Cyber Risks: Challenges To Insurance Sector- Literature review

Navneet Singh[1],Shobhit Kumar[2]

[1]*Scholar, College Of Computing Sciences And Information Technology (TMU)*

[2] *Assistant Professor, College Of Computing Sciences And Information Technology(TMU)*

1navneetgill206@gmail.com

2kumar.shobhit05@gmail.com

Abstract— **Concern over the cyber risks and cyber safety is growing across all the sectors of the global economy as cyber risks have grown and cyber criminals have become increasingly more sophisticated. For insurance sector cyber security incidents can harm the ability to conduct business, compromise the protection of the commercial and personal data of the insurance policy holders as well as of the insurers. This paper focuses on the cyber risks emerging trends in the Insurance sector as well as also describe some practices for the cyber resilience by the Insurance sector. It also describes some real-life Incidents that are occurred due to lack of cyber security in the insurance sector.**

Keywords— **Cyber risks, Cyber criminals, resilience.**

I. INTRODUCTION

The term cyber risk is broadly described by the CRO forum as "Any risk that takes place from the use of electronic media and its transmission, including technology tools such as internet and telecommunication networks". In Today's time mostly amount of data and information is shared through the electronic media ie. the internet. This information has several cyber risks and it needs protection from that risks. All the business sectors have risks from the cyber attacks on their data.

Regarding the insurance sector, All insurance companies regardless of size, complexity, or lines of business, collect, store, and share a lot of confidential information with various third-parties (e.g., service providers, reinsurers).This information is shared though various electronic media such as telephone, internet, e-mails etc. This private information should be kept secret from other users who don't have rights to know or use the information. The information shared through electronic media has several risks such as theft, Malware (phishing and pharming) , infecting the computers etc.

Cyber risk presents a growing challenge for the insurance sector because the cyber risks are growing day by day and every time , a new challenge arrises for the protection against it. This problem is not only limited with a city or country , it is a challenge for the whole world because almost all the countries insurance companies are suffering from it. For the cyber security purpose every company should know the latest ways though which they can be harmed, such that they can develop new ways to get protected from that harms.

II. CYBER RISKS TO INSURANCE SECTOR

Insurers collect, store and manage confidential personal information including personally identifiable information of the various policy holders as well as of their own company.

Potential adverse consequences of insurance sector cyber security incidents are highlighted below:-

A. Loss of confidential Information

Insurance company holds personal information of the policy holders such as names, birthdates, street and email addresses that should be kept personal by the company for its usage. The company also holds and manages its own personal policies and information that should be kept personal.
But if this information is accessed by some other person who has no rights on it then it can be misused by them that will lead to a lot of loss to the insurer and the policy holders too. These type of risks are more common and these should be well known by every insurance company such that they can develop specific cyber security ways to get protected themselves from these crimes.

B. Disruption of the operations

Cyber risks not only includes theft of the personal information , it may also be a disruption in the operations of the company such as network hacking. It can harm or disrupt the company network including the telephone lines, emails and business records .
if the network of the company is hacked then all the operations of the company will be disrupted and the company will not be able to continue its working until the network will be rebuilded. These type of risks can harm the different operations of the company that can lead to a lot of loss to the company as well as the people connected to it.

C. Theft of Funds

For the commercial insurance, the company holds personal business information of the policy holders. This information is too personal to be managed. This is one of the important cyber risk that can harm the company though various ways. The cyber criminals can steal the personal information of the business of the policy holders as well as can steal the funds of the company as well as the business owners. So, the commercial insurance companies should be aware of these type of thefts and should be alert from these attacks.

D. Reputational Loss

If any insurance company suffers from the data breach then the confidential information of the policy holders can be hacked. The policy holders who have trusted on the insurance company will be cheated. These type of risks and attacks can harm the reputation of the company that will lead to a lot of loss to the company in various ways such as loss in the number of the clients connected to the company and also will lead to the loss to the company in the market ie. the reputation of the country will be declined.

III. CYBER RESILIENCE PRACTICES

The various challenges presented by the cyber risk should be met by a broad response by the insurers. so , high level of management attention from the risk is necessary. To perform that , a lot of cyber security practices should be performed by the company. To apply these practices every company should have cyber cell department to get rid of cyber issues , such that the incidents that takes place due to lack of cyber security should be tackled.
Generally, a cyber risk management program includes ongoing process and control improvements. The different practices should be updated accordingly with the time and the cyber cell department should change its various practices too for the cyber risks management.
The best practices for the cyber resilience includes the following:-

A. Governance

Together with the engagement and commitment of the Board and Senior Management, a Proper cyber resilience framework can be designed. To provide a proper cyber resilience framework the company's

higher authority should communicate with the board to design an effective framework in the company for the protection against the cyber issues. This practice will provide an effective protection to the company against the cyber risks and incidents.

B. Identification

Identification means identifying the areas where the protection should be kept strict against the risks. There are many information categories that should need high level of security such as personal data of the insurers as well as the clients of the company , commercial information including the funds information should be protected.

Regular reviews should be done on the data because there may be many hidden areas that are prone to risks and need security so, that areas should be indentified and the protection should be done.

C. Protection

High level of protection should be provided by designing an effective framework for the company. The effective framework should be designed by using high level of control such as IT control that uses various effective ways for providing the security and alert against the cyber risks.

While designing protection, the "human factor" should also be taken into consideration because the cyber criminals are too the humans and they can apply various cyber practices through their own mind and thinking. so, the areas that need protection and attacked first should be identified on the basis of the mindset of the human.

D. Response and Recovery

It is not always possible to detect or prevent cyber incidents before they happen, even with the best practices in place. Because cyber risks is an ongoing process and it needs latest and high level practices that should be applied for the protection. But sometimes the attack happens because every time a new way for the attacks arrises and it is not always possible to detect and prevent ourself from the attack.

For this reason, incident response planning is the best practice to perform. If the company is having some best ways to overcome the loss that are happened because of the cyber attack then the company can continue its normal working and the reputation of the company should also be protected. So, Best response and recovery practices should be designed by the cyber cell of the company to get rid from the losses.

E. Situational Awareness

The insurer should be well aware of the various threats such that the insurer should be aware for the different situations and establishment of the threat intelligence process helps to mitigate the cyber risks.

IV. EXAMPLES OF CYBER SECURITY INCIDENTS IN THE INSURANCE SECTOR

There are many cyber incidents that have took place in the recent years. These cyber incidents have done a lot of loss to the insurer as well as to the clients of the insurance companies. Some of the cyber security incidents are described below:-

i. An incident took place in the U.S as a data server that was manage at the North Dakota was compromised. The personal information related to the workers
ii. compensation was exposed. While the personal information of the people was not exposed but it was also at the risk to be exposed by the breachers.
iii. In 2015, the testing performed by the internal audit team of an insurer in France found that unauthorised access to accounting tools had occurred. This cyber security incident could have had a substantial impact not only on the company but also on partners, service providers, and

policyholders because accounting information is one of the most important areas that should be took into consideration for the security purpose.

iv. In 2015, Anthem Blue Cross and Premera Blue Cross experienced data breaches in which credit card data and personally identifiable information, including health information were compromised. In this data breach the information of 91 million policy holders was exposed.The insurers should well understand that what type of protection should be provided to avoid the data breaches and if the breach has occurred then what ways should be applied to get rid of it by minimizing the losses.

V. CONCLUSION

The overall conclusion of this paper is that it describes various cyber risks to the insurance sector ie. the threats from which the Cyber industry can suffer when any industry becomes the victim of any cyber attack. This paper also describes various cyber resilience practices through which the insurance industries can safe themselves from the cyber attacks and also describes that if the insurance industry has already prepared some ways to get recovered from the attack if it has occurred then the insurance industry can save themselves from the loss to a great extent. This paper also describes some real life examples of the cyber attacks to the insurance sector to define which types of attacks can occur. In future research work we will focus to define effective and best practices for the cyber resilience to the insurance sector.

REFERENCES

1] New York state Development of financial services, "Report on cyber security in Insurance Sector", February 2015.

2] Kelvin Garrahan "Cyber Security landscape for the Insurance Industry".

3] "A BAE Systems Detica Cyber Insurance briefing" held in the Lloyd's of London library,24 November 2011.

4] Martin Eling, Werner schnell, "Ten key questions on cyber Risk and cyber risk insurance".

6] Insurance 2020 and beyond:"Reaping the dividends of cyber resilience",website-www.pwc.com/insurance.

7] Allianz Global Corporate and Speciality. A guide to Cyber risk,managing the impact of increasing interconnectivity, September 2015.

8] Cambridge centre for Risk Studies and LLOYDS: emerging risk report 2015, Society and security, business blackout: The insurance implications of a cyber attack on the US power grid.

9] Issues Paper On " Cyber Risk to the Insurance Sector" by IAIS (Insurance Association Of Insurance Supervisers), drafted 14 April 2016.

10] Rajesh Mohan More, Dr. Ajay Kumar," A Study of Current Scenario of Cyber Security Practices and Measures", International Journal of Engineering Research and General Science Volume 2, Issue 5, August-September, 2014 .

11] Atul M. Tonge, Suraj S. Kasture , Surbhi R. Chaudhari," Atul M. Tonge1, Suraj S. Kasture2 , Surbhi R. Chaudhari", Volume 12, Issue 2 (May. - Jun. 2013) ,PP 67-75.