Review Article | Impact Factor: 0.621 | ISSN: 2319-507X
Vishakha Rajukar, IJPRET, 2014; Volume 2 (9): 984-991 | IJPRET

INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

A REVIEW ON THE ECONOMICS OF CYBERSECURITY AND CYBERSECURITY POLICY

VISHAKHA M. RAJURKAR

Department of Computer Science & Engineering, IBSS College of Engineering, Amravati.

Accepted Date: 27/02/2014 ; Published Date: 01/05/2014

Abstract: The design of effective policies to enhance and maintain cyber security must take into account a complex set of incentives facing not only the providers and users of the internet and computer software, but also those of potential attackers. Measures undertaken to defend against attacks must take into account that, like other forms of criminal and terrorist activity, the attackers are not passive agents (unlike nature in the case of natural hazards), and the design of effective policies must recognize, to the extent possible, that the defensive measures will elicit strategic responses from the attacker. There also are potentially serious incentive issues arising from classical problems of externalities and public good problems that encourage underinvestment in cyber security by private parties (e.g. businesses and software developers). Lastly, reducing the probability of cyber attacks and/or the consequences of cyber attacks is not costless. In principle, well-designed policies should balance benefits from defensive measures against their costs (which include important concerns about privacy). The paper examines how these questions can be addressed using fairly standard principles and tools from economic policy analysis and potential policy research questions.

Keywords: Cyber security, Cyber security policies, Cyber attacks.

PAPER-QR CODE

Corresponding Author: MS. VISHAKHA M. RAJURKAR

Access Online On:

www.ijpret.com

How to Cite This Article:

Vishakha Rajukar, IJPRET, 2014; Volume 2 (9): 984-991

INTRODUCTION

In May 2011, McKinsey and Company released a major study documenting the world-wide economic impact of the internet. A widely-cited statistic from the report is that on average, the internet has added between 3 and 4 percentage points to the gross domestic products of the economies of the developed world. In terms of the United States, this translates into additional total output of between $440 and $580 billion, or between $1400 and $1,900 per capita. This amount does not include what economists call the "consumer surplus" associated with the internet which, according to McKinsey equals on the order of $200 to $330 per year in economic value enjoyed by consumers. As the report goes on to note, based on its estimated economic value, the contribution of the internet to economic output is comparable to or exceeds that of each of the following sectors in the economy: transportation, education, communication, agriculture, utilities, and mining. These amounts do not directly measure the key role played by the internet in areas such as national security, or as intermediate inputs into other economic sectors. Because of its considerable national importance, the internet poses a large and tempting target for criminal activities aimed at illegally extracting economic value from internet producers and consumers, as well as for terrorist activities aimed at inflicting economic or other harm on the United States through internet attacks. There is, therefore, broad social value, and also economic value, in identifying policies to reduce: (a) the likelihood of such attempts, (b) the likelihood that such attempts will succeed should they take place, and (c) the expected consequences of such activities.

Cyber attacks pose considerable risk for many companies. They cause business interruptions due to Denial of Service attacks and can result in the loss of intellectual property and business secrets. Potential losses include: merger plans, loss of customer data coupled with reputational damage and possible litigation costs etc. According to the Identity Theft Resource Center, 17,491,690 records where breachedin2012. Furthermore, the spread of new technologies such as Cloud Computing, mobile devices, and social media increases vulnerability to cyber attacks, as the focus of customers' lies on using those technologies to enhance the efficiency of their business - not the security. Due to heavy competition, producers of such technologies also prefer to focus on fast product development, not necessarily the security of those products and services.12 At the same time, more businesses have become increasingly reliant on storing massive amounts of data electronically, often using outsourcing or third-party software. Facing those threats, companies have developed an increasingly sophisticated supply of technologies and services. Facing those threats, companies have developed an increasingly sophisticated supply of technologies and services. These include firewalls and encryption over specialized personnel to specific cyber insurance policies.

LITERATURE REVIEW

Cyber Attacks

Cyber-attack is any type of offensive maneuver employed by individuals or whole organizations that targets computer information systems, infrastructures, computer networks, and/or personal computer devices by various means of malicious acts usually originating from an anonymous source that either steals, alters, or destroys a specified target by hacking into a susceptible system.

Factors for cyber-attacks

Fear factor

The most common, fear factor, a cyber terrorist will create fear amongst individuals, groups, or societies. The bombing of a Bali nightclub in 2002 created fear amongst the foreign tourists who frequently visited the venue. Once the bomb went off and casualties ensued, the influx of tourists to Bali significantly reduced due to fear of death.

Spectacular factor

With spectacular factors, it is the actual damage of the attack, meaning the attacks created direct losses and gained negative publicity. In 1999, a denial of service attack rendered Amazon.com unusable. Amazon experienced losses because of suspended trading and it was publicized worldwide.

Vulnerability factor

Vulnerability factor exploits how easy an organization or government establishment is vulnerable to cyber-attacks. An organization can easily be vulnerable to a denial of service attack or a government establishment can be defaced on a web page. A computer network attack disrupts the integrity or authenticity of data, usually through malicious code that alters program logic that controls data, leading to errors in output.

Cyberinsurance: What are the Issues?

Cyberinsurance is defined as “the transfer of financial risk associated with network and computer incidents to a third party,” the insurance company, in exchange for a premium. Cyberinsurance policies are usually very client-specific and negotiated on a case-by-case basis. Cyberinsurance policies are available for first-party and third-party coverage. Cyberinsurance policies offer benefits similar to insurance in other areas:

1.Without the possibility of transferring risks, risk-averse companies and companies looking to bear risks do not find each other in the market place, resulting in market inefficiency.

2.Because insurers can differentiate between companies through rates premiums and (lower premiums for low-risk companies), insurers can incentivize investment in IT security. This market-based process facilitates the adoption of standards and metrics for IT security.

3.As demand for cyberinsurance increases, best practices spread through the economy. Insurance improves the systemic resilience of a national economy and distributes risk fairly. Hence, insurance would help to boost IT security, rather than government regulations. From a practical perspective, there is a business case to be made for cyberinsurance. The losses incurred from cyber attacks are growing as new technologies spread and reliance on technology increases. There are also arguments against cyberinsurance and skepticism about its positive effects. Some believe that the risks associated with cyber attacks are not quantifiable and thus, not insurable (at least not to the degree promised by insurers). Another point against cyberinsurance is that it may provide companies with 'an easy way out': instead of working on their security, they just buy insurance. Many participants at a government sponsored roundtable discussion expressed skepticism about the capabilities of insurers to provide appropriate incentives for better IT security.

Evolution of the market and challenges

While there is disagreement about the exact birth date of cyberinsurance policies, it is clear that the market is relatively new and not yet mature. Considering the potential benefits of cyberinsurance as outlined above, the first cyberinsurance policies sparked hopes that "cyberinsurance might become as important and as ubiquitous in the IT security toolbox as [...] firewalls and antivirus software." Government officials also praised cyberinsurance as an important mechanism to increase IT security. However, the growth of the cyberinsurance market has somewhat been tentative and slow, prompting experts to revise their initial forecasts for the evolution of the market. Until recently, few companies planned to buy cyberinsurance policies and an even fewer number actually bought cyberinsurance policies. Still, the market for cyberinsurance policies is here to stay and expected to grow in the future. Yet, the market for cyberinsurance still faces challenges, some comparable to other new insurance markets

These challenges include:

1."traditional" insurance market challenges: a. information asymmetry b. moral hazard c. adverse selection

2. cyberinsurance challenges:

a. legal framework i. uncertainty about liability ii. spotty coverage and insurance loopholes iii. lack of standards or "bad" standards. The challenges under 2a affect companies, insurers, and the government (which is ultimately responsible for the legal framework). Liability rules have not caught up to the challenges new technologies create. This prompts questions like: "should companies focus their cyber risk management efforts on patching vulnerable IT products, or should IT manufacturers and suppliers focus on poorly written code before bringing their products to market?" Furthermore, coverage of cyber insurance policies remains very spotty, sometimes without companies realizing that a specific event is not covered. Policy exclusions have yet to face court judgments.

b. conceptual issues i. quantification of risks and costs ii. cyber risk not seen as a business problem or underestimated iii. correlated, interrelated and global risks iv. lack of re-insurance. The challenges under 2b provide a number of interesting questions for further research, many of which effect insurance companies.. As stated in the introduction, both stakeholders have difficulties quantifying risks and costs, be it for investments in IT security or for losses incurred through cyber attacks.

Suggestions for a research agenda

Cyberinsurance is a welcome and needed addition to the strategies used to deal with the risk of cyber attacks. As in other markets and initial skepticism notwithstanding, cyberinsurance policies are here to stay. However, as the foregoing discussion shows there open questions to what will lead to a more mature cyberinsurance market. The question remains whether one wants to give markets time and accept some initial inefficiencies, or whether one should actively address open issues, be it through research or government action. First steps in this direction are already being undertaken, see the studies by Advisen and Net Dilligence and the work of (Innerhofer-Oberperfler und Breu 2010). This type of research should be extended to cover not only the loss of data, but other risks and costs. To structure the research agenda, we have grouped some specific questions around the three categories Policy, Management, and Technology.

1.Policy

1.Establish a better understanding of CEO attitudes towards cyber risk and preferences towards mitigation strategies by engaging social science, cyber security and finance experts 2. Study regional variations in approaches to cyber insurance across the globe and identify common patterns and features.

2.Management

1.Explore feasibility of constructing a causal model of cyber threat/response mechanism at enterprise level. 2.Analyze potential of a global cyber loss data base with proper privacy controls and a business model that would make such a data base viable and sustainable.3. Develop a "big data" strategy linking actual cyber losses and specific variables under the control of management .

3.Technology

1.Map cyber risk variations for different technology platforms (both in house and Cloud) and provide insights on IT industry perspectives as these platforms change and become more interlinked. 2. Review Computer Science curricula and identify courses dealing with technology approaches to cyber risk and risk management as an explicit strategy.

Interview Outcomes

To complement the literature review, a handful of experts and professionals where ask to provide input. The information they provided is referenced as Questionnaire. he small sample of eight people included an insurance lawyer, two insurance companies that offer cyberinsurance policies, a commissioner from the

National Association of Insurance Commissioners, a representative at the Insurance Services Office, a representative from a defence contractor, a private sector CISO, and an academic. A snowball-sampling was used starting from an initial sample of publicly available contacts. Given resource constraints, the purpose of the sampling was not to be representative, but to get as many different perspectives on the issue as possible within a reasonable time frame. Once the sample was identified, data was collected through a questionnaire that was either sent to respondents via e-mail or was used as a basis for an interview (in the case respondents did not want to fill out the questionnaire but still provide insights). The interviews were not transcribed, but answers were noted by the researchers during the interview. All participants consented to being asked and have their answers used for this paper.

a. None of the interviewees thinks that cyberinsurance is just a fad. Instead, all agreed that the market will grow although they differed regarding the speed of growth.

b. Awareness of cyber risks varies wildly and while growing, risks are still misunderstood and underestimated.

c. Cyberinsurance should play a role in the overall risk management strategy of a company but it should be used in a strategy mix.

d. Cyber risks are different from other risks and insurers as well as companies have to take this into account.

Summary and Future Research

There are a number of areas in which future research can strengthen what is already known about the nexus between economics and cyber-security.

• From the perspective of policy analysis, much of the current literature is case-specific.

Specific policy applications are scattered throughout, often as brief examples. More work is needed to turn conceptual insights from this literature into practical policies.

• Policy analysis of cyber-security options can learn from the evolution of policy in other areas, most notably environmental policy and homeland security policy.

• Cyber security policy analysis can also benefit by drawing on insights from the research of Nobel Economics Laureate Elinor Ostrom which focuses on the development of voluntary institutions as response to private market failure.

• Insights can also be gained by comparative analysis of policies in other countries, especially the European Union.

• Empirical work on the effects of actual government policies is still relatively sparse. Important empirical questions about the effects of cyber security policies include: How does regulation affect the development and use of cyber security technologies? How can one measure the social costs and benefits of investments in cyber security? Based on the development of such measures, what are the measured benefits and costs of greater investment in cyber security.

REFERENCES

1. Anderson Ross and Moore, Tyler, 2006. "The Economics of Information Security" Science 314(27) pp. 610-613.

2. Anderson, Ross: Economics and Information Security Resource Page: http://www.cl.cam.ac.uk/~rja14/econsec.html#Homepages

3. Asaf, Dan, 2007. "Government Intervention in Information Infrastructure Provision."

4. Anderson, Roberta D. "Insurance Coverage for Cyber Attacks - Part One of a Two-Part Article." The Insurance Coverage Law Bulletin 12, no. 4 (2013).

5. Anderson, Roberta D. "Insurance Coverage for Cyber Attacks - Part Two of a Two-Part Article." The Insurance Coverage Law Bulletin 12, no. 5 (2013).

6. Clinton, Larry. "Cyber-Insurance Metrics and Impact on Cyber-Security." Internet Security Alliance, undated.

7. Duffy, Daintry. "Cybersecurity Insurance: Safety at a Premium." Cybersecurity Insurance: Safety at a Premium. http://www.cio.com/article/217739/Cybersecurity_Insurance_Safety_at_a_Premium, December 2002.

8. Gandal, Neil, 2006. "An Introduction fo Key Themes in the Economics of Cyber Security." Unpublished paper, Tel Aviv University and CEPR.

9. Murdoch, Steven, 2010. Security Economics. Presentation on Feb. 26, 2010.

10. Powell, Benjamin, 2004. "Is Cybersecurity a Public Good; Evidence from the Financial Services Industry." Unpublished working paper, San Jose State University.

11. Vila, Greenstad, and Molnar, 2003. "Why We Can't be Bothered to Read Privacy Policies: Models of Privacy as a Lemon's Market." Paper presented at the Fifth International Conference on Electronic Commerce (ICEC 2003), Pittsburgh, PA.