Discussion on Existing problems and Countermeasures of Cyber-security-insurance

Jianqiang GU
School of Economics and Management, Southeast University, Nanjing, CHINA

Abstract: Hackers can continue to find new vulnerabilities in information system, so the current rely solely on technology cannot completely eliminate the information system security risk. One new tool is the use of recently developed cyber-security-insurance to hedge its potential losses from cyber crime and shift risks of information security. This paper discusses the existing problems of the cyber-security-insurance and gives some relative countermeasures to solve these problems.

Keywords: Cyber Security; Insurance; Interdependent Risk; Moral Hazard; Countermeasure

1. Introduction

Internet and information systems plays an increasingly important role in the business, but hackers can continue to find new vulnerabilities in information systems. Intrusions can have obviously catastrophic results to a company, damaging its reputation and business, causing a loss of customers and market share. To reduce the probability of risk, many organizations invests in defence technologies, such as antivirus, firewall and intrusion detection technique. However, the current rely solely on technology cannot completely achieve a perfect protection and eliminate the information system security risk. A widely used way to eliminate the residual risk is through insurance. Cyber-security-insurance is a risk management tool by which information security risk are transferred to the commercial insurance companies and it is designed to mitigate losses from a variety of cyber incidents, including data breaches, business interruption, and network damage. With cyber-security-insurance, firms can balance their expenditures between investing in security protections and keeping away from the enormous risks. Having a right insurance coverage for the residual risk that enables a company to deal effectively with information security accidents and give an company some real competitive advantages.

There are many insurance companys offering cyber-security-insurance contracts, may offer coverages such as privacy and security liability, computer forensics investigation, hacker damage costs and cyber extortion. Survey by authoritative organisations report that cyber-security-insurance generates approximately $500 million in premiums and the market is growing at a steady rate of 10% to 25% annually with midsized and smaller companies making up a larger segment of customers. Despite the benefits of cyber-security-insurance, the market for cyber-security-insurance is also face with some significant challenges and development issues.

2. Existing Problems of Cyber-security-insurance

Accepted reasons for the developmental disorder of the cyber-security-insurance market are industry inexperience(scant empirical data), information asymmetries and interdependency of information security risks.

2.1. Industry Inexperience

Pricing of cyber-security-insurance products must rely on the massive historical data. However, cyber-security-insurance is a relatively new field, particular insurance risks assess and insurance premium calculation are based solely on models because of a lack of available data. Lack of data also makes cyber-security-insurance products appear less desirable to companies, while simultaneously increasing the price of cyber-security-insurance products. Such a trend is extremely detrimental to the future viability and long-range development of the information security industry.

2.2. Information Asymmetries

Cyber-security-insurance as a kind of new insurance mode, has not only the characteristics of general insurance ,but also its unique aspects. For example, Investment in hardware and personnel of the client can be observed by the insurance company. However, for the reasons of asymmetric information, the efforts of the client can't fully observation and supervision for the insurance company. Under the premise of minimizing the investment costs, the client maybe reduce their efforts in information security, this is the classic moral hazard prob-

lem. On the other hand, the output of information security has a certain randomness which lead both organization can not evaluate security result perfectly. It is perfectly possible that some security events can be observed on both sides; Some security events cannot be observed on both sides; some security events can only be observed unilaterally. Another feature is that responsibility is difficult to clear, this is mainly due to the incompleteness of contract, or removing evidence by the hacker. The insured may act in a more insecure manner by investing in less security after the acquisition of insurance because they now know that the insurer will bear the loss.

2.3. Interdependent Security

Given the increased interconnectivity by electronic data interchange (EDI) and the more recent vendor managed inventory (VMI) program, the security of one firm may depend on not only the security measures taken by itself but also the security measures taken by other firms. The hacker who has penetrated one firm's network may steal sensitive data about the partners or penetrate the connected firms via the trust connections relatively easily. Because of the network externalities of security investments, self-interested firms often invest at a level lower than the social optimal level. As the number of firms/organizations gets large, increasing marginal cost among individual firms also makes it harder to mount a coordinated policy response to increased risk that it will be contaminated by other unprotected firms. This makes the scope of security risk is difficult to be determined and increases the possibility of themselves suffering a destructive blow by multiple claims occurring at once. The propagation of computer viruses maybe cause "cyber-hurricane"– a major disaster resulting in great number of claims, which makes it difficult for insurance companies to spread the risk across its customers. It is represent an uncertain risk of very large losses, and as such are very difficult for insurers to withstand.

3. Countermeasures

Taking about problems emerging in the rapid development of cyber-security-insurance industry, we put forward some suggestions and measures as follows.

3.1. Gain Experience

It's an obvious but true statement that cyber-security-insurance is advancing at a rapid pace, probably more rapidly than at any other time. This is the golden opportunity for insurance companies to accumulate a large amount of historical data, the business process is just the process of collecting and accumulating historical data, clients' security information and market data. At present, information system has been established in almost every company, it is mainly used for dealing with daily work data, which lead to the accumulation of the enormous history data. Based on the enormous history data, insurance companies can analyze and find out the actuarial tables to conduct their business.

3.2. Contract Design

In some cases, different risk allocation means are provided in different contract conditions, which can lead customers to take appropriate responsibility to protect itself, resulting in more secure of the network. There are two ways to design contract. One way is to design different contracts for different risk types, relying on the agents' incentives to self-protect. Here, self-protect refers to protect themselves by technical measures of information security body (firewall technology, encryption technology, VPN, anti-virus software, etc.) to ensure that the information system security. That is, for the customers whose self-protect is lower than a critical level, the insurer may offer a high premium; for the customers whose self-protect is greater than a critical level, it may offer a low premium. Another way is to restrict insurance coverage,e.g. by requiring a deductible in the insurance policy. With a deductible, each individual has to bear part of their own loss and is likely to have more of an incentive to investment in self-protection.

3.3. Government Subsidies

Because of the influence of the infectious risk, this risk interdependent of information system security on the internet causes a negative externality that results in under-investment in self-protection relative to the socially efficient level by ignoring marginal external costs or benefits conferred on others. Mandatory safety standards maybe an effective way, but such a requirement appears practically difficult to implement. So the government should subsidise all or part of the enterprise, make the marginal private benefit is equal to the society as a whole, inducing firms to internalize the risk correlation effects and to adopt the socially optimal self-protection strategy. Government subsidies can be divided into two kinds, one is direct subsidies, through paying immediate cash to the companies, the second is indirect financing, including tax, technical guidance and other policies.

3.4. Reinsurance

Consider an effective approach aimed at controlling and reducing the fear of a "cyber-hurricane" among insurers, the government and relevant departments can increase the supply of cyber-insurance by providing reinsurance to cyber-security-insurance companies. Reinsurance refers to insurance purchased by an insurer, which is insurance for losses associated with natural disasters, such as hurricanes, earthquakes, and floods, which can also be applied to the fields of information security. This would increase the adoption of cyber-insurance by reducing prices, with price reduction caused both by decreased

supply cost and increased competition in the cyber-insurance market and will solve the most important problem with the cyber-insurance market, the fear of a "cyber-hurricane". Another approach is to offer a tax deduction to encourage insurers to increase the capital reserves used to pay out cyber-security-insurance claims.

3.5. Collaborate with MSSP

Outsourcing selected managed security services (MSS) by forming a partnership with a Managed Security Service Provider (MSSP) is often a good solution for managing information security risks. MSSP can leverage economies of scale by assembling skilled security professionals and have insight into security situations based on extensive experience, dealing with hundreds or thousands of potentially threatening situations every day.MSSP can help the insurance companies to overcome the information asymmetries through collection of operational information and to improve efficiency in enforcing the related requirements in contracts between the two organizations.

4. Conclusion

Managing information security risks is challenging to many firms. The appearance of cyber-security-insurance brought a new tool for the firms to transfer the security risks to a third party. However, the advent of cyber-security-insurance also brings many challengs that require our urgent attention, including industry inexperience(scant empirical data), information asymmetries and interdependency of information security risks. On how to solve the above developmental disorders, we present a range of solutions and measures, which concerns both the efficiency and the feasibility.

References

[1] Zhao X, Xue L, Whinston A B. Managing interdependent information security risks:cyberinsurance managed security services,and risk pooling arrangements[J].Journal of Management Information Systems, 2013,30(1):123-152.

[2] Kunreuther H, Heal G.. Interdependent security[J]. Journal of Risk and Uncertainty, 2003,26(2-3):231-249.

[3] Zhuang J, Bier V M, Gupta A.Subsidies in interdependent security with heterogeneous discount rates[J].The Engineering Economist, 2007,52(1):1-19.

[4] Shetty N, Schwartz G, Walrand J.Can Competitive Insurers improve Network Security[C]//Trust and Trustworthy Computing.Berlin: Springer-Verlag, 2010: 308-322.

[5] Schwartz G, Shetty N,Walrand J. Economics of Information Security and Privacy [M].Berlin: Springer-Verlag,2010.

[6] Garcia A, Horowitz B.The potential for underinvestment in internet security: implications for regulatory policy[J].Journal of Regulatory Economics, 2007, 31:37-55.

[7] Lelarge M, Bolot J.Economic incentives to increase security in the internet:The case for insurance[C]//INFOCOM, Los Alamitos: IEEE, 2009:1494–1502.

[8] Juliette F, Insurance industry responds to cyber attack increase, Insurance Networking News[N]. (Apr. 20, 2012).

[9] Radosavac S, Kempf J, Kozat U.Using insurance to increase internet security[C]//Proceedings of NetEcon, Seattle:ACM, 2008:43-48.

[10] Majuca R P, Yurcik W, Kesan J P.The evolution of cyberinsurance[R].ACM Computing Research Repository,2006.