INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 2 ISSUE 6 (2016) PAGES 1477 - 1481
RECEIVED : 24/11/2016. PUBLISHED: 08/12/2016
December 8, 2016

IMPROVING TECHNICAL SECURITY USING NETWORK SECURITY THROUGH CYBER INSURANCE

[1]Ramanavathi.B, [2]Anjugam.P,
[1]M.Phil Scholar, Dept of computer science and Applications, KMG College of Arts & Science, Gudiyatham,
[2]Asst prof, PG and Research Dept of computer science and Applications, KMG College of Arts & Science, Gudiyatham.

Abstract:

In recent years, security researchers have well established the fact that technical security solutions alone will not result in a robust cyberspace due to several issues jointly related to the economics and technology of computer security. In this regard some of them pro-posed cyber-insurance as a suitable risk management technique that has the potential to jointly align with the various incentives of security vendors (e.g., Symantec, Microsoft, etc.), cyber-insurers (e.g., security vendors, ISPs, cloud providers, etc.), regulatory agencies (e.g., government), and network users (individuals and organizations), in turn paving the way for robust cyber-security. In this work, we theoretically investigate the following important question: can cyber-insurance really improve the security in a network? To answer our question we adopt a market-based approach. We analyze regulated monopolistic and competitive cyber-insurance markets in our work, where the market elements consist of risk-averse cyber-insurers, risk-averse network users, a regulatory agency, and security vendors (SVs).

Keywords : ISP, Cyber Insurance, Network.

1. INTRODUCTION

The infrastructure, the users, and the services offered on computer networks today are all subject to a wide variety of risks posed by threats that include distributed denial of service attacks, intrusions of various kinds, eavesdropping, hacking, phishing, worms, viruses, spams, etc. In order to counter the risk posed by these threats, network users have traditionally resorted to antivirus and anti-spam software, firewalls, intrusion-detection systems (IDSs), and other add-ons to reduce the likelihood of being affected by threats. In practice,a large industry (companies like Symantec, McAfee, etc.) as well as considerable research efforts are currently centered around developing and deploying tools and techniques to detect threats and anomalies in order to protect the cyber infrastructure and its users from the resulting negative impact of the anomalies. Cyber-insurance is a risk management technique via which network user risks are transferred to an insurance company, in return for a fee, i.e., the insurance premium. Examples of potential cyber-insurers might include ISP, cloud provider, traditional insurance organizations. Proponents of cyber-insurance believe that cyber-insurance would lead to the design of insurance contracts that would shift appropriate amounts of self-defense liability to the clients, thereby making the cyberspace more robust. Here the term ‘self-defense’ implies the efforts by a network user to secure their system through technical solutions such as anti-virus and anti-spam software, firewalls, using secure operating systems, etc. Cyber-insurance has also the potential to be a market solution that can align with economic incentives of cyber-insurers, users (individuals/organizations), policy makers, and security software vendors. i.e., the cyber-insurers will earn profit from appropriately pricing premiums, network users will seek to hedge potential losses by

jointly buying insurance and investing in self-defense mechanisms, policy makers would ensure the increase in overall network security, and the security software vendors could experience an increase in their product sales via forming alliances with cyberinsurers.

2. RELATED WORK

The establishment of the EU Telecom Package Article 13a breach notification regime is one plank in the evolving European regulatory regime governing cyber-security which will lead to a more systematic collection of actual data in relation to incidents. The EU Directive 2009/140/EC16 amends existing directives on telecommunications networks and associated facilities. Article 13a introduces a requirement for providers of public communications networks to take measures to guarantee the security and integrity of these networks and to ensure continuity of services provided over these networks. In particular, paragraph 3 says that providers should report significant security breaches and losses of integrity to the respective National Regulatory Authorities (NRAs). Annually, summary reports should be sent to ENISA (European Network and Information Security Agency) and the European Commission. The aggregated analysis of the incident reports will describe the current trends and provide knowledge and information to NRAs and operators. Similarly, the recent announcements under the reform of the EU's legal framework governing privacy and data protection that breach disclosure reporting (with possible fines) has the potential to play into the market communication of risk. In January 2012, EU's Justice and Fundamental Rights Directorate General disclosed that breach notification was being proposed to apply to certain Internet businesses controlling or processing personal data (in line with the extant EU Data Protection Directive 95/46/EC). The proposed law would require such business to inform a regulator within hours after having become aware of an attack and data subjects as soon as reasonably feasible. Since there are different views in the literature about whether being insured is the IT risk or the cost of IT risk (conceptually two different things) perhaps better information on the likely costs of IT risks would help to address these problems. Note that this is different from a breaching cost, which takes into account and may perhaps even focus exclusively on secondary costs. Finally, an example of recent relevant regulatory intervention from across the Atlantic can be seen in the United States where the Securities and Exchange Commission (SEC) in 2011 required that all regulated firms should disclose the risk of cyber incidents. Expectations in the market are that this will trigger many firms buying cyber-insurance in order to communicate to the market information that they are properly managing these risks. The new rules also require those regulated by the SEC to evaluate and take into account all available relevant information including prior cybersecurity incidents and severity and frequency of those incidents. Disclosures under these rules require that the regulated firms include a description of relevant insurance coverage.

3. CYBER INSURANCE

Cyber insurance refers to insurance contracts having the purpose of covering a broad range of issues relating to risks in cyberspace. Researchers have identified contracts as covering things like: liability issues, property loss and theft, data damage, loss of income from network outage and computer failures or web-site defacement. Other examples may include data asset protection, cyber-extortion and, more indirectly, liability arising from negligence relating to personally identifiable data. In addition, there is also coverage for cyber-liability which covers the insured's liabilities (defence and compensatory damages) where a third party, under a negligence claim, can pursue a tortuous or delict claim for injury. For example: the third party being affected by a virus; personally identifiable

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 2 ISSUE 6 (2016) PAGES 1477 - 1481
RECEIVED : 24/11/2016. PUBLISHED: 08/12/2016
December 8, 2016

data belonging to the third party was disclosed or the business of the third party was interrupted as a result of negligence by the insured. Many first and third party risks of this nature are generally excluded from traditional commercial general liability policies. An insurance contract (policy) binds an insurance company in the occurrence of contractually defined loss events to pay a specified amount (claim) to the insurance holder. In return, the insurance holder pays a fixed sum (premium) to the insurance company. The cyber-insurance contract is signed between the insured company and the insurer and includes aspects relating to the selection of the coverage type, the risk assessment phase of security and cyber protections and the evaluation of the security systems and tools by IT specialist and insurer. In many respects, cyber-security risks appear to exhibit some of these properties as to make them a valid candidate for insurance. Many people use similar operating systems, software so there are a large number of similar exposure units. Moreover, there is the potential for accidental loss. Finally, it is certainly possible to identify the time of a loss. Conversely (as we shall see) losses might be interdependent and there is uncertainty as to the upper bound – there is no robust data which would help underwriters predict, calculate losses or indeed whether they might be catastrophically large.

4. ANALYSIS

Some of the measures that can be taken by a firm to protect itself against damages arising from a cyber-incident can be identified as: self -protection, self-insurance and cyber- insurance. Self – insurance and cyber-insurance both aim at the reduction of the losses' size. With cyber insurance the firm purchases insurance from a third party while self-insurance is an internal investment to be used in case of loss. On the other hand, self-protection attempts to reduce the probability of any losses that may occur. In addition, a firm may be exempt from liability in certain regulated areas as stipulated by criteria set out a specific National Regulatory Authority. Confounding the theoretical barriers and literature indicating that there is no mature cyber- insurance market identified above, according to a recent report by Lloyds, the market for cyber-insurance has 'taken off'.

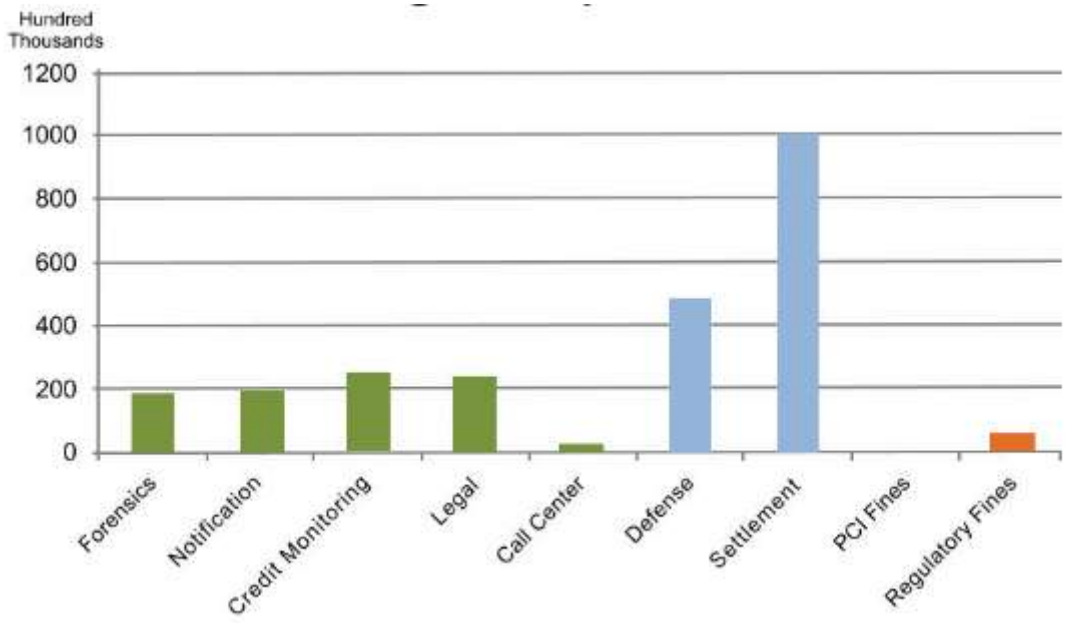

Fig.1.System Analysis

This is spurred on by strengthened legislation in both the US and Europe. Sectors typically buying cyber insurance include retailers, healthcare providers, hotels and financial services – all of which typically buy data breach insurance. Demand was reported to be growing amongst UK and European companies following expectation about regulatory intervention for breach notifications. The state of market offerings is also of course related to the question of re-insurance with which we deal below. Nonetheless, some industry data as presented appears to contradict the assertions that this market is either immature or non-existent. At a recent conference on emerging risks, it was suggested that the overall UK market (in terms of exposure for claims) for cyber-insurance was worth US$250m. The insurance carrier issues and upholds the risk associated with an insurance policy. The 2011 Betterley Report concluded – based on a survey of the cyber/privacy/media liability market in the US - that there were some carriers in the market but that the number of data breaches is increasing, raising a note of concern as to whether coverage will remain available concludes. This report also defines insurance products as covering data risks for example losses of customer client records, e-commerce (selling products, services or content) or social networking. It goes on to remark that, in 2011, The demand side is made up of organisations interested in or having purchased or renewing an insurance policy which covers them in case of a realisation of a risk. PwC's Global State of Information Security Survey in 2010 reported that 4 out of 10 firms surveyed were taking out insurance policies to protect against damage caused by data loss. This is driven by high profile legal problems, according to the firm.

CONCLUSION

Collecting data on such re-insurance activities across the EU Member States in other contexts (e.g. in the domain of terrorism). This recommendation could be investigated by Member States and the European Commission. In conclusion, we have seen that there exists a deal of uncertainty about the cyber-insurance market and about whether the theoretical barriers identified actually play a role. There appears to be contradictory evidence in this regard. On the one hand, economists and those studying the economics of information security84 argue that these barriers are preventing a market from developing. On the other hand, there are indications that this market does exist and there are offerings and firms both supplying and demanding cyber-insurance. Further exploration of this gap, along with some simple 'quick-wins' might be worthy of further consideration, under the caveat that they would not claim to 'solve' a problem of which we are still uncertain actually exists.

REFERENCES

[1] Information Asymmetry. Internet Wikipedia Source.

[2] G. A. Akerlof. The market for lemons - quality uncertainty and the market mecha- nism. Quarterly Journal of Economics, 84(3), 1970.

[3] R. Anderson, C. Barton, R. Bohme, R. Clayton, M. J. G. Eaten, M. Levi, T. Moore, and S. Savage. Measuring the cost of cybercrime. In WEIS, 2012.

[4] R. Anderson and T. Moore. Information security economics and beyond. In Informa- tion Security Summit, 2008.

[5] A. L. Barabasi and R. Albert. Emergence of scaling in random networks. Science, 286, 1999.

[6] R. Bohme. Personal communication.

[7] R. Bohme and G. Kataria. Models and measures for correlation in cyber-insurance. In WEIS, 2006.

[8] R. Bohme and G. Schwartz. Modeling cyber-insurance: Towards a unifying frame- work. In WEIS, 2010.

[9] P. B. Bonacich. Power and centrality: A family of measures. American Journal of Sociology, 92, 1987.

[10] O. Candogan, K. BImpikis, and A. Ozdaglar. Optimal pricing in networks with exter- nalities. INFORMS Operations Research, 60(4), 2012.