CYBER INSURANCE: GETTING IT RIGHT

Anamika Kumari *examines the outlook for the evolution of the cyber insurance market*

The cyber insurance market is constantly evolving as a paradoxical segment where fear continues to drive custom, while conversely industry inefficiency ensures growth of the insurance industry. Whether large corporations or small-to-medium-sized enterprises, consumers understand the key importance of data that they operate on or possess. And yet the apparent cyber resilience is not enough cover for the nodes of vulnerabilities.

Stories about major cyber breaches are popping up in the news with alarming regularity. Yahoo and Anthem recently surfaced as high-profile examples of the undesirable chain of events that can tarnish the reputation of a major corporation and disrupt its operations with just a single hack. This has generated a considerable amount of fear. Being inspired by the concept is one thing, being foolish enough to refute the chances of falling victim to a cyber incident is a different thing altogether. Fortunately, the leading organisations are wise to understand the difference.

The element of fear stands as the keystone to the terrific growth of the global market. It is a rat race out there, with cyber insurance seekers and providers trying to connect with one another. However, the participants of the race, which was triggered out of fear, were not aware or prepared for the hurdles ahead. This is the primary reason as to why the market faces several issues within its functional structure.

IMPROVING AWARENESS

Without exception, across geographical regions and business groups there exists extremely low levels of awareness among the present generation of users and providers with regard to the competencies of cyber insurance policies. It could be considered as a general shortcoming on the beneficiaries account, but the operations of the entire industry come under the spotlight if cyber insurance providers fall short on their side of the service.

The brokers need to improve their visibility and at the same time be able to explain the consequences of uninsured exposure to cyber threats. In addition, they need to be able to fully outline the aftermath of a third-party breach even when a comprehensive policy covers the organisation. When this is not the case, it becomes essential for people to recount these consequences, which are liable to put the organisation through additional havoc in the event of being a victim of a cyber hack.

However, the brokers and finance agencies are not the only ones to blame. Reluctant and resilient prospective beneficiaries are equal participants in the shabby state of the global cyber insurance industry.

In November 2016, Tesco Bank stopped online payments for current account customers after hackers stole money from 20,000 accounts

Picture credit: Getty

The first step to a successful contractual coverage is the end-to-end understanding of the associated risks before market entry, and not just for the beneficiaries. The providers need to attain equivalent level of proficiency in order to be able to guide better. When this isn't the case, it is safe to consider that the chain of problems has just begun.

The global market is flooded with small-scale and distributed cyber insurance brokers with limited knowledge of the extensive field in which they are dealing. Experts identify that the desire for broad profit margins is the primary reason behind the mushrooming of several small-scale organisations. On the other hand, the insurance seekers hit a dead end when these services fail to handle all of the loose ends during a crisis.

There is always more than meets the eye, and in the case of cyber insurance coverage it is vital to consider the small print. Most insurance seekers realise too late that the policies they signed up for do not completely cover their risks. Geographical boundaries generally define the exclusive clauses. Once people fully understand that the insurance against the usage of the 'world wide web' does not necessarily cover the entire globe format, they begin to realise that they should have taken more care to read the offer document more than once – by which time it will all too often be too late. There is no help with the limited coverage offered by the handful of broking agencies, but the very least that can be done is to be fully aware of what one is getting into.

It is completely unrealistic for enterprises to boast about every other security measure that has been undertaken to ensure that its organisational assets are safe and intact when the bigger picture has not been fully considered. Most will go rambling on about the innovative technical facilities introduced to upgrade their operational procedures. Taking big data management and storage to the cloud is indeed contextual to upgrading in industry status. It increases the trust factor among the clients and gives them the idea that they are being associated with the best in class.

However, risk mitigation officers find it much more difficult to get the organisations onboard when it comes to cyber risk management and pertinent insurance. What they do not realise is that being

STORIES ABOUT MAJOR CYBER BREACHES ARE POPPING UP WITH ALARMING REGULARITY

equipped with a policy will provide far better control over the projected risks, and they can then advertise their insurance cover to convert a large number of client queries.

AVOID COMPLACENCY

Unfortunate as it might sound, the enterprises live in a confidence bubble that is not impervious to the security risks that exist around them. As per general conception, they like to think that their in-house IT facilities are sufficiently adept at handling the probable security risks. This is not definitive, of course. Despite a strong internal protective mechanism being put in place, becoming over confident or complacent is really the last thing that is needed.

A single external bug is more than enough to destroy both a business' reputation and rapport in one fail swoop. Apart from losing the entire clientele, organisations can also face legal charges for irresponsible, unprofessional conduct. Before you know it, the true costs of the lapse in judgment will be soaring out of control.

So, are we to conclude that the broking agencies have been inefficient so far in meeting customer expectations? Yes. Does that imply that users will drift away from the service and refrain from availing it in the future? No. With a just few simple amendments made to the current situation, the functional channels can be straightened out to work in a perfect state of harmony.

Unlike the majority of horizontal industries, the cyber insurance market is one among the few in the IT arena that is yet to settle in terms of commodity flow and distribution structure. The standards of operation and the regulations pertinent to the segment remain to be fully put in place. There exists immense scope for improvisation, innovation and customisation in product and service modules. With enough deliberation the financial agencies

and the financial institutions, in collaboration with the federal organisations, should be able to resolve the loopholes in regulatory formats through making unified decisions.

The small-scale distributed brokers have the option of collaborating with other firms. This move will help them to build on their knowledge and provide informed insurance advisory services. With proper inferences drawn from their collective experience, everyone should stand to benefit. The events following unattended system components or access nodes is on the users. The blame is on them for being unable to employ active software solutions to properly protect their data storage and exchange mediums. However, it must be the partial responsibility of the advisory groups to help them pick out the right protection tools for the job.

A SINGLE EXTERNAL BUG IS MORE THAN ENOUGH TO DESTROY A BUSINESS' REPUTATION

Talking of shared responsibilities, chief risk officers must take a stand regarding the needful. They must perform whatever it takes to convince the decision makers to opt for a comprehensive cyber insurance policy. They need to draw up a convincing case to fully explain the vulnerable fronts and the correct software tools that can add to the in-house security assurance. Once persuaded, the next step involves choosing the best-suited security applications to preserve access within a desired community of users. This is a complimentary addition to the policy, which ensures that when an incident occurs, the organisation has the advantageous edge and not the insurance provider.

Where all fear fails, law prevails. Regulating trade practices by the force of federal regulations is not new. Apart from setting up regulatory frameworks to decide what clause inclusions are being made, governments could also focus on mandating insurance policies for those enterprises that deal beyond a certain level of public data. The organisations could be forced to function only after they compliantly get themselves insured by a registered agent or agency. This would be for the greater good and security of the nation, as well as being viewed in complete goodwill. Cyber insurance providers would eventually offer enhanced and cost-competitive services.

GETTING IT RIGHT

As per the latest report released by Allied Market Research, the global cyber insurance market looks set to generate revenue worth $14 billion towards the end of 2022. Industry analysts estimate that the market will grow at a CAGR of 28 percent during the forecast period 2016-2022. The costs of availing cyber insurance policies are extremely high, with around 50 percent accredited to broker margins. And that is when most of them are not even the masters of the game. The industry vendors and those related need to work upon the stabilisation of surge in costs or bring the wide gap in service and prices to a point where they are on a par with each other. If they don't, the consequences could be very dire indeed ●

Anamika Kumari is a content writer at Allied Analytics LLP. She is deeply fascinated by the impact of modern technology on human life and the earth at large. Being a voracious reader, passionate writer and a critical observer of market dynamics, she has a strong taste for the hidden science behind all arts.

Picture credit: Getty

Yahoo is another large corporation to have suffered the humiliation of becoming a victim of cyber crime