

Study of insurance in cyberspace and its infrastructure in Iran and other countries

Behzad Lotfy^a, Hengameh Vatankhah^b

^a *master of computer engineering, Hakim Nezami University, Quchan, Iran*

^b *Bachelor student of information technology, Sadjad University of Technology, Mashhad, Iran*

Abstract

Cyber insurance is a new type of insurance coverage and an efficient tool to improve the security of Internet activity. Cyber insurance policies have become more comprehensive as insurers better understand the risk landscape and specific business needs. In this paper, the formation and evolution of cyber insurance, with the problems facing it checked. Finally, we trace Iran's organizational needs to this type of insurance and discuss how to remove them, and offer a solution for Iran's development of cyber insurance.

Keywords: Cyber insurance, Insurance Infrastructure, Organizational needs

Introduction:

The development of cyberspace and its influence in all aspects of people's lives caused abuse and fraud because of the ignorance and lack of enough information. Therefore, the construction of secure and reliable space is very important for ministerial the culture of people to use the cyberspace. Although some interactions have been done in this regard, but it is still problematic. So by using a specific structure such as insurance, we can compensate the potential losses. Since cyber insurance in general and especially in Iran is a new concept, solving problems and negative views on the challenges ahead are crucial.

This article describes the application of cyber insurance, introduces its necessary infrastructure, and discusses the strengths, weaknesses and challenges of this type of insurance. Then we describe the organizational needs in Iran and discuss how to remove them. At the end, strategies for the development of insurance in Iran cyberspace and its cooperation with some electronic transactions are provided.

Cyber insurance

Cyber insurance is often used to describe the coverage for damages resulting from unauthorized access, destruction or theft of data and online extortion. This insurance covers computer viruses, denial of service attacks (DOS) and also unauthorized electronic transactions. In fact, Coverage provided by cyber-insurance policies may include first or third-party coverage against losses such as data and property destruction. Cyber insurance or internet insurance is insurance policy which is provided on behalf of insurers to align market incentives and improve the security of cyberspace. [1]

Empirical information on cyber risk is relatively limited. One of the few fields that is well documented is data breach for which the Ponemon Institute annually provides cross-country and cross-industry information. It finds that security and data breaches resulted in an average financial impact of US\$9.4 million in 2013 and expect that number to increase significantly in the coming years. McAfee estimates the global economic impact of cybercrime and cyber espionage at US\$300 billion to US\$1 trillion. [2]

A data breach can be a serious incident for a business and could cost an enormous sum of money to handle. The average cost of a data breach in 2010 was \$214 per lost record. This may seem like an insignificant amount of money at first glance but when it is taken into consideration that most companies who suffer a data breach will lose hundreds, thousands, or even millions of records, depending on the size of the company, the average cost of a data breach can become expensive in a very short amount of time. According to a recent study by the Insurance Information Institute, “the average organizational cost of a data breach is \$7.2 million”. Some of the costs that are taken into consideration when determining the average cost of a data breach include the “cost of detection, escalation, notification and response. Then consider the legal, investigative, administrative and reparation expenses. [3]

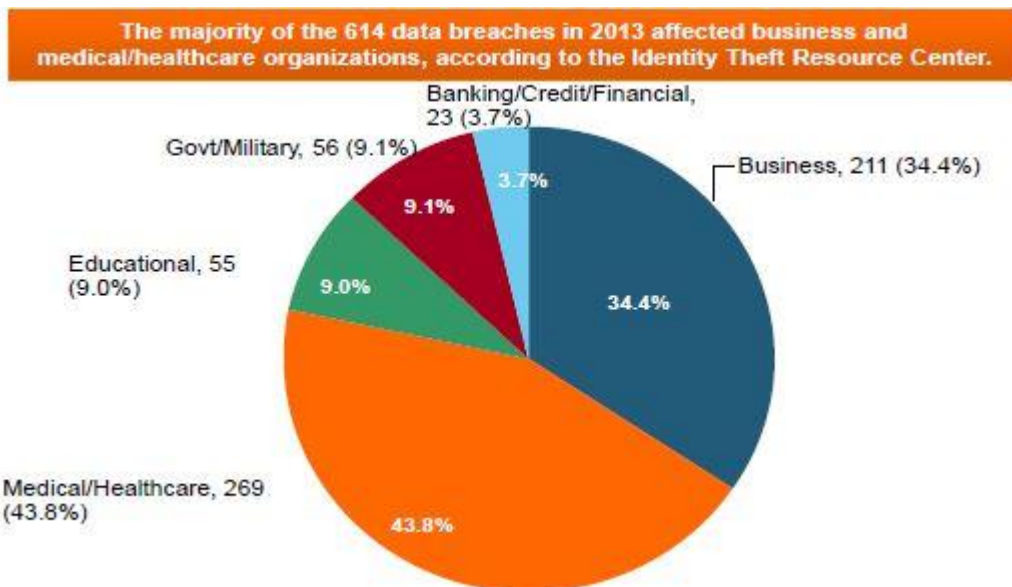


Figure (1): 2013 data breaches by business category, by number of breaches [4]

According to many experts, there are two major problems in the cyber insurance; First, unfortunately, many companies have not yet understood the necessity of Cyber insurance and it may become too late to realize its necessity. Second, many Companies do not open data losses caused by hacker breach to the public, so that it may reveal their system weaknesses. This secrecy causes less-than-estimated the risk of losing information and no detailed statistics for the losses suffered by insurance companies and subsequently cyber insurance.

In dealing with these problems, Security and Exchange commission of America established requirements for companies in October 2011 so that companies must disclose the cost of cyber attacks to their shareholders. Experts predict that these requirements would increase the supply and demand of cyber insurance.

To enhance the role of insurance in cyberspace, the insurance industry is required to provide different coverages. Cyber coverages are generally divided into two categories: 1. The first person coverage, including damage to property and financial intelligence of individuals 2. Third party coverage, including losses related to Internet content, Internet security and necessary defense expenditures.

Infrastructure of cyber insurance

To create this type of coverage in developed countries, measures are taken, including: Risk transfer mechanisms, working with governments to raise awareness of online risks big companies, working with leading IT industry to develop computer network security best condition. In addition to these measures, and cooperation at the same time increases the risk of cyberattacks, legislation was drafted that some of them are mentioned in Table 1.

Table 1: Federal/State Legislation Pertaining to Electronic Records

Legislation	Description
Health Insurance Portability & Accountability Act (HIPAA) (1996)	Mandates confidentiality, integrity, and availability of patient and other medical records and requires healthcare providers to secure the stored records.
SEC 17 a-3 & 17 a-4 (revised 2002)	Requires financial entities to retain client correspondence and all electronic records preserving integrity for auditing.
Gramm-Leach-Bliley Act (1999)	Requires financial entities to disclose policies for protecting confidential customer information and ensure integrity and confidentiality while preventing unauthorized access.
Sarbanes-Oxley Act (2002)	Ensures accuracy and reliability of corporate disclosures by requiring validation of integrity and accuracy of financial records.
California State Law SB 1386 (2002)	Requires all state agencies and businesses that store client information to promptly disclose security breaches.

Firms who recently purchased new cyber insurance products cite as among its advantages:

- (a) the ability to transfer risk to an insurer so they feel sheltered;
- (b) the capability to take fast action against a threat;
- (c) continuous monitoring by experts;
- (d) Informing businesses about efficient methods of security control;
- (e) Investment boom in information technology;
- (f) Increase social welfare.

In contrast the many advantages of this type of insurance, the primary weakness of its, is the inability of compensate of the lost reputation of individuals and corporate.

Issues facing the development of cyber insurance policies and solutions of insurers

In developing cyber insurance from the traditional insurance products to the early hacker insurance policies to where it is now, cyber insurers had several important implementation issues to address. In this section we examine these implementation issues and the mechanisms cyber insurers are using to deal with them.

1. Adverse selection

In insurance settings, these problems arise when insurers are unaware of whether an applicant is high-risk or low-risk. Since the applicant knows whether he/she is high-risk or low-risk while the insurer does not, there is an information asymmetry between them that leads to what is known in the economics literature as the adverse selection problem.

To address the adverse selection problem, cyber insurers require applicants to undergo thorough, detailed, and extensive risk assessments. As a condition to developing coverage, cyber insurers evaluate the applicant's security through a myriad of offsite and on-site activities with a view of reviewing the applicant's vulnerabilities.

2. Moral hazard

The second major problem that insurers need to address in developing cyber insurance coverage is the "moral hazard" problem. The problem is when firms are covered by insurance they may either intentionally cause the loss or take fewer measures to prevent the loss from occurring. For example, firms may slack in their security work when they are covered by insurance. Thus, they may either not invest in security infrastructure or they may not have incentive to maintain or upgrade their existing level of security.

In insurance economics literature, a well-known device to work around the moral hazard problem is for insurers to observe the level of care that the insured takes to prevent the loss and tie the insurance premium to that amount of self-protection care. This way, the presence of insurance can in fact increase the level of self-protection that the insured takes rather than decrease it.

Insurance companies according to the security level of policyholders, set a series of Exception in insurance policies, in this Conditions insurers have no responsibility for payment of compensation. In addition of exceptions, insurers advantages to applicants consider that the number of them is in Table 2.

[1]

Table 2: Exclusions that address the Moral Hazard Problem in Recent Cyber insurance Policies

EXCLUSIONS	Net Advantage Security	e-Comprehensive	Web net Protection
Failure to back-up	Y	Y	Y
Failure to take reasonable steps to maintain and upgrade security	Y	Y	Y
Fraudulent, dishonest and criminal acts of insured	Y	Y	Y
Ordinary wear and tear of insured's info assets	Y	Y	Y
Claim arising out of liability to related parties	Y	Y	Y
OTHER RELEVANT PROVISIONS			
Retentions	Y	Y	Y
Liability Limits	Y	Y	Y
Criminal Reward Fund/Investigative Expenses Covered	Y		Y
Services by Information Risk Group to mitigate the impact of 1 st party loss, covered		Y	
Representations Relied Upon	Y	Y	Y
Regular/Annual Surveys of Insured's Facilities	Y	Y	Y

Organizational requirements in Iran

We don't have any cyber insurance in Iran while there are some organizations should be supported in the following fields:

- Information theft
- Loss of information.
- Staff abuses
- Disruption and change in transactions
- Cell bank mobile
- Voice Over Internet Protocol (VOIP)

Unfortunately, there have not been effective measures to meet the needs in our country. To meet these requirements in Iran, government should deal with this type of insurance and provide the appropriate infrastructure in collaboration with other organizations.*

* Retrieved from Research

Research method

In this research, in order to analyze the tendency of people for using the facilities of cyberspace and insurance in this space, a questionnaire was developed and completed by 220 different people including university students, banks and government staff and ordinary people. Then the results were analyzed with charts.

Findings

By analyzing the questionnaires we achieved important results which are indicated in the following charts. Scale used in the charts is 'percent'. Red lines in the charts represent values above 50%, orange lines represent 50% and yellow lines represent the values below 50%.



Figure (2): doing online works

The highest application is related to banking (such as paying tuition fees, pay-to-charge SIM card, etc.) and the least application is allocated to items such as stocks buying and selling, hotel reservation and so on.(Figure 2)

Although nowadays most of activities are done electronically, there are weaknesses in the use of these facilities in Iran because of lack of awareness and trust in cyberspace. As a result, banks and virtual stores and those who provide services to the people in this space can cooperate with insurance companies to improve safe and reliable space for using by more and more people and provide an effective step toward improving e-business boom.

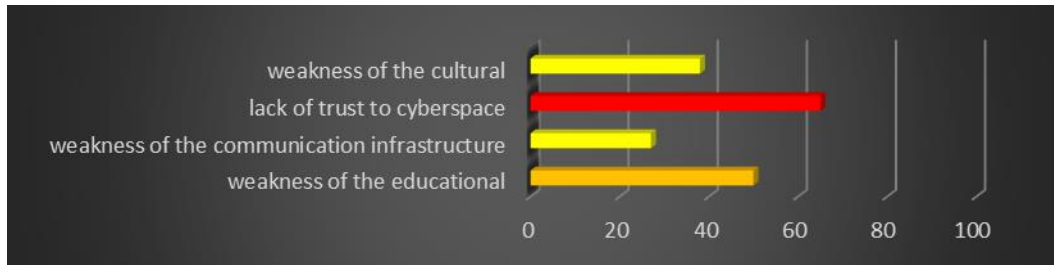


Figure (3): Causes of Refuse from doing online works

As it has been pointed out in Figure 3 Most of people believe that the reason for refusing to carry out their work electronically is lack of trust to cyberspace and they are afraid of disclosure of their information in this space. Some others are also declined it is due to the weakness of the educational, cultural and communication infrastructures. So, all companies and institutions that provide public services in cyberspace should cooperate with the government and insurance companies in order to attract more customers and provide a suitable and reliable environment as well as increasing people's knowledge and attitude by education.

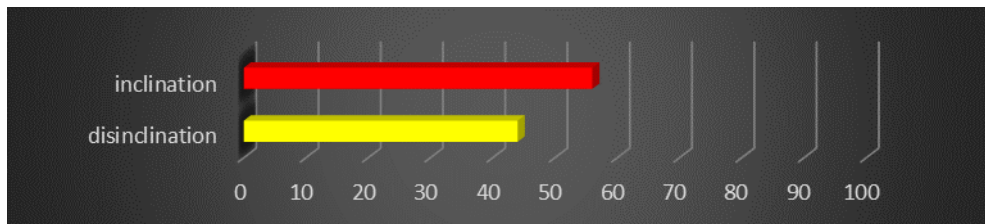


Figure (4): The tendency of individuals to use the cyber Insurance

In Figure 4 you can see that a significant percentage of people are reluctant to use the cyber insurance. The reason may be lack of awareness of cyber insurance coverage or lack of public trust in insurance and accountability. As a result, to attract people to use the cyber insurance, insurance companies charged with two main tasks:

- 1- acknowledging people about different kinds of cyber insurance coverages which bring them comfort and security in cyberspace.
- 2- ensuring confidence and reliability of the people, by improving the shortcomings and problems in other insurance coverage or through appropriate advertisements for children and the young who are going to do electronical business in the future.

Conclusions and recommendations

In this article we have described cyber insurance and discussed the problems and solutions, and insurance development in various fields. In addition to coverages mentioned in this article, there are some other ways for benefiting from this type of insurance.

Unlike some foreign countries that vehicle or housing deals can be done electronically and remotely, this feature does not exist in Iran and this has many reason. One of the most important reasons is cultural weakness and lack of proper action of different Organizations in Iran. So if we want to do all the things in the cyberspace as developed countries, we need to make the cultural infrastructure properly

and coordinate related departments together and ordained a contract between them and the insurance company with experience, to perform secure transactions. More statistics about the Iranian insurance business can be found in Saeedpoor et al. (2015).

References:

- [1] Majuca, R. P., Yurcik, W., & Kesan, J.P. (2006). The evolution of cyber insurance. arXiv preprint cs/0601020.
- [2] Biener, C., Eling, M., & Wirfs, J.H. (2015). Insurability of Cyber Risk: An Empirical Analysis. *The Geneva Papers on Risk and Insurance-Issues and Practice*, 40(1), 131-158.
- [3] Iitaker, Jastin, (2013). *Cyber and Reputational Risk Insurance: Past, Present, and Future*. Appalachian State University.
- [4] Hartwig, Robert P, (2014). *Cyber Risks: The Growing Threat* insurance information institute.
- [5] Bernik, I. (2014). Cybercrime: The Cost of Investments into Protection. *Varstvoslovje*, 16(2), 105.
- [6] Robinson, N. (2012). Incentives and Barriers of the Cyber Insurance Market in Europe.
- [7] Shim, W. (2010). *Interdependent Risk and Cyber Security: An Analysis of Security Investment and Cyber Insurance*. ProQuest LLC. 789 East Eisenhower Parkway, PO Box 1346, Ann Arbor, MI 48106.
- [8] Kelly, Jason. (2015). *Beyond Data Breaches: Cyber Trends and Exposures*. American International Group.
- [9] Saeedpoor M., Vafadarnikjoo A., Mobin M., Rastegari A., (2015) A SERVQUAL Model Approach Integrated with Fuzzy AHP and Fuzzy TOPSIS Methodologies to Rank Insurance Firms, *Proceedings of the 2015 American Society of Engineering Management Conference (ASEM2015)*, Indiana, USA.