Imperial Journal of Interdisciplinary Research (IJIR)
Vol.2, Issue-1 , 2016
ISSN : 2454-1362 , www.onlinejournal.in

CYBER LIABILITY INSURANCE IN INDIA: GROWING IMPORTANCE

Sree Krishna Bharadwaj H

BBA LL.B. (Hons.), LL.M., PGDHRM

Abstract

There is always a threat to the protection of data of either individual or company especially in country like India where there is improper control over the cyber technology and ineffective dealing with cyber crimes. This paper explores the growing importance of cyber liability insurance in India.

1. Introduction

In 2010-11, India was the 10th, a lot of heavily cyber-attacked country; today it is additional abandoned to United States. With internet acceptance ascent exponentially-from 202 actor users in march 2010 to 412 million in advance 2011 to 485 million in march 2012, India is now additional abandoned to China in the bulk of devices(including corpuscle phones) affiliated to the internet.

This aswell makes India abnormally vulnerable. Intelligence antecedent say that, in the contempo past, awful activities adjoin Indian networks accept originated from hosts in 20 countries: Emphasizing the baggy attributes of cyber-attack, sources analyze that could accept been baffled through those countries after the hosts even getting acquainted of this activity. During the aforementioned period, several attacks away were detected as basic from hosts amid in India. [1]

2. Definition

The appellation " Cyber liability insurance" is generally acclimated to alarm an ambit of covers - in actual abundant the aforementioned way that the chat cyber is acclimated to alarm an ample ambit of advice aegis accompanying tools, processes and services.

At the moment, cyber accountability insurance awning can include:

Data breach/privacy crisis administration cover: For example, costs accompanying to the administration of an incident, the investigation, the remediation, abstracts accountable notification, alarm management, acclaim blockage for abstracts subjects, acknowledged costs, cloister appearance and authoritative fines.

Multimedia/Media accountability cover: Third-party amercement covered can awning specific birthmark of website and bookish acreage rights infringement.

Extortion accountability cover: Typically, losses due to a blackmail of extortion, able fees accompanying to ambidextrous with the extortion.

Network aegis liability: Third-party amercement as an aftereffect of abnegation of access, costs accompanying to abstracts on third-party suppliers and costs accompanying to the annexation of abstracts on third-party systems.[2]

Modern analogue of cyber liability action can awning some or all of the following:

- The third affair technology able insurance.
- Aloofness Accountability (Covers accident of abandoned identifiable agent and customer information.)
- Aegis Accountability (Covers abortion to anticipate the access or advance of a virus/hacker attack.)
- Website Media Accountability (Covers libel, aspersion and absorb contravention from your website content.)
- First Affair Cyber Extortion (Covers costs to acknowledge to a blackmail to abuse or release abstracts as able-bodied as awning bribe payments if necessary.)
- First Affair Aloofness Aperture Response (It is accepted to sublimit the advantage to an amount lower than the anniversary accumulated limit.)

– Chump Notification Expense

– Acclaim Monitoring Expense

–Computer and Acknowledged Forensic Expense

–Acclaim and Identity Repair Expense

- First Affair Business Abeyance and Abstracts Recovery Extra Expense
- Authoritative Defense and Penalty[3]

3. Risks in cyber business

The following are the main risks in the cyber business which although not exclusive provides the most common types of risks and uncertainties:

- Cyber abomination and cyber terrorism
- accidental loss of own or anyone else's abstracts
- physical accident of systems
- liability for your online activities or comments fabricated in emails.[4]

4. Reasons for cyber accountability insurance

- affordable
- It can protect and provide more added than you think.
- You apparently don't accept an accident administration team.
- Even if you don't host your abstracts yourself, you're still responsible.
- The general policy will not cover you.

5. Cyber insurance in India

Indian companies are added adversity huge losses due to ascent cyber attacks that leads to abeyance of business and accident of chump data.

However, with abandoned 100-150 behavior accoutrement cyber abomination accountability insurance getting awash in the country, majority companies are clumsily able adjoin the growing menace, as per many insurance providers.

Financial area that carries out banking affairs and handles banknote is an allotment of the high-risk targets, but a lot of banks in India, barring a few ample clandestine lenders, do not accept cyber abomination accountability insurance.

Industry admiral said this could potentially advance to abundant business losses if the computer systems are afraid and chump abstracts is stolen.

The cyber accountability insurance advantage is the everyman in the auberge and hospital sectors, which has analytical abstracts on customers, which if afraid and stolen, can accept adverse appulse on audience and patients, and abuse the business itself.[5]

Cyber insurance in India has become an able absoluteness in India these days. Abounding companies accept apparent their interests in accepting cyber insurance and some of them accept in fact acquired the same.

Before demography upped a cyber insurance action in India, the anxious aggregation or abandoned accept to be able-bodied acquainted of the techno acknowledged acquiescence requirements of India and the abeyant cyber risks. This abandoned would advice it/him/her to yield a lot of adapted cyber insurance policy.

Similarly, an abnormal cyber insurance action that is not accoutrement the cyber risks in absoluteness and leaves ambit for ambiguity and acknowledged complications while claiming the insured bulk should be avoided. A techno acknowledged vetting of cyber insurance policies acquired in India is a complete accept to afore accepting the same.

Just like acknowledged due diligence, a techno acknowledged cyber insurance action due activity accept to be conducted afore signing any such cyber insurance policy. The acceding and altitude of such cyber insurance action accept to be thoroughly analysed band by band to abstain any abortive and abruptness outcome. Merely signing of a cyber insurance action does not beggarly that in case of a cyber aperture the anxious insurance aggregation would absolution the insured amount.

Insured companies and individuals who accept acquired a cyber insurance action accept to aswell be acquainted if the issues like privacy, abstracts aegis, abstracts security, e-discovery, cyber forensics, cyber crimes investigation, etc. This does not beggarly that those insured themselves accept to be able of managing the techno acknowledged aspects of these issues and fields.

Similarly, insurance companies accept to aswell accomplish it abiding that Indian companies and added stakeholders accept already alien and implemented cyber aegis best practices, cyber forensics best practices, e-discovery best practices,

cyber law due activity, e-commerce due diligence, etc. This would anticipate approaching disputes amid the insurance companies and the insured stakeholders if a cyber aperture occurs. Insurance companies can aswell accommodate a added absolute cyber insurance action to those companies and individuals who can authenticate application of a able-bodied cyber aegis basement and techno acknowledged best practices for their business activities.

Insurance business is able-bodied structured and able-bodied accustomed in India. Even the authoritative framework in the acceptable insurance area is able-bodied managed by Indian government. With the access of time, new avenues are now accessible for the insurance business. One such access comes from the acceptance of information and communication technology (ICT) in our circadian lives and the abusage of the aforementioned by bent elements.

Information Technology Act, 2000 (IT Act 2000) prescribes acceptance of able cyber aegis practices and cyber law due activity by Indian companies and individuals. Even technology companies, banking institutions and e-commerce websites are appropriate to beam cyber due activity in India and this claim cannot be abandoned anymore. A appropriate absorption accept to be accustomed to Information Technology (Intermediaries Guidelines) Rules 2011 and Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011by those affianced in technology accompanying business in India.

Regulatory acquiescence requirements beneath the Indian Companies Act 2013 accept added abounding acknowledged obligations on the allotment of Indian companies and their directors. These awning the accountability of admiral for cyber law and cyber aegis breaches and a accountability for not afterward cyber law and cyber aegis acknowledged obligations while administering the functions of their corresponding companies.

Foreign companies and e-commerce websites accepting a business attendance in India would now be appropriate to annals in India. This would aswell accomplish them amendable to Indian laws and to face acknowledged obligations for their non compliances.[6]

Cyber breaches in India would accession complicated cyber law issues in the abreast future. For instance, cyber aegis issues of e-commerce business in India charge to be discussed and implemented by Indian government and insurance companies. Similarly, cyber due activity accept to aswell be categorical and implemented for online transaction makers. Maintenance and analysis of certificate in agenda anatomy beneath accumulated laws of India would aswell accession privacy, data aegis and cyber aegis issues.

All these aspects charge a committed techno acknowledged framework that is anon missing in India. Similarly, accumulated frauds investigations in India would charge accurate technologies and methods like e-discovery, cyber forensics, etc. If cyber aegis and cyber forensics trends in India are considered, this is a big claiming for Indian government, insurance companies and added accumulated stakeholders. If cyber insurance has to be advised to be a abeyant antecedent of acquirement by insurance companies and able aegis by Indian aggregation i.e., they accept to plan harder in their corresponding fields.

Merely entering into an insurance acceding for cyber insurance purposes would actualize added agitation than solutions as complicated techno acknowledged issues are complex in all-embracing cyber abomination and cyber advance cases. For instance, insurance companies and afflicted companies may aswell face and accept to accouterment battle of laws in cyberspace, antecedent allegation for cyber abomination and cyber attacks, abnegation and non cooperation by adopted governments and companies in cyber crimes investigations, etc.

In these circumstances, not abandoned the cyber insurance agreements accept to be appropriately drafted by insurance companies but techno acknowledged analysis abilities accept to aswell be acclimated for investigating cyber crimes and cyber attacks cases by both the afflicted companies and insurance companies.

6. Conclusion

Thus it can be said that cyber insurance has gained importance in the modern society run by the computers and technology. The regulatory mechanism on the cyber world by the Government is very vague with no proper rapid response team or cyber protection of any sort. The private companies have started provided insurance cover for private companies which hold important data whether citizen related or not.

References

[1] UNISON, Cyber Liability Insurance, http://www.unisoninsurance.net/cyber-

liability.html (last visited on: October 21, 2015)

[2] Sarb Sembhi, An introduction to cyber liability insurance cover, http://www.computerweekly.com/news/2240202703/An-introduction-to-cyber-liability-insurance-cover (last visited on: October 21, 2015)

[3] Amwins, What is cyber liability?, http://www.amwins.com/SiteCollectionDocuments/Client%20Advisories/Client_Advisory-What-Is-Cyberliability.pdf (last visited on: October 22, 2015)

[4] Marsh, Cyber Risks Explained, http://uk.marsh.com/Portals/18/Documents/Cyber_risk_client_briefing_FINAL_exp%20Apr13.pdf (last visited on: October 21, 2015)

[5] Manju AB, Indian companies mostly uninsured against cyber attacks, http://www.dnaindia.com/money/report-indian-companies-mostly-uninsured-against-cyber-attacks-2108378 (last visited on: October 23, 2015)

[6] PLTB, Cyber Laws In India And Technology Laws And Regulations In India, http://perry4law.org/cyberlawsinindia/?p=128 (last visited on: October 24, 2015)