International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 6 Issue 1, November-December 2021 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Information Risk Insurance: Concept and Basic Aspects

Holboev A. Yu.

Tashkent Financial Institute, Tashkent, Uzbekistan

ABSTRACT

The article discusses the essence and history of the emergence of information insurance, identifies the stages, features and problems of the development of insurance of information risks at the present time. The article touches upon such an urgent topic for modern reality as insurance of information risks. Analyzed the characteristic features and the need for this type of insurance. The author considers insurance as the main financial method of information risk management. Particular attention is paid to information risks and their insurance. The work describes in detail the objects of insurance, types of insurance risks. The insurance contract is considered, the main stages of its life cycle are reflected.

KEYWORDS: *risk, protection, cyber crime, cyber insurance, information risks, information security, cyber risk, cyber attack, insurance, insurance of information risks*

How to cite this paper: Holboev A. Yu. "Information Risk Insurance: Concept and Basic Aspects" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-6 | Issue-1, December 2021, pp.760-766, URL: www.ijtsrd.com/papers/ijtsrd47910.pdf

IJTSRD47910

1. INTRODUCTION

Over the past few years, information has begun to play a crucial role in all spheres of human life, which is associated with the gradual formation of the information society. For the development of mankind, not only material, instrumental and other resources have become necessary, but also informational. The present time is marked by a rapid growth of information flows covering the entire globe, since with the transition to the modern stage of development, characterized by an increasing rate of technical and technological innovations, the amount of knowledge that is needed to substantiate, develop, implement and disseminate them should increase significantly. The largest increase in the volume of information is observed in such industries as industry, trade, education, and banking and finance. Information turns into a most valuable type of product, the total cost of which in the near future should exceed the total cost of material production products, since to ensure the successful resource-saving creation of material goods and services, it is necessary to use a fundamentally new technology that ensures the growth of knowledge, their effective search, storage, distribution and implementation.

In view of these changes in the economy, information, information technology and the emerging market of information services require close attention and study, since it is obvious that due to the possession, use and transfer of valuable and important information, a number of risks can arise that can cause tangible damage to the company, the state and the economy. generally.

Due to the widespread use of network technologies and mobile devices, the problem of protecting valuable information is more acute than ever. Among the main tasks of companies, in addition to the usual ones, there have appeared such as protection and ensuring the confidentiality of data, reducing information risks and preventing hacker attacks. Niktoneis insured against such undesirable consequences as theft, interception of information, infection of a computer with a virus, destruction of information and many others.

Currently, a significant percentage of organizations of various organizational and legal forms are companies whose core business is working with electronic data carriers and for which failures in information systems

can cost huge monetary, reputational and temporary losses.

In this regard, more and more attention is paid to the risks that the informatization of organizations carries, as well as their insurance.

2. Literature review.

Many experts (Sharapov 2010) put the following meaning into the concept of "information risk": information risk is a possible event as a result of which information is unauthorizedly deleted, distorted, or its confidentiality or availability violated. That is, the concept of information risk is used as a synonym for the concept of information security threat.

Management of such information risks comes down to information protection. Moreover, some of the authors of such an interpretation of information risk under the protection of information understand its protection mainly from malicious actions (cyber attacks, cybercrime).

At the moment, there has not yet been an unambiguous concept of what information risk is. Some experts (Baranova 2015, Zamula et al. 2009, Kiseleva and Iskajyan, 2017) consider information risk as an event that has a direct impact on information: its deletion, distortion, violation of its confidentiality or availability.

Some experts (Michel 2007) approach the concept of "information risks" from a different point of view - the economic one. By definition, they mean "the risk of loss or damage as a result of the company's use of information technology. In other words, IT risks are associated with the creation, transmission, storage and use of information using electronic media and other means of communication. "

Tepman (2016) suggests understanding information risk as a measure of information danger, which characterizes the likelihood of a hazard and the extent of damage to the reputation of an enterprise.

Shangin (2014) considers information risk as "the possibility of damage in the form of losses as a result of the use of information technology by an enterprise."

A modern developing society is characterized primarily by global interconnections between various actors. In this regard, cybercrime is becoming more and more widespread in the world. Efremova (2000) defines that cybercrime is a general name for computer offenses (file hacking, theft of secrets and money from bank accounts), as well as computer hooliganism (introduction of viruses, etc.)).

Ivanov (2016) believes that one of the possible methods of protection against cyber attacks and the negative consequences from them can be cyber insurance. Cyber insurance is an insurance product for the protection of information risks of any company whose business is directly or indirectly related to the processing and storage of data.

Simply put, cybercrime involves the theft of money and securities from the accounts of organizations, important information by hacking the security system. Today, the non-cash form of money has become more widespread than cash, and it is much easier to steal non-cash money, because it is much easier to crack a password than, for example, stone walls of vaults.

Nomokonov and Tropina (2010) argue that cybercrime is now a fairly widespread phenomenon in the world. Its share in the total volume of crimes in the financial services sector is approximately 40% and is second only to misappropriation of assets in frequency.

Thanks to the development of a modern society, characterized by global interconnections between various actors, cybercrime, which quite recently could be observed on the example of the WannaCru ransom ware attack, is gaining an ever-increasing scale. As investigators Mamaeva and Larionov (2018) and Smirnov (2015) note, cyber insurance can be one of the possible methods of protection against cyber attacks and the negative consequences from them. This type of insurance provides a financial mechanism for recovering from large losses, helping enterprises to return to normal operation, maintaining stability, solvency and reducing losses as a result of interruption in production caused by various kinds of cyber threats.

3. Research methodology.

The methodological basis of the study is the generalization of empirical analyzes and the concept in the field of information and cyber risks, as well as international and domestic practice of insurance of information risks and the activities of insurance companies.

4. Analysis and results.

In the modern global economy, information is becoming one of the key elements of business development. The business process of an enterprise directly depends on the operability of the information system and the quality of the IT technologies used.

Already in the mid-1990s, foreign companies realized that the development of information technology (IT) brings with it the emergence of new risks, and, accordingly, a new demand market. The first to actively use the new IT were the banks that

previously used the "General Banking Policy" (Banker's BlanketBond, BBB). This policy provided for insurance of bank property, transported cash, and also covered the risks associated with fraudulent actions of employees, including their activities related to forgery and the use of counterfeit currency. However, the BBB did not provide for damage from hacker attacks and other computer crimes, although, according to the British Federation of Entrepreneurs, the average loss from penetration of banking networks by hackers at that time was about $ 500 thousand. Therefore, the locomotive that moved information insurance off the ground , is precisely the banking sector. Since it is not possible to compensate for the damage caused to information assets under the standard conditions of business insurance, it was decided to develop special insurance programs for the IT sector.

The most famous players in the global IT insurance market are such giants as AIG, Marsh, Zurich Financial Services Group, Lloyd's. In the West, the insurance of risks associated with e-commerce has developed in parallel with the insurance of banking electronic equipment and the banking sector, in particular. One of the main tasks of IT insurance, repeatedly highlighted in the releases of foreign companies, is the creation of favorable conditions for the development of network trade. The most famous such insurance program, Internet Asset and Income Protection Coverage, was provided by Lloyd's. A significant feature of the company's policy is the ability to choose a supplier of security products. This program covers the risks of loss or damage to information assets due to hacking or a security failure. Information assets include primarily customer lists, credit card numbers, working papers and any other data.

Among the main prerequisites for the creation of an information risk insurance system at present, the following can be noted:

- intensive development of the information market in the country;
- the relevance of the issue of protecting information systems for both government and commercial organizations;
- the existence of real threats of information loss due to an increase in information "hacking" and the impact of virus programs;
- the need to distribute responsibility for the storage and distribution of information between developers, owners and users of information systems.

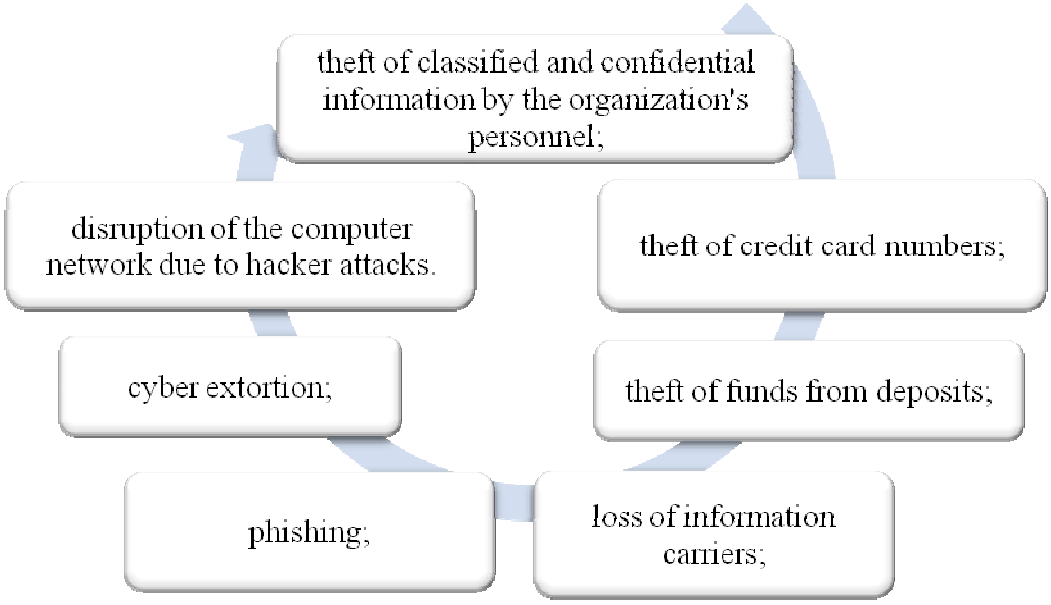
All information risks can be classified into different groups based on several criteria:

1. According to sources, information risks are divided into internal and external;
2. By nature - intentional and unintentional;
3. By type - direct or indirect;
4. As a result - violation of the reliability of information, violation of the relevance of information, violation of the completeness of information, violation of confidentiality, etc.
5. By the mechanism of action: natural disasters, accidents, mistakes of specialists, etc.

Undoubtedly, this type of insurance is considered as a method of risk management and protection against various threats arising from the implementation of electronic commerce. The main risks include the following risks (Figure-1), but the central task of cyber insurance remains protection against large-scale hacker attacks.

Thus, the main goals of creating an information risk insurance system are as follows:

- formation of a mechanism for compensation of financial losses to the owners, owners and users of information systems, resources and technologies due to theft, loss, change or blocking of information as a result of computer crimes, unauthorized actions of third parties, fraud, as well as failures, failures and errors arising in technical and computer software and other reasons;
- accumulation of financial resources at the expense of insurance premiums of participants in the insurance system and their investment in the field of communications and informatization in order to form and implement an effective scientific, technical and industrial policy, to promote the intensive development of the market of information resources, systems and technologies;
- financing of measures to protect information from the fund of preventive measures of insurance companies in order to minimize the risks of loss or change of information and reduce insurance compensation.



Picture 1 The main risks when insuring e-commerce

The most developed segment of this market is insurance against electronic and computer crimes, which provides compensation for losses incurred as a result of:

- unauthorized data entry or changes;
- introduction of fraudulently prepared or modified commands into the computer system;
- damage, destruction or interception of information;
- blocking access to data and to the website;
- exposure to computer viruses.

In this case, the object of insurance is property interests related to the possession, use and disposal of information on electronic media. At the same time, this insurance product most often acts as a concomitant in the package of comprehensive bank insurance (BBB), although similar products appear, designed for other organizations. An important distinguishing feature of this type of insurance is the ability to insure the risks of only the policyholder himself and only in his favor, i.e. in insurance against computer and electronic crimes, the concepts "insured person" and "beneficiary" are inapplicable.

Currently, in world practice, insurance companies offer insurance coverage for the following types of risks:

1. The risk of theft of confidential information and its further use by the employees of the organization;
2. Risk of theft by criminals of information about bank customers, such as credit card and account numbers;
3. Risk of stealing money from bank customers' accounts;
4. The risk of disclosing classified information of company employees;
5. The risk of stopping the work of the enterprise due to failures of the computer network, the site of the organization, etc.;
6. Receipt of losses by the organization in connection with the placement of false information, etc. (Romanenko 2018).

Many insurance companies offer a comprehensive insurance package containing several of the named types of insurance claims.

The purpose of the information risk insurance system is to create a mechanism for reimbursing financial costs to owners of information assets due to loss, loss, theft of information, fraud and unauthorized actions of third parties, failures and errors in hardware and software, intentional and unintentional actions of personnel and other reasons. In accordance with world practice, information is insured at the cost of its restoration.

Taking into account the above, after analyzing the current regulatory legal acts in the field of informatization and insurance, the author systematized objects of insurance and insurance risks in the following form.

Insurance objects:

1. Information assets: information (including that for which there is a possibility of loss without the possibility of recovery), general and special software, databases, electronic documents, information resources.
2. Financial assets in electronic form (including in client-bank systems), billing systems.

3. Technical means: computer (including Web-servers), telecommunications and other equipment.
4. Costs associated with liability to third parties.
5. Costs associated with business interruptions.

Insurance risks:

1. Loss, deliberate and unintentional change, destruction of insured information assets due to errors in the creation, development and improper maintenance of the information system of the enterprise (policyholder) and the actions of computer viruses and attacks.
2. Loss, intentional and unintentional change, destruction of insured financial assets in the form of their illegal write-off from the accounts of the enterprise (policyholder) due to unauthorized modification of programs, entering fraudulent electronic commands into IT systems and transmitting fraudulent (falsified) electronic orders to the bank or the depository of the enterprise (policyholder) from third parties due to their unauthorized access to information.
3. Loss, intentional and unintentional change, destruction of insured information assets or financial assets in electronic form due to unlawful intentional actions of an employee of the company (policyholder) in order to obtain financial benefits and damage the company.

In addition to the main information risks, the following can also be insured:

- expenses incurred as a result of stopping the economic activities of enterprises due to failures in the operation of information systems;
- costs associated with maintaining the current activities of the enterprise during the recovery period, if there are alternative ways of storing and using information;
- costs associated with the urgent restoration of information resources and economic activities, if necessary;
- additional costs associated with the restoration of the company's business reputation.

In addition to insurance of information risks, civil liability insurance of organizations that provide services for the protection of information resources and information services to a large number of users is of great importance:

1. Insurance of civil liability of suppliers and developers of information protection means.
2. Liability insurance of trading floors and stock exchanges.
3. Civil liability insurance of certification centers operating in the public key infrastructure.

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

If in the West appraisal companies have a great practice of reliable appraisal of assets expressed in the form of information, then domestic appraisers, having only a truncated method of appraisal of intangible assets, will not always be able to assess the cost of information in a way that suits both the client and the insurance company.

So, European companies distinguish the following elements that affect the insurance rate:

- The cost of the insured object. This parameter has the opposite effect on the rate, i.e. the higher the cost, the lower the rate and vice versa. For example, Lloyd defines an insurance premium of $ 20,000 (i.e. 5%) for an information cost of $ 1 million and $ 75,000 (i.e. 0.75%) for an increase in the cost of information to $ 10 million (Böhme 2010) ...
- The presence of anti-viruses and other similar means of protection also inversely affects the value of the bet. So the more reliable, stronger and more famous the used protection system, the lower the insurance rate.
- Number of attacks on the policyholder, as well as on other companies in a similar industry.

It should be noted that the information insurance contract does not cover the risks associated with:

- damage caused by an employee or persons in collusion with the policyholder;
- with third parties gaining access to confidential information;
- using unlicensed computer programs (Pal vaboshyalar 2016, Bienervaboshyalar 2015).

In the event of an insured event, compensation is paid for the funds necessary to restore damaged or lost information, and losses caused by the forced termination of work. The costs of purchasing new electronic devices or their component parts, including the costs of delivery, installation and commissioning, may also be taken into account.

In addition, it should not be forgotten that in today's business environment, the reputation of any company depends to a large extent on the security and stability of IP. This is especially noticeable in the activities of

domestic companies, where the slightest information failure is enough to nullify the customer confidence that has been earned over the years. The consequence of this reaction can be considered the increasing reluctance of banks to disclose their losses from the actions of hackers. This is understandable, because indirect losses due to the churn of clients can cause much more damage than the cost of the lost information assets themselves. No sum insured does not include losses associated with the loss of the company's positive image.

When concluding a contract, the insurance company has the right to demand that preventive measures be taken before concluding the contract or within a certain period specified in it. Failure by the client to comply with any instructions usually entails early termination of the contract. For example, the following means of protection can be offered to e-commerce enterprises: data backup, use of antivirus programs, data encryption technologies, authentication systems (introduction of an electronic digital signature to verify the authorship and authenticity of a document), firewalls (firewalls); filtering traffic entering the network or server, etc.

Of course, the usual precautions aimed at reducing the risk will also be checked: proper maintenance, adherence to fire safety rules, the use of air conditioning systems required by the technical and technological conditions, etc. In addition, the insurance contract may include a list of standard rules to ensure the safety of electronic business processes.

However, one cannot exclude the possibility of state regulation in the insurance of information risks. Such intervention should contribute to the development of this type of insurance and attracting new customers, for example, trade and service Internet companies, which stubbornly do not understand the threat of a virus-hacker scourge that threatens them. Restraining factors of insurers are the lack of well-developed legislative issues and statistics for the correct calculation of tariffs, as well as the lack of transparency of domestic business, which makes it difficult to assess the possible damage of the insured companies.

In general, it should be noted that the development of information insurance is almost entirely dependent on the development of a general business culture in Uzbekistan, which is observed not only in the verbal support of large businesses by the state, but also in the increase in the importance of the IT industry as a whole. And now, despite the existing difficulties and high risks, more and more online stores appear and carry out settlements of electronic payment systems, offline enterprises one after another install ERP, CRM and other management systems, which allows most experts to look optimistically into the future and hope for the further development of information insurance as a promising mechanism for protecting IP and the electronic sector of the economy as a whole.

5. Conclusion and suggestions.

Thus, the development of the cyber insurance market in Uzbekistan is currently at an initial stage, but over time it can become a high-quality means of ensuring information security and protection against cyber threats, because the potential market for such insurance is huge, since any bank, company, that possesses valuable data and important information are at risk.

Clearly, cyber insurance helps protect customer data even before a hacker attack. Insurance programs include an audit - experts point out to clients the most significant risks and give recommendations on how to minimize the consequences of hacker attacks. This service is becoming more and more popular every year not only among financial, but also among trade organizations.

The potential market for cyber insurance is huge, as any company that is involved in data storage, operations and data transfer is at risk. Not only Big Data are vulnerable to hackers, but also personal pages on social networks, email inboxes, websites of communities or bloggers, and online gaming companies.

And also in the future, when insuring cyber risks or information risks, insurers may face serious problems of cost optimization. Companies will have to consider addressing this issue by making greater use of advanced analytics such as blockchain, underwriting, and smart contracts. To develop the cyber insurance market, digital distribution and virtual services must be expanded to cut costs and gain a competitive edge.

Literature

[1] Sharapov A.V. (2010) the problem of defining the concept of information risks. Security of information technologies. Volume 17, No. 2 S. 58-60.

[2] Baranova E.K. (2015) Methods of analysis and assessment of information security risks // Bulletin of the Moscow University. S. Yu. Witte. Series 3: Educational Resources and Technology. No. 1 (9). P. 73–79

[3] A. A. Zamula, A. S. Odarchenko, A. A. Deineko (2009) Methods for assessing and managing information risks / Applied radio electronics, volume 8, No. 3. P.382-387.

[4] Kiseleva I. A., Iskajyan S. O. (2017) Management of information risks in business // Innov: electronic scientific journal, №1 (30). P. 5.

[5] Michelle M. (2007) Information Risk Management // Financial Director. - No. 9, p. 64-68.

[6] Tepman L. N. (2016) Information Risk Management: Textbook / L. N. Tepman, N. D. Eriashvili. - M.: UNITI, - 215 p.

[7] Shangin V. F. (2014) Information security and information protection / V. F. Shangin. - M.: DMK, - 702 p.

[8] Efremova T. F. (2000) New Dictionary of the Russian Language. Explanatory and derivational. - M.: Russian language.

[9] Ivanov I. K. (2016) Cyber insurance: how to ensure information security for business // Big portal for small business, No. 16, pp. 13-24

[10] V.A. NomokonovTropina T.L. (2017) Cybercrime as a new criminal threat // Criminology: yesterday, today, tomorrow. No. 24. S. 45-55

[11] Mamaeva L. N. Larionov V. I. (2018) Cyber insurance as a way to ensure information security. Economic security and quality. No. 1 (30) P. 76-79

[12] Smirnov S. A. (2015) Cyber risk insurance in Russia: analysis of the state and development prospects // Collection of scientific works / ed. G. D. Drozdov. SPb., Pp. 303–306.

[13] Romanenko N. A. (2018) Insurance of information risks of enterprises as a tool of risk management // Financial research no. S. 13-24

[14] Böhme R., Schwartz G. (2010) Modeling Cyber-Insurance: Towards A Unifying Framework. URL: http://www.econinfosec.org/archive/weis2010

[15] Pal R., Golubchik L., Psounis K. (2016) A Novel Cyber-Insurance Model. 2016 URL: http://wwwbcf.usc.edu/~kpsounis/Papers/aegis.pdf.

[16] Biener C., Eling M., Wirfs J.H. (2015) Insurability of Cyber Risk: An Empirical Analysis. Working Paperson Risk Management and Insurance, 2015, no. 151. www.ivw.unisg.ch/media/internet/content/instituteundcenters/wp151.pdf.