Role of cyber insurance in managing digital risk

Mo'minova Dilnoza Muhiddin qizi

Tashkent State University of Law
dilnozamominova84@gmail.com

Abstract

Information and communication technologies in mass ensuring information security due to paperless automated management is becoming more complex and important. That's why it's automated a new modern technology of information protection has appeared in information systems is happening. Owners of information and authorized state bodies value personal information, caused by its loss and the cost of the protection mechanism the necessary level of information protection and the type of system, protection it is necessary to determine methods and means. Value of information and required the reliability of protection is directly related to each other. In this article, we will research cyber insurance, why cyber insurance important, how cyber insurance work, who is cyber insurance important to, how to choose cyber liability insurance. Apart from that, we analyze the strengths and weaknesses of cyber security insurance.

Keywords: Digital risk, Cyber law, Cyber threats, Digital attacks, Cyber security, Managing risks, Cyber insurance

I Introduction.

Cyber insurance is an insurance product used to protect businesses from Internet based risks and more generally from risks relating to information technology infrastructure and activaties. Risks of this nature are typically excluded from traditional commercial general liability policies. Coverages provided by cyber-insurance policies may include first party coverage against losses such as data destruction, extortion, theft, hacking and denial of service attacks; liability coverage indemnifying companies for losses to other caused, for example, by errors and omissions, failure to safeguard data,

or defamation; and other benefits including regular security audits, post-incident public relations and investigative expenses and criminal reward funds.[1]

Cyber security insurance coverage in many countries still compared to other insurance products due to its small size, its increasing determination of its role in the fight against cyberattacks difficult. However, people of cyberattacks and the impact on enterprises is significant. Therefore, insurance companies that provide protection are developing services. This advantages of developments insurers performed for cyberspace incidents it is visible in incremental payments.

Cyber security insurance is the information security of your organization it is an opportunity to protect against associated risk. This gives you with increasing threats today allows you to avoid related losses- for example, hacking attacks, data loss, confidential data leakage.

Cybercrime is on the rise, and more companies are at risk of data compromises, ransomware attacks, and other types of cyber incident. While various tools and solutions within a cybersecurity platform can protect your company and stop data breaches, a company is still liable if it fails to protect sensitive data from being stolen due to a cyber attack.

Cyber insurance, a company's losses due to a cyber attack are usually kept to a minimum, and even if something catastrophic happens, the financial impact is mitigated. Cyber insurance is one of the options for reducing the degree of cyber risks associated with running an online business.

Cybercrime is an increasingly complex and widespread problem; the introduction of new technologies makes threats more diverse; the number of cyber crimes is increasing. Today, people, organizations and goverments consider protecting against cyber attacks a strategic priority as the amount of data stored grows rapidly. The article examines the options for insurer to provide cyber security and obstacles to cyber insurance development.

II Methodology

To analyse the impact of cybersecurity insurance in managing digital risks, the research methodology for this article adopted a mixed-methods approach. This approach deduction method techniques to provide a comprehensive understanding of the research topic.

In particular, academic research and industry reports have been included to reflect the state of the field, presented by academics and practitioners.

Selected information sources include leading computer science and information security journals, research papers, scientific articles, reports and conference proceedings, which provides informations to understand the field of Cyber Insurance in Managing Digital Risk.

III Results

Obtaining cyber insurance can benefit the firm. First, cyber insurers require an upfront risk assessment which, in return, may increase awareness of cybersecurity and encourage self-protection. A cyber resiliency score is one way to evaluate how prepared a firm is to handle cyber attacks. Insurers calculate these scores based on data supplied by the insured and scans of the firm's computer system.

On the other hand, managing cyber risk by transferring it to an insurer is challenging for several reasons. Among other factors, the extant research points out that the randomness of cyber incident, the information involved with these adverse events and the limited coverage of cyber insurance policies are noteworthy[2]

IV Discussion

Managing cyber risks involves several processes including the identification, analysis and measurement of potential effects in the context of cyber incidents. Furthermore, implementing well-established preventive measures and action plans for potential cyber incidents is crucial to build a more resilient system. The participating insurance groups seem to be aware of the importance of these aspects. The results show that 100% of the groups include cyber risk in their Operational Risk Managament

(ORM), either implicity (37%) or explicity (63%) and 80% of the groups include cyber risk in their Own Risk and Solvency Assessment (ORSA).[3]

There is a breakdown or failure in these system, the organization will realise a direct negative impact on the processes it supports, resulting in reduction of service and disruptions that ultimately impact on the organisations ability to meet its objectives.[4]

Top 10 reasons you we need cyber insurance:

1.Hakers are highly organized. Cybercrime is big business, and is not just perpetrated by individuals, but often by highly organized criminal teams from countries like China, Russia and North Korea.

2. Cyber risks are constantly changing. As technology envolves, so do the risks that threaten your business and the data you use every day. Having insurance to protect against new and envolving risks is critical.

3. A cyber attack happens every 20 seconds. In fact, the odds of we becoming a victim of a cybercrime are greater than experiencing a loss due to flood or fire.

4. A data breach can be devastating. Nearly 40% of cybercrime victims spent $50,000or more responding to the attack. The kind of money could damage or cripple a small business.

5. You don’t have to be a big business. Nearly half of all data breaches target small businesses. That’s because cybercriminals are looking for vulnerabilities and small businesses with outsourced or underfunded IT departments often have them.

6. You don’t have to be targeted by a criminal. Cyber insurance helps to respond to an unintentional leak of personal data or records.

7. Nearly all businesses are at risk. If we depend on a computer, tablet, smart phone or the internet to conduct business, we are exposed to cyber risks. Any digital device can be entry points for cybercriminals.

8. Businesses don’t often budget for the risk. If you don’t have insurance cover a risk, this type of expense could put a small business out of business.

9.Coverage costs less than many other types of insurance. Compared to the cost of other types of business insurance, cyber coverage costs less for the level of protection it provides.

10. Cyber insurance covers a broad range of costs associated with cyber risk. Our cyber insurance includes coverage for computer attacks, data breaches, cyber extortion, liability, misdirected payment and telecommunications fraud and identity theft.

Despite the benefits of cyber insurance, the market for cyber insurance is adversely affected by a number of problems.

First and foremost, insurers are afraid of a “cyber-hurricane”- a major disaster resulting in great number of claims. Cyber-hurricanes represent an uncertain risk of very large losses, and such as are very difficult for insurerto plan for.

Second, because cyber insurance is a relatively new area, insurers are hampered by a lack of actuarial data with which calculated premiums. In addition to increasing price, a lack of data leads to problems with the risk analysis undertaking by companies when deciding whether insurance against a particular risk is worthwhile.[5]

In almost all insurance cases, the most difficult issue is the issue of reliable assessment of the cost lost information.

Also, not everything is clear with the payment of insurance coverage, calculated as the amount of expenses incurred to restore the violated right. It will be quite difficult to prove the need for a particular expense or its amount, therefore it is advisable to prescribe an approximate list of such expenses and the limits of their cost in insurance contracts in advance.

Insurance coverage may include:

Losses due to violations of personal data or corporate information;

Losses as aresult of a long interruption in functioning of the network;

Money paid to limit or stop a security threat that would otherwise cause a loss;

Covering the costs of regulatory investigations;

Covering costs associated with the recovery, recollection or reconstruction of information after a data breach or unauthorized use;

Crises management costs;

Damage caused to third parties.

Conclusion

There no standarts in the field of cyber insurance, and legislation is poorly developed in terms of determining liability for violations and crimes in the field of information security. But the situation should change in the near future.

Any insurance statistics and actuarial accounts based on books. In the cyber sphere, such calculations are difficult to make because statitics very little. The facts leads to the development of cyber insurance there will be an obstacle. Product for insurers there are general standarts for development not. Each company relies on its own experience and offers its own version of cyber insurance, that, is the coverage conditions in each case, carefully consider extensions and expections need to learn.

Another obstacle is the appropriate regulation of absence- the only legal definition of such risks no. This type of insurance processes is also unregulated, in terms of contracting there no recommendations, this is their confirmation significantly complicates the process. Legislative regulation and law enforcement development of practice , including intangible assets, data or damage to them tax potential insurance payments for it is necessary to carry out work on weighing.

Another factor is that in risk assessment difficulties arise from business insurance and protecting insurer to customer stops. In addition to complex underwriting,

insurance for protection against cyber security companies require a certain infrastructure does: check the event and its consequences it is necessary to minimize.

Succesful development of cyber security to identify a cyberatack and make it more transparent verification mechanism are necessary. In addition, information in business doing a general job to improve safety important.

Perhaps cyber insurance in the near future, as if mandatory car liability for a car like insurance, to an integral part of the business rotates. Buying a car and for it compulsory car liability insurance policy to compensate the owner losses by obtaining can be sure.

References

1. DHS Secretary Michael Chertoff. ISA-Cyber Insurance Metrics and Impact on Cyber Security.pdf.April 29, 2005.
2. Asligul Erkan-Barlow Brenda P. Wells-Dietel. Journal of Insurance Regulation. The Current State of Cyber Insurance and Regulation in the Context of Investment Efficiency and Moral Hazard: A Literature Review.
3. Cyber risk for insurer- challenges and opportunities. https://eiopa.europa.eu/
4. Gareth William Peters and others published Understanding Cyber Risk and Cyber Insurance.pdf. On Jan 1, 2017 https://www.researchgate.net/publication/321231043_Understanding_Cyber_Insurance/link/6150c765522ef665fb6195b1/