TRADEMARK IN THE ERA OF SOCIAL MEDIA

Written by ***Shubham Sharma***

BA LLB Graduate, NALSAR University of Law

INTRODUCTION

Insurance is a means to indemnify the loss suffered by the assured, Origins of insurance law took place on the high seas as a means of reducing the risk a merchant took, theses were "bottomry contract" where it was understood that if shipments were lost at seas loans did not have to be repaid.[i] The first insurance companies started after the Great Fire of London in 1666, from there the insurance sector expanded and branched off into many fields.

With the advancements in technology and the creation of Information Technology business have under gone a change in how they operate, businesses have moved there actives online such as keeping accounts, digital marketing, social networking, digital communication and cloud computing, trade secrets and plethora of other actives. The Information Technology sector possess its on forms of risk for business. These threats are in forms of cyber attacks which can result in the loss of Data, malware attacks can cause various problems such as but not limited to hindering a company's ability to conduct business , IT theft loss, phishing, cyber extortion, , e-mail spoofing and cyber stalking, Cyber Attacks cause more intangible loss to a company then physical damage.

Cyber frauds are globally one the fast emerging threat business and specifically to financial institutions such as banks, Financial advisers and stock exchanges where data is as valuable as gold. India is of the most heavily cyber targeted country in the world in 2011 it ranked number 10[ii]. As of 2018, within the last 12-18 months it has been estimated that Indian companies have incurred nearly 500,000 USD worth of damages due to cyber attacks[iii]. Therefore, more and more companies are moving towards cyber insurance. Cyber insurance is a forum of insurance which has been tailor-made of the IT sector which offers comprehensive cover for third party liability and first party expenses in case of unauthorized access or use of physical or electronic data. Cyber Insurance provides coverage incase liability arises if there is data destruction, theft, extortion, denial of service attacks and hacking. Cyber insurance is not limited by damages,

© thelawbrigade.com

the coverage is expanding to cover for business interruption, cost of notifying customers and regulatory investigations.

POLICY COVERAGE

Cyber Insurances, is a new field of insurance, which is still under development, there are various questions as to what policy should be adopted by a company. As data breaches occur more frequently, businesses are under additional pressures to step up efforts to protect personal information in their possession. Every company had different needs with respect to what form of coverage they need. Large Companies and Institutions like banks are targets of cyber attacks, however it is estimated that a large number of cyber attacks occur on small business as, they are easy targets[iv]. Smaller business is often reluctant to look for coverage they need, or may buy coverage they don't need due to a lack of clarity as to what is possible in the industry, which coverage covers which risk. Most common types of risk associated with cyber insurance are as follows[v]:

1. ***Identity theft:*** Is a form hacking where sensitive information is stolen form by a hack or is disclosed inadvertently, the information stolen can be in such forms as Social Security(vaguely similar to addhar) numbers, employee identification, credit card numbers, PIN numbers, drivers' license numbers or any information relating to ones identify which is stored in form of IT
2. ***Business interruption:*** is a form of an attack which hampers the daily function by causing the network to slow down or shutting down completely.
3. ***Reputation:*** Cyber attacks can cause damage to the firm's reputation by various means, such as removing trust over the company by stake holders or public, or by leaking sensitive information about the companies doing.
4. ***Data cost:*** When an attack leaves damages to the data records, costs associated with recover and restoration.
5. ***Theft of assets:*** Where sensitive digital assets such as business trade secrets, customer list, dealing and other electronic business assets are stolen, the damage caused by the leak of such information.

© thelawbrigade.com

6. ***Malware:*** Where the host computer system is infected by malware, worms and other malicious computer code.
7. ***Human error:*** an inadvertent disclosure of sensitive information to an unintended party
8. ***Privacy and notification:*** cost of notifications to the affected parties and customers parties post a breach.
9. ***Lawsuits and extortion***: Cost of expenses due to cyber extortion, legal settlements and regulatory fines, legal expenses incurred due to theft of intellectual property and confidential information.

Commercial insurance policies in the United States provide for general liability coverage which is a protection from injury or property damage. However, these policies do not cover cyber risks which have been mentioned above. Therefore, to cover for cyber risk there you would need to purchase a specific cyber insurance policy which will cover the special cyber liabilities. However, cyber liabilities pose a challenge for insurance underwrites, traditionally in a general policy through statistical calculation of risk or life expectancy one can qualify for a cretin policy, this is based on the insurers redness to take the risk of covering that entity or individual. In cyber liability there is an inherent lack of actuarial data which leads to difficulties in quantifying the damages for the underwrites. This has led to highly customized policies for cyber risk which are costlier as it involves a greater risk on part of the insurance company. The customization depends largely on the type of business operations size and scope of the business, as a finance company would be riskier to insure vs. a small family owned business. each of these factors play a role in coverage needs and pricing.

Currently, the cyber insurance sector is lacking, as of 2017, 200 cyber insurance policies have been sold throughout India; despite the fact Indian companies are more prone to cyber attacks. as of 2011 India was the 10th most effected country by cyber attacks. Coverage offered by Indian insurance providers such as Tata AIG, HDFC Ergo, Bajaj Allianz and ICICI Lombard provide a coverage for the following liabilities[vi]. Firstly, Investigation, determining the cause of cybercrime and preventive solutions to insure protection against reoccurrence of such cybercrimes. secondly, covering Business losses due to third party attacks as well as of negligence due to human errors which results in monetary losses due to network downtime,

© thelawbrigade.com

data loss recovery, business interruption and costs involved in managing a crisis. third, covers the cost of privacy and notification to customers and other affected parties. lastly covers the liability in case of a lawsuits and extortion.

The coverage varies from business to business, however cyber insurance policies India are around Rs.15 crore with a premium range of Rs.15 lakh to Rs.1 crore, the premium is heavily depended on the size of the coverage and risks involved. [vii]

CASE LAW

In the case of *Columbia Casualty Co v Cottage Health System*[viii], coverage was denied because the insured did not comply with the underlying obligations. In this case the insured did not meet the cretin technical standards of procedures and risk controls, which meant that there was an obligation on part of the insured to meet and follow minimum required practices.

In the case of *P.F. Chang's v Federal Insurance Co*,[ix] coverage denied because the wrong party was injured. In this instant case P.F. Chang's, the insured made an insurance claim due to breach of data which had resulted in the loss of customers personal data. However since P.F Chang did not suffer any injury do to the loss of data the courts concluded that the insurance policy did not cover damages to third party, the policy required the injury to be suffered by the claimant, P.F Chang. The policy at issue was marketed as "a flexible insurance solution designed by cyber risk experts to address the full breadth of risks associated with doing business in today's technology-dependent world."

In case of *Zurich American Insurance Co v Sony Corp of America et al*[x], coverage was denied because the wrong part was Injured. In the present case a claim was made by Sony with respect to damages for defense and indemnification caused by loss of data breach due to criminal hacking. The policy to which Sony was subscribed to covered damages caused by "oral or written publication in any manner of the material that violates a person's right of privacy.", if these publications were made by Sony. However, since the publications were made by a criminal hacker and not Sony the policy did not cover this situation hence the court held, that since the publication were not made by Sony, there was no obligation to indemnify Sony.

© thelawbrigade.com

The *Apache Corp v Great American Insurance Company*[xi] case created a diffraction between use of computers and loss incurred due to Information Technology, the case ruled out coverage of activates which were merely incidental to cyber activities. It was state that a cyber security insurance coverage would only cover loss which occur as a result of cyber activities. In the present case, the insured was defrauded, the insured became a victim after an employee wrongfully determined that a vendors phone and email request to transfer money were authentic requests. therefore the insured claimed loss under "loss of, and loss from damage to, money, securities and other property resulting directly from the use of any computer to fraudulently cause a transfer…". It was held by the courts that the present circumstances were not covered because the merely using a computer does not amount to cyber activities, the cause of the damage has to be a direct result of the loss, and not merely incidental. However, One could argue that the cause of the damage resulted in the negligence of the employee, which is a covered risk under cyber risks. But in the present case, the activities were not limited to solely cyber activities, as there were intervening steps of the [post-email] confirmation phone call and supervisory approval.

In a first of its type, the District Court of Utah , USA, In the judgment of *Travelers Property Casualty Company of America v Federal Recovery Services Inc*[xii] held that a cyber insurance claim does not arise out of alleged misuse of data. The insured made claim for the cost o litigation resulting from a tort claim for intentional misuse of data storage activities. The claim was denied by the insurance company on the grounds that the policy only provides for coverage, if the loss was caused by "any error, omission or negligent act." The courts held that since "knowledge, willfulness, and malice" were not covered under the policy the claim would fall. Through this, it can be understood that a insurance can provide for coverage of certain claims while excluding others.

BUYING CYBER INSURANCE

For purchasing cyber insurance, a buyer needs to do due diligence with respect to the policy they my enter into, as it was disused in the case laws above, it is important to the know the extent of coverage your policy provides to ensure it caters to the needs of the company.

© thelawbrigade.com

1. whether the insurance company offer one or more type of cyber policy, if the policy is an extension on an existing policy or if it is a standalone policy. Most of the times a stand-alone policy is the best option as it is more comprehensive. to what extent the policy is customizable to suit the needs of an organization.
2. What are the deductibles?
3. To what extent does the coverage and limits apply to both first and third parties? whether the policy cover third-party service providers.
4. If the policy covers any form of cyber attack against that sector of business or if the policy only covers direct attacks against the organization.
5. If the policy covers non-malicious actions by an employee, due to negligence or human error.
6. Does the policy cover social engineering attacks such as phishing or advanced persistent threats (APTs) along with network attacks?
7. Whether in cases of APTs, which can take months if not years cause damage, does the policy create a time frames within which the coverage takes place, to ensure damage done can be rolled back to the date of hacking.

BEST PRACTICES TO REDUCE RISK

Best practices are set of "things to do", services to implement, steps you take, actions and plans, risk management and claims mitigation techniques a company adopts to protects themselves from cyber attacks. From the perspective of an insurance company, they want to reduce the risk they take, so if a company follows the best practices and has assessed its vulnerability to cyber attack they would get a better policy with has more coverage and lesser premium. As of now there is no set standard for best practices, however while refer to cyber security laws you can identify some best practices[xiii]:

1. Create a corporate security policy and ensure all you employees understand and follow them.

© thelawbrigade.com

2. Train employees in security protocol such as acceptable use, password polices, defenses against social engineering and phishing attacks.
3. Encrypt the data you have stored, especially sensitive data
4. Create a backups of your data and regularly back up your data and have a re-image tools at your disposal.
5. Test your system frequently to insure back up and re-imaging perform as expected
6. Prevent malicious insider action by screening you employees
7. Use network access control (NAC) to defend your network behind firewalls to block any unauthorized access from third party devices.

Therefore, it is understood that for an insurers writing the coverage, there first concern would be risk-management techniques that the company has adopted in order to protect its network and its assets. A business' disaster response plan would be evaluate enlight of the business' risk management of its networks, Intellectual property, its physical assets, and its website. Thirdly, who is able to access the secured data, whether its limited to employees or third party service providers are able to access the data. At the very least information about they type of t antivirus and anti-malware software that is used by the company and the performance of inbuilt systems such as firewalls would all be a factors which will contribute to risk management, in order to evaluated the effective policy coverage.

CONCLUSION

Cyber insurance is an emerging field, currently countries are grappling to find effective regulatory framework to regulate the sector and set industry standers to prevent either the insurer or insured form loss. there are still confusion on basics of coverage for cyber attacks, according to a Greyhound survey, *State of Cyber Insurance,2017,* companies are still see errors and omissions (E&O)[xiv] insurance and cyber liability insurance coverage (CLIC)[xv] are similar, hence they are covered by one policy. Cyber insurance is still maturing, it is projected[xvi] that every company in one form or another will have cyber insurance, this will cause an industry wide standardization, which will resolve the preliminary doubts that priest today and also lead to more affordable insurance coverage as premium prices drop.

© thelawbrigade.com

REFERENCES

[i] Encyclopedia Britannica. (2018). *Insurance - Historical development of insurance*. [online] Available at: https://www.britannica.com/topic/insurance/Historical-development-of-insurance

[ii] Bharadwaj, S. (2016). CYBER LIABILITY INSURANCE IN INDIA: GROWING IMPORTANCE. *Imperial Journal of Interdisciplinary Research*, [online] 2(1). Available at: https://www.onlinejournal.in/IJIRV2I1/004.pdf [Accessed 14 Apr. 2018].

[iii] Anon, (2018.). *Indian companies lost $500,000 to cyber attacks in 1.5 years: CISCO*. [online] Available at: https://economictimes.indiatimes.com/tech/internet/indian-companies-lost-500000-to-cyber-attacks-in-1-5-years-cisco/articleshow/63019927.cms.

[iv] Vox Creative. (2018). *Why every small business should care about cyberattacks, in 5 charts*. [online] Available at: https://www.vox.com/sponsored/11196054/why-every-small-business-should-care-about-cyber-attacks-in-5-charts

[v] Harrigan, B. and Miliefsky, G. (2016). *Best Practices in Cyber Security*. [online] InsuranceThoughtLeadership. Available at: http://insurancethoughtleadership.com/best-practices-in-cyber-security/ [Accessed 14 Apr. 2018].

[vi] *Cyber attack: Bajaj Allianz launches first cyber insurance cover*. [online] Available at: https://www.businesstoday.in/sectors/banks/bajaj-allianz-cyber-attack-cyber-insurance-cover--malware-attack-financial-loss-it-theft/story/263228.html.

[vii] Gonsalves, R. (2017). *All you need to know about cyber insurance*. [online] Cafemutual. Available at: http://cafemutual.com/news/insurance/8635-all-you-need-to-know-about-cyber-insurance [Accessed 14 Apr. 2018].

[viii] *Columbia Casualty Co v Cottage Health System*: No. 2:15-cv-03432 (C.D. Cal.) (filed May 7, 2015).

[ix] *.F. Chang's China Bistro, Inc. v. Federal Insurance Company*, No. 15-cv-1322 (SMM), 2016 WL 3055111 (D. Ariz. May 31, 2016),

[x] Zurich American Insurance Co v Sony Corp of America et al N.Y. Sup. Ct. Feb. 21, 2014)

[xi] *Apache Corp. v. Great American Insurance Co.*, No. 15-20499, 2016 WL 6090901 (5th Cir. Oct. 18, 2016).

[xii] *Travelers Property Casualty Company of America, et al. v. Federal Recovery Services, Inc., et al* (Case No. 2:14-CV-170 TS)

[xiii] G. Miliefsky**.** *Leveraging Best Practices in Cyber Security*. [online] Available at: http://insurancethoughtleadership.com/best-practices-in-cyber-security/.

[xiv] E &O, also known as a professional liability insurance protects against losses from negligence claims made by a client.

[xv] CLIC covers technology related losses.

[xvi] Sharma, S. (2018). *Cyber risk insurance in India: More window shoppers than converts even after attacks | FactorDaily*. [online] FactorDaily. Available at: https://factordaily.com/cyber-risk-insurance-india/

© thelawbrigade.com