CYBER-INSURANCE: NEED OF THE HOUR?

Written by ***Shilpa Sai***

5th Year B.B.A L.L.B. (Honours) Student, School of Law, Christ University

ABSTRACT

There have been a lot of instances of hacking of databases & databanks and spreading of viruses to erase all the data possessed by individuals or multi-national companies. With the increase in the use of crypto-currencies, the crime of crypto-jacking is on the rise.

The ransomware attack in the year 2018 shook companies across the globe. Multi-National Companies which run on Big Data and their businesses that are solely dependent on their databases, were affected. A ransomware attack is when a virus is spread, to latch onto to confidential information of companies, which can only be removed upon meeting the cyber-attacker's demands. Similar to ransomwares, are malware attacks, which are attacks where certain computer soft-wares are created, just to disrupt or corrupt the memory of databases, causing loss of information.

In the 21st Century, data and information is all what the world survives on, and any loss of data can prove to be fatal. There is a lot of money involved in the processing and accessing of data, and hence, the Insurance sector has seen a rise in the concept of cyber-insurance.

With an already prevalent Insurance sector, the author would like to bring to light, the niche created by cyber-insurance in the insurance market, examine the fundamental difference and relationship between cyber-insurance and cyber-security in order to establish the reasons as to why they are indispensable to each other, being independently, equally important.

Key Words: cyber-insurance, cyber-security, insurance sector, cyber-crimes, legal development.

INTRODUCTION

ISSN 2581 3382

There have been a lot of instances of hacking of databases & databanks and spreading of viruses to erase all the data possessed by individuals or multi-national companies. Furthermore, with the increase in the use of crypto-currencies, the crime of crypto-jacking is on the rise.

This article primarily focuses on elucidating what cyber-insurance is and why is it imperative to be cyber-insured against a host of cyber-crimes, in the current times.

The Insurance Regulatory Development Authority of India (IRDAI) does not make a mention of what Cyber-insurance is and hence, there are no strict policies, rules or regulations to that effect to regulate the cyber-insurance sector in India.

Based on a preliminary research on Cyber-insurance policies in India, it was found that, a lot of private entities that deal with general and life insurances are now expanding their business portfolios to include Cyber-insurance as a product to offer.

Cyber-insurance

A cyber insurance policy, also referred to as cyber risk insurance or cyber liability insurance coverage (CLIC), is designed to help an organization mitigate risk exposure by offsetting costs involved with recovery after a cyber-related or internet based security issues and threats, security breach or similar events.[i]

Cyber insurance typically includes indemnification from lawsuits related to data breaches, such as errors and omissions. It also covers losses from network security breaches, theft of intellectual property and loss of privacy.[ii]

With its roots in errors and omissions (E&O) insurance, cyber insurance began catching on in the year 2005, with the total value of premiums forecasted to reach $7.5 billion by 2020. According to PwC, about one-third of U.S. companies currently purchase some type of cyber insurance.[iii]

Cyber-insurance is generally taken by big organizations that handle big-data, huge databases, cloud-computing software, essentially everything that is dependent on the internet and cyber-based work.

ISSN 2581 3382

Cyber-insurance can be considered as a contract of indemnity because, here the subject-matter being data, the loss of which can be quantified in terms of numbers and hence can be indemnified, unlike in the case of life insurances.

The need for cyber-insurance

Now that we have discussed what cyber-insurance is, it is prudent to ask, "why do we require cyber-insurance?" Well, the answer to that question is, just like any other insurance policy, where some are purely for investment purposes and some are for actual coverage of loss due to fire, rain, motor-vehicle accidents, etc., cyber-insurances are usually taken to cover or indemnify for the losses caused due to loss of information, hacking of databases and other allied damages borne by the insured because of the cyber-attack.

The intensity of the damage that is usually caused by cyber-attacks may not be fathomable by a lay-person at the moment because the realm of cyber-attacks hasn't percolated into the common man's domain yet. But, if the companies, individuals and organizations that deal with data, or any category of information that requires for it to be on the internet, gets hacked or deleted or there is a loss in the data which causes substantial damage to the capital and resources of such an entity are to comment on this issue, they would elucidate the necessity of a cyber-insurance.

Data which is present on the internet is very volatile and susceptible to be hacked.

Cybercrime is always in the news off-late. The ransomware attack- WannaCry that struck users and firms across the world, impacted over 2,00,000 computers in over 150 countries of the world. This cyber-attack held these victims to a ransom and at the mercy of the cyber-attackers.[iv]

While this incident might have brought the matter back into the limelight, cybercrime is already a day-to-day phenomenon. More than 4,000 ransomware attacks occurred every day across the globe in 2016 — up from 1,000 attacks a day in 2015. Cybercrime damages costed the world $3 trillion in 2016; this figure will rise to $21 trillion, according to experts. Further, cyber malwares are spreading to smartphones and other devices[v].

Indian companies and users are equally at risk. At nearly the same time when the ransomware attack occurred, 17 million user records were stolen from a prominent Indian food portal,

ISSN 2581 3382

despite these being stored in an encrypted format. We have already witnessed one of the biggest ever breaches of financial data involving 3.2 million debit cards in India in October 2016.[vi]

During a survey conducted by PwC's 18th Annual Global CEO Survey, to which 1,322 CEOs participated, 71% of insurance CEOs, 79% of banking CEOs (the highest of any sector) and 61% of business leaders across all industries saw cyber-attacks as a threat to growth, ranking it higher than shifts in consumer behaviour, the speed of technological change and supply chain disruption.[vii]

Hence, the necessity of cyber-insurance has been manifested by the top management of various sectors of the economy as they have realised the importance of it, and the gravity of the situation that would trail, if one fails to take cyber-insurance.

Legal position of cyber-insurance in India and in other jurisdictions

India

In India, there are absolutely no legislations enacted by the Parliament or guidelines or notifications or regulations issued by the IRDAI with reference to cyber-insurance.

Let alone regulations or guidelines, there isn't even a mention of cyber-insurance on the official website of IRDAI.

But, for the first time in 2017, individuals can buy insurance cover against cybercrime, including loss of funds to online fraud, identity theft, cyberstalking and extortion, phishing and malware attack. The Cyber Safe policy designed by Bajaj Allianz General Insurance is aimed at improving the level of comfort among individual internet and e-commerce users.[viii]

United States of America

In contrast, in the United States of America, the first set of "internet insurance" covers were introduced in the late 1990s to tackle exposures to online content or software. These covers were offered as an extension under professional indemnity policies with smaller limits. With the enactment of data privacy law in the US, a stand-alone cyber insurance product was formulated[ix].

ISSN 2581 3382

In a recent effort to strengthen its cyber security laws, the federal government of the US had introduced several new cyber security laws as well as amending the older ones for a better security ecosystem. Below are a few of them[x]:

Cybersecurity Information Sharing Act (CISA) – Its objective is to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes. The law allows the sharing of Internet traffic information between the U.S. government and technology and manufacturing companies. The bill was introduced in the U.S. Senate on July 10, 2014, and passed in the Senate October 27, 2015

Cybersecurity Enhancement Act of 20141: It was signed into law December 18, 2014. It provides an ongoing, voluntary public-private partnership to improve cybersecurity and strengthen cybersecurity research and development, workforce development and education and public awareness and preparedness.

Federal Exchange Data Breach Notification Act of 2015: This bill requires a health insurance exchange to notify each individual whose personal information is known to have been acquired or accessed as a result of a breach of security of any system maintained by the exchange as soon as possible but not later than 60 days after discovery of the breach.

National Cybersecurity Protection Advancement Act of 2015: This law amends the Homeland Security Act of 2002 to allow the Department of Homeland Security's (DHS's) national cyber security and communications integration centre (NCCIC) to include tribal governments, information sharing, and analysis centres, and private entities among its non-federal representatives.[xi]

At present, the principal cover under the policy is for damages and legal costs in connection with a data breach. It also pays for various costs associated with the company, negating an impact on its reputation — that is, costs for notifying customers, hiring reputation management agencies and credit monitoring services for affected customers. In addition, the policy pays for cost of forensics investigation and expenses incurred in recreating any lost data. In case of a cyber extortion situation like in the case of WannaCry, the policy would pay the ransom as well as costs of a specialist engaged to handle such a situation. In case of an outage of services (denial of service attacks) due to a cyberattack, loss of profits are also covered.[xii]

ISSN 2581 3382

United Kingdom

The Department for Digital, Culture, Media and Sport (DCMS) made the admission in a paper setting out its plans to implement the EU's Network and Information Security (NIS) Directive into UK law.[xiii]

The Network and Information Systems Regulations 2018 (NIS Regulations) came into effect on 10 May 2018 pursuant to the Cybersecurity Directive (also known as the Network and Information Security or NIS Directive). They have potential impact on businesses that rely on IT systems in the following sectors: energy, transport, health, drinking water supply and distribution, digital infrastructure (OESs) and online marketplaces, online search engines and cloud computing services (DSPs). Like the General Data Protection Regulation (GDPR), the NIS Regulations impose security and incident reporting requirements and provide for high penalties (up to £17,000,000 in the case of the NIS Regulations), but their focus is on security of IT systems, rather than security of the personal data processed by those systems, but in practice the two regimes are inextricably linked. OESs and DSPs must comply with notification and registration requirements before 10 August 2018 and 1 November 2018 respectively.[xiv] According to the DCMS, fines will only be served as a "last resort" and will not be issued where operators of essential services "have assessed the risks adequately, taken appropriate security measures and engaged with regulators but still suffered an attack". Under the new UK regime, different 'competent authorities' will have responsibility for monitoring compliance and enforcement depending on which sector organisations subject to the rules operate. Government ministers for energy, health and transport, for example, will act as competent authorities, as will industry regulators Ofgem and Ofcom and data protection watchdog the Information Commissioner's Office (ICO).[xv]

What is the difference between cyber-insurance and cyber-security?

Fundamentally and etymologically there is no difference between the two – cyber-insurance and cyber-security.

But legally speaking, as the name suggests, cyber-insurance is a product of the Insurance Companies which is open for the customer to take and get indemnified on the happening of the event as mentioned in the insurance policy, whereas cyber-security on the other

ISSN 2581 3382

hand is just a safety precaution or mechanisms undertaken by individuals or entities to avoid or mitigate the monetary damage that they would face due to cyber-attacks.

Though different, they are ultimately inseparable because concept-wise, these two are terms that always go hand in hand. One cannot exist without the other, in theory or in use.

Market share market penetration / of cyber-insurance in the Insurance Sector Though cyber risk is acknowledged as a critical threat to business today, investments in cyber insurance remain small. The global cyber insurance market is estimated at $4 billion and is expected to grow to $20 billion by 2025. The Indian cyber insurance market stands at approximately 300 million and should expand to approximately 750 million by 2020. While these forecasts convey a major uptrend, they may not be sufficient given that technology-related risks will only grow in size and frequency in the new tech era. More importantly, this new-age risk is vastly different from traditional risks such as fire or marine losses. It does not remain confined to a pattern nor can it be entirely restricted by a defined set of preventive actions.[xvi]

Cyber-insurance can still be considered as a baby in the Insurance sector. Insurances like marine insurance, general insurance, life insurance, etc., have been present for a substantial amount of time due to which, it is evident that they do consume most of the market share.

But cyber-insurance like technology, will soon become indispensable to the lives of all organizations and maybe also private entities, who may have majority of their interests vested in the cyber-world.

Conclusion

Cyber-insurance is an emerging trend and soon will be one of the most availed insurance policies, there is.

Cyber-insurance and cyber-security go hand in hand. It finally boils down to the fact that, Cyber-insurance is a type of cyber-security and cyber-security means cyber-insurance. They are indispensable to each other.

Cyber-insurance shall soon become a crucial product of the insurance sector. Currently, due to the lack of a proper legal framework on the said subject matter, there is still a shade of scepticism to invest in that market. But once that issue is taken care of, by the way of

ISSN 2581 3382

legislations on that matter, cyber-insurance will be seen with a different approach altogether.

The moment there is a legal backing for a particular emerging venture, the potential investors start gaining confidence in it.

Regulations or legislations would also need to put in place the aspect of liabilities and strict adherence policies, in order to facilitate better enforcement of the same.

In conclusion, although no insurance policy is not mandatory in nature, it is always wise to invest in one, as in the event of an unforeseen situation, a cyber-insurance would help in mitigating the losses that would have to be borne by the victim of a cyber-attack.

REFERENCES

[i] Kim Edros and Ed Tittel, What is Cyber insurance and why you need it? CIO from IDG. Retrieved from https://www.cio.com/article/3065655/cyber-attacks-espionage/what-is-cyber-insurance-and-why-you-need-it.html (accessed September 2, 2018)
[ii]Cyber Insurance, Techopedia. Retrieved from https://www.techopedia.com/definition/32532/cyber-insurance (accessed September 2, 2018)
[iii] *Supra* at n.1
[iv] Bhargav Dasgupta, India Inc must step up on cyber insurance, ICICI Lombard Blog. Retrieved from https://www.icicilombard.com/experts-blogs/story/india-inc-must-step-up-on-cyber-insurance, Original Source – Business Standard (accessed September 2, 2018)
[v] *Supra* at n.4
[vi] *Id.*
[vii] Insurance 2020 & beyond: Reaping the dividends of cyber resilience, PwC Publication, P 9. Retrieved from https://www.pwc.com/gx/en/insurance/publications/assets/reaping-dividends-cyber-resilience.pdf (accessed September 5, 2018)
[viii] Mayur Shetty, In a first, cybercrime insurance cover for individuals, Economic Times. Retrieved from //economictimes.indiatimes.com/articleshow/61476025.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst (accessed September 5, 2018)

[ix] *Supra* at n.4
[x] A Glance at the United States Cyber Security Laws, Appknox. Retrieved from https://blog.appknox.com/a-glance-at-the-united-states-cyber-security-laws/ (accessed September 5, 2018)
[xi] *Id.*
[xii] *Supra* at n.4
[xiii] UK finalizes plan to implement new cybersecurity laws, Out-Law.com, (last seen 5 September 2018, 9:24 PM), available at: https://www.out-law.com/en/articles/2018/january/uk-finalises-plans-to-implement-new-cybersecurity-laws/.
[xiv] Phil Thompson, Partner, and Nick Mathys, Partner, White & Black Limited, UK Cybersecurity Law, Practical Law, Thomson Reuters, (last seen 5 September 2018, 9:18 PM), available at:

ISSN 2581 3382

https://uk.practicallaw.thomsonreuters.com/5-616-1485?transitionType=Default&contextData=(sc.Default).

[xv] *Supra* at n. 12.
[xvi] *Supra* at n.4

ISSN 2581 3382