World Applied Sciences Journal 6 (Supplement 1): 32-37, 2009
ISSN 1818-4952

Role of Cyberinsurace in it Security Risk Management

N. Ghavami, R. Kalantari and M. Rahimi

Researcher, IT security group of Iran Telecommunication Research Center, Iran

Abstract: Uncertainty and Relativity are the most important subjects in concept of cyber space security. There are plenty of potential threats in cyber space that might be converted into attacks which cause destruction, distortion, omission, exposure and even some times prevent from transmitting data. Using different security mechanisms and technologies can not prevent these attacks so we need other mechanisms for cyber-losses compensation. Cyberinsurance is a powerful tool to align market incentives toward improving Internet security. In recent years, regarding to existence of new technologies in field of information and communication technology and lack of experience in Information security field, the rate of attacks has increased dramatically, therefore cyber-losses compensation is obviously necessary. For preparing the total solution for countries such as Iran, in this paper, we are using cyberinsurance in IT risk management. Our risk management approach is based on transferring the cyber-losses risks to insurance companies.

Key words: IT Security Risk · Risk management · Cyberspace · Cyberinsurance

INTRODUCTION

There are many serious and costly challenges for protecting information assets in cyber space. Threats are the latent agents that cause security problems. Actually threats create attacks, it causes destruction, distortion, omission, exposure and even some times prevent from transmitting data. By mitigating and transferring the risk can manage the risks. Security Specialist mitigates the risk by using protecting and security mechanism whereas protection from harm on any networked computer system will never be 100% so there are so many insurance companies coming into existence.

Cyberinsurance covers the cyber-losses because of lack of Security mechanisms.

Insurance industry is new and is started in 1998 but necessity for this knowledge has been rapidly growing day by day. Cyberinsurance is like the traditional insurance and has many policies. Insurer and Insured Company are at the two points of this contraction and have to respect the instructions.

IT specialists have to evaluate the security items of the insured company. Security parameters of the insured company are related to the system security, software, hardware and clients who work in this domain. They suggest solution to improve security statements and encourage them to use from special productions. The premium will be estimated by insurer and it depends on the security statements and the budgets. After contract, insured company pays the premium and insurer covers cost of cyber-losses. Every agreemental cases or changes must be written in insurance policies. Improving this knowledge is moving slowly because it is new and a few companies know about the benefits of this industry. Most of the companies tend to use it for third party liability to cover customer-losses. Nowadays insured companies seldom invest for first party insurance.

Risk Management in Cyberspace: Risk was evaluated in 3 levels (low, moderate and high). It is based on the value of assets and vulnerabilities existed by threats. We try to prevent from high risk. Totally there are four options for managing the risks:

- Avoiding the risk
- Retaining the risk
- Mitigating the risk
- Transferring the risk

The first option is to avoid being exposed to cyber-risks by not having any dependence on computers, networked machines, or any internet website. For most

Corresponding Author: N. Ghavami, Researcher, IT security group of Iran Telecommunication Research Center, Iran
E-mail: N.ghavam@itrc.ac.ir

commercial organizations this is not economically possible. The second option is to retain the risk based on a conscious decision that it is more cost effective to absorb any loss internally or other risk management options are unaffordable. Retaining the risk is sometimes the only choice due to lack of financial resources. The third option is to mitigate risk using managerial and technical processes. This involves investment in people and devices to identify threats and prepare counter-measures with continually improving security processes. The fourth option is to transfer risk to a third party, in which case this third party must be licensed as an insurance company for performing this function. Insurance allows an individual or organization to smooth payouts for uncertain events into predictable periodic costs. Typically an individual or organization employs a combination of these risk management options simultaneously- retaining some of the risk, mitigating some of the risk and insuring the rest of the risk. For example, a firm may choose to have an internet website protected by security processes but yet avoid the risks of certain internet transactions. One increasingly common risk management approach is to retain all or most of the risk while transferring the risk mitigation function to a third party due to a superior expertise and cost efficiencies of the third party. Another common risk management hybrid is transferring specific risks via a product warranty or service contract. Combining the two perspectives of insurers and individuals/organizations together, the primary business logic of cyberinsurance is as follows:

- As internet connectivity increases, the vulnerability of organizations to damages, organizations seek to manage this risk using cyberinsurance as one option in concert with other risk management options.
- Organizations that manage risk using cyberinsurance as one option have increasing economic incentives to reduce exposure in tangible ways, for example by following 'best practices' specification of the techniques and equipment to be used for security protection. The economic incentives take two primary forms: (1) lower insurance premiums (discounts) for better security protection and (2) financial oversight which increasingly requires individuals/organizations to demonstrate that they protect their networked resources (considered part of fiduciary duty for executives in most commercial organizations).
- Cyber insurers recognize the opportunity to profit from the cyber insurance risk management option and offer policies while simultaneously developing standards for insurability. Insurers are driven to find the best metrics in order to define profitable price ranges for different coverage's given supply and demand.
- The end result is a market-solution with aligned economic incentives between cyberinsurers and individuals/organizations. Cyberinsurers seek profit opportunities from accurately pricing cyberinsurance and individuals/organizations seek to hedge potential losses [1].

History of Cyberinsurance: The first wave of specialized coverage for computer crime appeared in the late 1970s in the US. These policies were an extension of traditional crime insurance for electronic banking and were primarily designed to cover the uncertain losses which arose from outsiders gaining physical access to the computer systems [1].

Lloyd's of London is oldest British insurance market and serves as a meeting place where multiple financial member whether individuals or corporations, come together to pool and spread risk. After April 1998 a new insurance product to protect against the effects of actual or potential attacks on an insured's computer systems has been introduced by this company and Lloyd's broker Jardine Lloyd Thompson [3].

In 1998, the first advent of insurance policies against electronic holes was seen. These hacker protection products were partnerships between technology and insurance companies to offer a combination of technology services and first party insurance. These products provided limited coverage amounts of approximately US$250,000 per year [1].

The Y2K phenomenon saw the inception of a new variant of cyber insurance. These products focused upon the effects of Y2K type system interruptions rather than cyber crime. Post 2002, as traditional business insurance excluded cyber risks, a small number of insurance companies began to develop specialized products which better catered for the modern range of cyber risks.

Furthermore, February of 2000 had seen a series of coordinated DoS attacks launched against US corporations (including Yahoo.com, eBay.com, Buy.com, Amazon.com, CNN.com, ZDNet.com, Datek, E-Trade and others). In addition to these, cyber criminals began

engaging in a myriad of attacks, including website defacements, phishing, identity theft, computer intrusions and attacking authentication systems [1].

Meanwhile, the cyber-hurricane seemingly arrived. Events surrounding September 11th, 2001 somewhat undermined the development of cyber insurance products. The 9/11 terrorist attacks brought about an increasing fear in insurers regarding exposure to exotic risk categories. The three most serious Internet worm attacks took place during the three month period around 9/11, namely Code Red in July, Nimda in September and Klez in October of 2001. Slammer hit in January of 2003 [1].

At that time computer security Institute of FBI announced In one week approximately 1200 U.S. sites, including those belonging to the White House or another governmental agency had been subjected to DoS attacks or defaced with pro-Chinese images [5].

With businesses and government agencies heavily affected during 2000-2003, a re-focus on the need for managing IT security risks became apparent [1].

All these factors ultimately gave rise to the subsequent redevelopment of cyber insurance products [1]. The Insurance Information Institute in 2002 forecasted that cyber insurance could become a US$2.5 billion market by 2005 to 2006 [1].

In 2005 analyzed several cyberinsurance policies and compared economic theory with the reality of what was happening in the marketplace [1].

"Unfortunately, most companies are operating in a 21st century threat environment with 20th century insurance coverage," states John Spagnuolo, cyber expert for the Insurance Information Institute (I.I.I.). "The dynamics of risk management have changed with technology."

The insurance industry has developed cyber insurance products to help businesses confront the growing number of network security risks that have the potential to shutdown a network, destroy vital data or steal customer information. For example, as the public becomes more concerned about privacy, businesses will become more aware that they are liable if their customers' personal information is compromised. However, only a small number of businesses are reportedly properly insured.

The business community's awareness of cyberinsurance does not seem high. Only 7 percent of business respondents in an survey said they knew for sure that their firms have specific insurance coverage for cyber risks [7].

Historical background of insurance in Iran goes back to 80 years ago when two Russian companies ventured to open their branch offices In the early 1970s many new insurance companies were established and at the same time the Law establishing Bimeh Markazi Iran (Central Insurance of Iran) was passed in the Parliament. After the Islamic Revolution in 1979, the work permission of foreign insurance agencies in Iran has been withdrawn and ten of the insurance companies were merged in Dana Insurance Co.

For the first times in Iran, cyberinsurance researches in concepts and policies have been started since 2006 in Iran Telecommunication Research Center.

Coverage Types of Cyberinsurance: Cyber insurance covers legal liability to others, web content liability, professional liability, network security property loss, business interruption, crisis communication. Most of the references are divided cyberinsurance to three general classes:

First party coverage: First party coverage typically cover destruction or loss of information assets, internet business interruption, cyber extortion, loss due to denial of service attacks, reimbursement for public relation expenses and even fraudulent electronic fund transfers.

Third Party Liability Coverage: Third party coverage typically cover claims arising from Internet content, Internet security, technology errors and omissions and defense costs.

Exclusions: Exclusion relates to losses due to failures of electric and telecommunication facilities, including electronic failure and satellite malfunction.

These conditions are featured in policy exclusions and typically include: failure to backup, failure to take reasonable steps to maintain and upgrade security mechanisms, fraudulent, dishonest and criminal acts of the insured and claims arising out of liability to related parties.

Cyberinsurance Contract Steps: Insured company and insurer have to sign the insurance contract. It is the steps:

Ex ante is initial step that there is no contraction then the insured company selects the type of insurance coverage. The risk assessment starts with the applicant filling in an application form with the detailed security questionnaire, some consisting of about 250 queries,

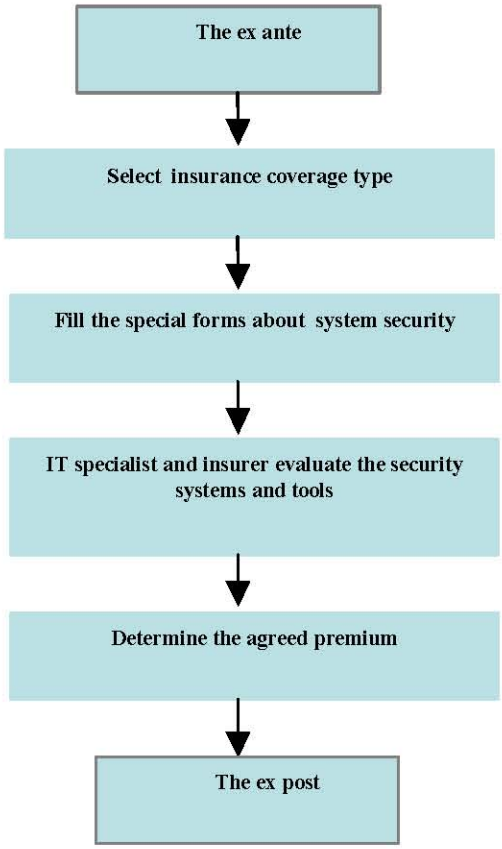

Fig. 1: Cyber insurance contract steps

to assess security risks and cyber protections (technology budget, security infrastructure, virus-protection programs, testing and safety procedures and outsourcing). General background questions include information on the applicant's Standard Industrial Classification (SIC) code; what Internet sites are proposed for insurance, including number of pages, customers/users and page views; the annual sales and revenues, including revenue generated from Internet activities; IT budget and percentage of it earmarked for security; and what are specific Internet activities conducted (e.g., email and web browsing, production and internal processes integration, e-commerce, VPN, third party hosting services, consulting, etc.) [1].

After this step according to the value of information and the risk, premium will be estimated. Policies were listed in the contract. The beginning and ending of contraction, responsibilities and premium are registered.

Whereas IT security level is low, Insurers also use monitoring of the firm's security processes; IT level depends on:

- Investment in technological products
- Rules and policies in IT security
- Security awareness and training program's level of IT security.

Some of the insurer company suggest insured company to use special products because they rely on them knowing about the security level of these products.

The Barriers to the Diffusion of the Cyber Insurance: Since insurers rely on measures of predictability to forecast probable risk and set prices, the absence of enough historical and actuarial data for Internet risks makes it harder to determine prices. It takes both time and stability to develop statistical data for actuarial tables; At the Internet new ventures are developed at a fast pace, flaws in software change dynamically and new attacks are released daily. Furthermore, future risks are unknown since both hackers and anti-hacking technology are getting better. New attacks in cyberspace are released daily and they are unpredictable so there are several forces preventing the diffusion of cyber insurance. Regarding to prematurely of information security in developing countries these problems are more little than the developed countries, it sounds many problems in this type of insurance industry. Some of these problems are as fallows:

- Lack of agreement on basic policy definitions and language: Constant developments in IT environments result in ambiguity about what is insured, what risks are covered and how losses will be assessed. Thus, lack of standard policy language is preventing the expansion and maturity of the cyber insurance market.
- Cyber insurance is relatively new and more importantly firms have resisted revealing losses resulting from vulnerabilities. These cause:
- Insured Organizations are less likely to invest in order to maintain or upgrade security measures because they rely on the coverage of the insurer to maintain the agreed level of preventative measures ex post (after contract agreement) so they invest lower to prevent from these problems [4].
- Risk has different levels. A low premium for a low coverage contract which is designed to cover low risk firms and a high premium for a high coverage contract which is designed to cover high risk firms

[4]. Adverse selection arises from the information asymmetry problem. In an ideal world, parties to a contract will have perfect information ex ante (prior to contract agreement).

However, it is generally acknowledged that such symmetry in information does not exist in the real word. Consequently, in the insurance setting, it can be difficult for the insurer to differentiate between high and low risk applicants, skewing the intended insurance portfolio with a disproportionate amount of high risk applicants.

In the case where the insurer cannot differentiate high and low risk firms, there is incentive for the high risk applicant to mimic the low risk applicant and purchase the low premium product. Consequently the initial objective would not be obtained [4].

- One of the barriers to the diffusion of the cyber insurance is lack of adequate reinsurance. In other fields of property/casualty insurance, underwriters commonly purchase reinsurance to protect themselves against unusual, extreme losses. But the limited nature of claims experience for IT security is restricting the growth of the related reinsurance industry.
- Like other property/casually policies, those covering vulnerabilities of IT security typically exclude claims resulting from acts of war, riot, civil commotion and similar disaster known as force major. Yet these may be precisely the risks that businesses fear most and want to insure against.
- Assessment the value of IT security investment isn't defined as a standard so insured company face to determine premium.

CONCLUSION

Although cyberinsurance started near 10 years ago, only few companies in telecommunication and information technology field, are aware of that. Cultural activities and public informing are the first steps to introduce this kind of insurance to others. It is very important that insured companies deliver complete and accurate information about their security mechanism and policy to insurer companies to sign a contract and calculate the premium. A supervisor team is assigned a to test and check security important items such as implemented computer systems, staff personality and software applications to find the security status of insured company and determine corresponding premium. In order to resolve adverse selection and appropriate investing for setting up security in communication and information technology section, they suggest reliable security products. In this way not only insurer is informed about the security level of insured company but also insured company gets a discount for installing a professional security system and pay lower premium. Based on initial field studies in some IT companies in Iran, following activities must be carried on in order to use this type of insurance:

- Cultural activity and public informing related to cyberinsurance.
- Estimate premium corresponding with security investment.
- Supply insurance policy after consultation and negotiation between insurer and insured company.(It is important to know that writing an insurance policy is too hard because in this space we observed attacks and vulnerability are continuously changed.)
- Having confidence and secrecy are the most important things for developing and implementing insurance policy [13].

REFERENCES

1. Kesan Jay P., P. Majuca Rupterto and J. Yurcik William, 2006. The evolution of cyberinsurance, Department of Economics,College of Law, University of Illinois at Urbana-Champaign.
2. ISN, 1998. Information Risk Group Joins Underwriters at Lloyd's -- London ….,From: mea culpa.
3. Insurance service network, LLOYD'S MARKET OFFFRS 'ANTI-HACKER' INSURANCE.
4. The Economic Viability of Cyber Insurance: Seeking Financial Certainty in IT Security, 2006. version:1.00,Presented by SIFT, Originated in Australia,
5. Vatis Micheal, June 2002. Cyber Attacks:Protecting America's Security against Digital Threats, ESDP-2002-04.
6. Gohring Nancy, 2002. July. Cyberinsurance may cover damage of computer woes, http:// seattletimes. nwsource.com/ html/ businesstechnology/ 134502269_cyberinsurance29.html, By, Seattle Times business reporter

7. National News, Insurance Journal, 2003. Aug.
8. Kevin Savez, 2002. May. Data Insurance, Cover your Most Value Assets- The Intangible Ones, First Published: New Architect.
9. Kesan, Jay P., P. Majuca Rupterto and J. Yurcik William, 2005. CyberInsurance As a Market-Based Solution to the Problem of CyberSecurity-A Case Study.
10. Karhade, Prasanna, Security of Information Technology Assets and the Diffusion of Cyber Insurance, Term paper.
11. Bohme, R., 2005. Cyber-Insurance Revisited.
12. Bohme, R. and G. Kataria, 2006. Models and Measures for Correlation in Cyber-Insurance (Working Paper: Revision 0.3).
13. Kalantari, R., N. Ghavami and M. Rahimi, 2007. Feasibility study report of Using cyberinsurance in Iran, 2007. Iran Telecommunication Research Center.