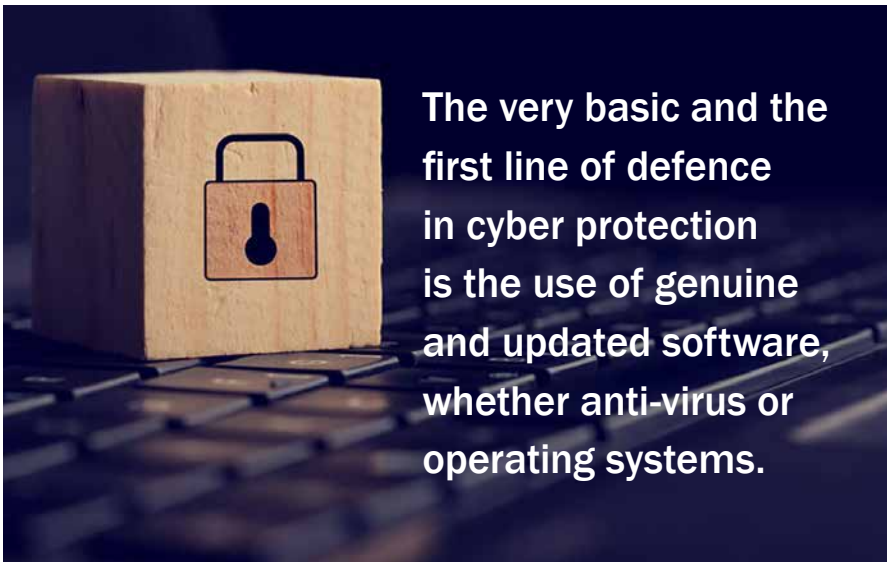
While insurance can help safeguard against cyber risks and contribute by implementing the best practices, developing them remains a monumental task which will need to be tackled by society at large.

Monetisation of cyber-risk to ensure adequate risk coverage

The cyber risk policies in the Indian market today offer both reputational risk cover and financial risk cover as standard coverage since the two often go hand in hand. A cyber attack most often results in both a financial loss and a reputational loss since most business today is driven by the perception the public holds for a firm.

Elaborating on this aspect, Mr Adidamu said: "The corporate clients need to keep in mind both the monetary value they would associate with a business interruption loss or a possible cyber extortion (larger & more reputed firms will get higher ransom demands) and their exposure to third part legal suits for things such as privacy or data breach etc (again a larger firm with a lot of third party data on their servers will have much higher liability as compared to a small firm with minimal or no third party data)."

For individuals, their presence or exposure on social media, their public image and their financial status will play a major role in deciding the limit for the cover they should buy.



Strategy to counter the 'dynamic' cyber-risks

The nature of cyber risk is extremely dynamic, and it can cripple every aspect of the modern society infrastructure. With digital footprints getting larger by the day and the new avenues and technology like crypto currency adopted by hackers, it has become even more essential to safeguard oneself from the potential cyber risks.

Speaking about the lack of preparedness, Mr Adidamu said: "It is alarming to see this lack of preparedness, which is leading to the increase in frequency of cyber attacks. You can't predict when your computer system will be compromised, hence one needs to assume that they are always under attack."

"There needs to be a strong recovery plan and one must have back-ups in place. There is a need to constantly change and evaluate the infrastructure and prepare a framework to tackle these hostile forces online. Continuously updating and upgrading our defences is the only way to guard against the emerging new type of cyber risks," he added.

Responsibility of the entire society

Just like in any society, there will always be good and bad elements in online society as well. Developing this society, the right way is a combined responsibility to be shouldered on all the internet users and institutions including legal, regulatory and judicial institutions.

Mr Adidamu concluded by saying: "While insurance can help safeguard against the risks and contribute by implementing the best practices, developing them remains a monumental task which will need to be tackled by society at large."