CYBERSECURITY AS A RELATIVE CONCEPT

Xingan LI

Abstract: Based on the relativity of the concept of cybersecurity, this article analyzes the economic impact of cybersecurity breaches, identifies cybersecurity as a private good that should be provided mainly by the private sector. However, public provision is also necessary when severe security breaches occur and liability mechanisms should be triggered.

Keywords: Cybersecurity, Illegal Behavior, Economic Analysis.

Introduction

The Internet has become a critical infrastructure for both public and private sectors and has brought new levels of productivity, convenience, and efficiency. The increasing incidents of Internet attacks representing examples of how vulnerable the information systems are, how far the offensive technology outpaces the defensive technology, how easy various malicious programs are created and how smart they can spread all over the Internet rapidly, have started to impact the practical facets of our lives. At the same time, the attackers are able to conceal their attacks by disabling logging facilities or modifying event logs, so their activity goes undetected. Even worse, some automated programs have been designed to specifically disable anti-virus software or penetrate firewalls. The security violations have multi-dimensional impacts on both consumers and businesses, including time, human resources, monetary losses and psychological losses.

The Internet and the larger information infrastructure are not secure.[1] McCormick identified five reasons why Internet is vulnerable: failing to enforce policies, ignoring new vulnerabilities, relying too much on technology, failing to thoroughly investigate job candidates, and expecting too much from technical skills.[2] These risks cause serious insecurity problems in the information society.[3]

While the governments have made efforts to better secure their own computer networks to prevent terrorists from hacking into computer systems, the governments have been increasingly concerned that the private sector is vulnerable to cyberterror-

INFORMATION & SECURITY. An International Journal, Vol.18, 2006, 11-24.

ism. The question being asked is whether private businesses provide enough cybersecurity, or some form of government involvement is justified. Many empirical studies examined the economic impact of cybersecurity breaches. Theories diversify in regarding the cybersecurity as an externality,[4] a public good,[5] or a private good.[6]

Based on the concept of relative cybersecurity, this paper analyzes the economic impact of cybersecurity breaches, whether cybersecurity is a public good or a private good. It also establishes liability mechanism for cybersecurity breaches.

Impact of Cybersecurity Breaches

Increasing Investment of Users in Cybersecurity

The users' investment in cybersecurity takes on the tendency of increasing. Although exact statistics on these expenditures is unavailable, the add-up of global users' financial costs will reach a surprising figure. According to a survey conducted by the Computer Security Institute (CSI) and the Federal Bureau of Investigation (FBI), nearly all of the companies surveyed in 2005 used anti-virus software, firewall, and some measures of access control. Besides the hardware and software, the organizational users also have to employ security personnel or institutions to maintain their systems. These measures induce the increase of the investment of network users. But in fact, security measures can hardly ever be a perfect assurance against damage and accidents. Absolute security becomes too expensive to be reasonable.[7]

Frequent Occurrence of Cybersecurity Breaches

Although the investment in cybersecurity is increasing year by year, the breaches still occur frequently. The potential for information security breaches, as well as the magnitude of potential losses associated with such breaches, has been confirmed by empirical studies.

The annual surveys on information security breaches have pointed out that cybersecurity breaches are ubiquitous. The 2005 survey conducted by CSI and FBI revealed that 56 percent of the surveyed 693 U.S. computer security practitioners acknowledged unauthorized use of a computer in their organization in the last 12 months.[8] CERT Coordination Center reported that the computer security vulnerabilities increased nearly 35-fold during one decade with 171 separate holes reported in 1995 and 5,990 reported in 2005.[9] In the recent years, the publicly disclosed virus attacks are billing the global computer users in an accelerated speed, even though many of the users are unaware of, or unwilling to report the losses.

Increasing Costs of Cybersecurity Breaches

As a consequence of the frequent occurrence of cybersecurity breaches, the losses of these breaches are increasing as well. The losses can be divided into direct and indirect, tangible and intangible, and short-term and long-term. Neumann stated that costs of cybercrime are difficult to measure; however, these costs are reasonably substantial and growing rapidly.[10] Scholars proposed various models to try to measure the costs of security breaches, such as in the Forrester Research. Howe and colleagues' analysis indicated that, if the perpetrators were to unlawfully transfer $1 million from an online bank, the financial influence to the bank would reach $106 million.[11]

The direct losses are those directly involved in the attacks, including interruption of business, destruction of software and hardware, expenditure on recovering the systems, installation and update of security means, recruiting security personnel, etc. The indirect losses are losses indirectly related to the attacks, such as reduction of consumers, decrease of stock prices, etc. The other kinds of losses are also easy to emerge.

The 2005 CSI/FBI survey noted that, of the 639 respondents that were willing and/or able to estimate losses due to security breaches, such breaches resulted in losses close to $130 million.[12] On the other hand, Lukasik claims that cybercrime costs are essentially doubling each year.[13] The problem becomes even more complex when one considers the "black figure" of these crimes. Ullman and Ferrera mentioned that, according to FBI estimates, only 17 percent of computer crimes are reported to government authorities.[14]

Relativity of the Cybersecurity Concept

There are various answers to the question "What is cybersecurity?" Cybersecurity is a comparative concept. On one hand, it includes the comparison between security and attack techniques. On the other hand, it includes comparison between different security techniques and measures. Considering the comparison between the techniques for security and attack, it is publicly well recognized that the attack techniques develop faster than the security techniques, regardless of the reasons. In other words, the hardware, the software, or the other information system components are always vulnerable and this fact can be exploited. We could call this the absolute level of security. Considering the comparison between the different security techniques, the existence of different environments, the possession of different hardware, software and other equipment, and the adoption of different security techniques, all this leads to difference in the level of security. Therefore, each of the individual or organizational users has a different security level.

Some viewpoints regard cybersecurity as an externality.[15] Camp and Wolfram point out that if a company does a poor job at cybersecurity, other companies may be affected negatively. Thus, the cost is an externality to the owner of the infected machine.[16] However, if we identify cybersecurity as an externality, it is inevitable that to the extent investments in computer security create positive externalities, too little will be provided.

Security is not the reason that drives the attackers to violate security and launch attacks, nor the condition that facilitates the attacks, but the target that the attacks aim at. In fact, there is no clear boundary between security and insecurity. Security and insecurity have only quantitative difference, but no quality distinction. Neither absolute security nor complete insecurity exists. That is to say, security and insecurity should be considered as security between zero percent and 100 percent. Therefore, security is a relative concept. The security of a higher level is security, while the security of a lower level is insecurity.

Although the information systems on the Internet all have a similar framework, they lack any central control system and are uncontrollable. Not only the physical system, but also the operational process is uncontrollable. Thus, to a great extent, the security of the Internet depends on the security measures taken by the end users, either individuals or organizations. However, the security measures of individual and organizational users are widely different due to the difference in hardware, software, and human resources.

The level of security of the end users on the network is different; an absolute value of security does not exist. Security is just a comparison of relative values. It is both the result of comparison between users and the comparison between past and present, i.e., horizontal and vertical comparison. Due to the large number of network users and the rapid change in the network environment, the result of this comparison changes constantly. In general, a higher level security will change quickly into a lower level security (insecurity) with transformation of techniques and the environment. Therefore, the cybersecurity measures have to be updated and renewed timely, frequently, and efficiently.

If the cybersecurity measures cannot be updated and renewed in a timely, frequent and efficient manner, vulnerabilities might occur. Vulnerability is not the security or insecurity themselves, but a factor that makes it impossible to realize perfect security, and an extra loophole caused by the external factors in the investor's production of the expected complete security. It is the natural adversary of the security product, i.e., flaws that can be detected and exploited by the potential attackers to commit harm and cause loss.

Table 1: Classical Division of Goods in Economy.[17]

Classic Division of Goods in Economy		*Exclusion from Consumption*	
		YES	*NO*
Competition in Consumption	*YES*	Private Good: Food, Clothing, Toys, Furniture, Cars…	Common Good: Natural Environment
	NO	Club Good: Private Schools, Cinemas, Clubs…	Public Good: National Security (Army and Police Forces)

Provision of Cybersecurity as a Private Good

In economics, goods are traditionally classified into four categories as listed in Table 1.

Besides other issues, private good and public good can be generally regarded as a pair of opposites. The main features of the private good are excludability and rivalry. According to Samuelson,[18] public good is a good that produces a positive externality and which is characterized by non-rival consumption and non-excludability. The private provision of private goods, or public provision of public goods are not the unique ways in providing these two kinds of goods (let us not consider the other kinds of goods here). The ways of provision of these two kinds of goods can be illustrated as shown in Table 2.

The public good is usually confronted with the problem of being underprovided or not being provided when it is put on the private market. Such a problem appears in providing cybersecurity. Generally, a higher level of cybersecurity would benefit both the individual or organizational owner and users other than the owner. Because insecure computers are vulnerable to be manipulated to launch attacks against other computers, it is reasonable to assume that if an owner maintains a higher level of cybersecurity, the other users' computers may experience a lesser risk of being attacked. Then the other users would have the good reason to reduce their investment in security protection. The computer users' security provision only diminishes the probability of the others' computers being attacked. However, since individuals are not generally liable for the damage caused when a hacker uses their computer, they do not benefit from the increased security.[19] And because users with ability to provide security do not benefit, they will fail to provide it. The same applies to other computer

Table 2: Ways of Provision of Private Goods and Public Goods.

Different Ways of Provision of Different Goods	*Private Provision*	*Government Provision*	*Mixed Provision*
Private Goods	Clothes, Food, Cars, Private Housing	Food Supply as in Communist China in the End of 1950s	Transportation, Medical Care
Public Goods	Foreign Aid	National Defense	Pollution Reduction

owners, and, therefore, everybody is in a worse situation than would be if everyone provided the security that would have spillover benefits for everyone else.

As we have seen, cybersecurity is both excludable and rivalrous. Cybersecurity has neither territorial boundary nor industrial limit. In the global village, all individuals and organizations are confronted with risks of the same level. In this environment, the security of individuals or organizations' systems matters firstly to themselves. Only in some accidental situations are others involved, such as in the case of DOS attacks.

Powell provides evidence from the financial services industry to prove that cybersecurity is hardly a public good.[20] Individuals and organizations have excludability in cybersecurity. The excludability of cybersecurity roots in the three characteristics of cybersecurity, i.e., confidentiality, integrity and availability, among which confidentiality fully expresses the excludability of cybersecurity. We could see the situation this way: if security is available to one user, it is unavailable to other users, and if others enjoy security, ones' security does not exist any longer. Unsurprisingly, cybersecurity is characterized as preservation of confidentiality, ensuring that information is accessible only to those authorized to have access; integrity, safeguarding the accuracy and completeness of information and processing methods; availability, ensuring that authorized users have access to information and associated assets when required. The users' security is enjoyed solely by themselves. Any sharing entails that systems become insecure. In fact, hackers are precisely the exploiters and sharers of insecure systems. Therefore, cybersecurity has more excludability than any private good.

On the other hand, the cost of expanding security to others is not zero, but enormously high. If one user enjoys a higher level of security, the level of security of the others will relatively decrease. As mentioned above, there is no perfect security. Security and insecurity are relative concepts that exist in comparisons. If one enjoys a higher level of cybersecurity, the level of security of the others will decrease to insecurity. The competition between the security measures is the reason that causes increase of the difference between the relative securities. Of course, the enhancement of the total security level benefits from that competition.

Katyal's study stresses that to some extent private security measures may increase crime.[21] The basic assumption behind this argument is that, if one household locks its door, the thief will turn to the neighbor whose doors are left unlocked. Therefore, locking of one's own door breaks the reciprocity and mutual trust in the neighborhood. If we consider the fact that currently nearly all households, companies, and even government agencies "lock their own doors," we can easily conclude that this assumption is absurd. Only when every household, company and governmental agency is convinced not to take such "inefficient" measures is such an assumption significant. The author believes that such an assumption ignores the dual value of locking in the prevention of crime: on one hand, locking protects from damage and harm, making the potential criminals shrink back at the sight, or taking criminals more time before suffering losses; on the other hand, locking increases the potential criminals' time consumption and material costs in looking for new victims, and even making it impossible for them to find one. If none of the households and organizations locks their doors, potential criminals can easily find possible targets. Therefore, the difficulty of crime will decrease, and the efficiency will increase. The potential criminals are indifferent about costs, benefits, likelihood of success.

This pertains particularly to cybersecurity. If every computer owner is encouraged not to use security control, the computer will be more vulnerable to attacks. Assuming that the environment and the potential of all individual and organizations' computers are the same and the risk of being attacked is also approximately similar, then only when the benefits related to cybersecurity are equal could the provision of public cybersecurity be efficient. But this situation rarely exists in reality. Therefore, an unlimited public cybersecurity would be excessive for some individuals and organizations and insufficient for others. The situation of abundance is economically inefficient, while the situation of insufficiency is inefficient in terms of security. Hence, both ways, the public cybersecurity control cannot function optimally. In result, if cybersecurity is provided in the mode of public good, it is impossible to be more beneficial than as a private good.

Kobayashi notes that cybersecurity is different from traditional security.[22] To discourage crime *ex ante* in the general criminal context, the government could implement sufficient level of punishment to deter the crime from accruing. In the case of cybercrime, the likelihood of detecting is so low that the penalty imposed would have to be of considerable magnitude to deter cybercrime. In what follows, the author will explore the possibility of establishing liability for the different participants in the process of cybersecurity provision.

Public Provision of Cybersecurity: Liability Mechanisms

Even if it were technically feasible to keep all systems 100% secure, the costs would have been so prohibitive as to render such an approach an economic prescription for disaster. The government can neither provide cybersecurity nor manipulate the systems. Naturally, one of the Ernst & Young survey's key findings was that only 11% deemed government security-driven regulations as being highly effective in improving their information security posture or in reducing data protection risks.[23] However, any argument stating that the governments can play no role in the field of cybersecurity is over skeptical. The governments can play a necessary role in deterring the attackers, but they are by no means helpless in the maintenance of an adequate level of cybersecurity. Their roles are to impose penalty through legislation and deter crime by means of *ex post* law enforcement. Providing cybersecurity as a public good is confronted with greater difficulties in international cooperation than as a private good. Even if some countries can convince their taxpayers to pay for the expenses involved in the public provision of cybersecurity, if you cannot simultaneously convince all countries to do so, it will not be cost-efficient. In this section, the author will analyze the characteristics of the possible liability of various players in the field of cybersecurity.

Liability of Hackers

Ballon argues that the major benefits of holding the hacker liable for the damage he causes is that the target has more choices and control in applying the law against hackers.[24] Compared to a criminal action, the liability of hackers can be justified by that it grants the plaintiff "greater control over the litigation and potentially better long-term relief;" that it encourages attack reporting;[25] and that a target will have the motive to recover losses at the same time of punishing the perpetrator.[26]

The disadvantage of tort liability of hackers lies in two aspects: on one hand, the plaintiff has to pay a significant amount of money before receiving any compensation; on the other hand, most hackers have had and will have greater incentives to be judgment-proof.[27] If a hacker has little to lose under tort liability mechanism, his most rational choice will be to hide more secretly himself and his assets.[28] In the networked world, tracking a hacker or finding his money will need more energy, time, and costs, and will even prove to be an impossible task. As a result, the hacker would carry out the act more judgment-proof. Even worse, the hacker might be forced by the civil actions to commit other money-harvesting offences to support his actions.

Currently, dozens of countries have enacted domestic law against cybercrime. In addition, there have also been successful international legal actions, such as the Convention on Cybercrime (2001) and other domestic provisions.[29] Although the legisla-

tion is already there, the practical effects are doubtful. There are many hackers but the detection probability is quite low and the application of legislation is rare.

Liability of Internet Service Providers

Internet Service Providers (ISP)'s tort liability plays an important role in the following two cases: first, a lower level of ISP's security standard might be exploited by hackers; and second, the ISP's vicarious liability for its employee's security breach makes it easier to recover the target's losses.[30] To justify the first aspect, an important economic consideration is that the ISP's cost to improve its security level is lower compared to the hackers' high potential cost to society, and with the security standard the security condition becomes more certain and reliable.[31] This would be expected to lower the overall cost of the Internet service, provide incentive for Internet participation, and increase the value of the network to society.[32] There is no theoretical obstacle in applying the tort liability to cybersecurity breaches.

The only problems in applying tort liability to all ISPs is that there is no uniform standard; that it would be difficult to provide such a standard; and that dual or multiple standard would surely motivate some ISPs to maintain a lower level of security due to economic reasons. The result of this dilemma will be that no deterrence functions on hackers.

Liability of Security Problems Publishers

The security (holes) publisher has two aspects of gain from the publication, one is that the publication can prevent some harm suffered by the general public, the other is that the publication realises more economic or other benefits. However, it takes great risk resulting in users' losses in case hackers exploit the publicized loopholes. In addition, the users have to invest in improving their security protection when they know the new publicized loopholes.

According to Coarse's general principle,[33] whether the publisher should be held liable for his publication is a question of whether the gain of both the general public users from stopping the potential harm and the publisher himself from obtaining a higher confidence value is greater than the losses that the users suffer from the attacks launched exploiting the publicized loopholes and from the extra investment in preventing such attacks. In different cases, the cost effectiveness is different, and is hard to prove. Finally, as Preston and Lefton put it:

> The question is not whether an individual publication causes more harm than good; it is whether a particular rule of liability governing computer security publications causes more harm than good.[34]

Liability of Security Providers

The rapid growth of the computer security industry leads people to consider whether security providers should be held liable when their products and services fail to protect against hackers. Developing higher security level of products and providing high security level of services are costly, but work to prevent hacking from taking place. Security providers' liability will create incentives for them to provide products or services of at least a standard level. The products and services containing security holes take great risks of product liability if their advertisements stated that they are "hack-proof."[35]

The problem with holding security providers liable is that goods and services are usually provided subject to contract or licensing agreements, making tort liability inappropriate because the parties have bargained to allocate the risk between them.[36] The reasonable way in which the agreements are concluded is that neither of the two parties wants to bear more risk. But in general, the party of product or service users might have the greater discretion in choosing with more guarantees and less expenses. The security providers will be generally worse-off.

Liability of Software Vendors

Most of the security holes come from the bad design of software (and sometimes hardware). The software vendors control the only key to solve this problem through fixing their software. However, this work also consumes human resources and investments in terms of money. Therefore, vendors generally do not have the incentive to do so. A way to incorporate their better work into their best interests is to raise the risk of liability, which will raise the cost of their products. If software vendors have liability costs, they will pass those on to users. In turn, the vendors might as well pay to fix the problems.

Liability of Software Authors

Since the authors of software (the programmers) have the biggest opportunity to prevent problems, it seems appropriate to focus on making them responsible for the security of their products.[37] Nonetheless, there are some unique aspects of computer software that make it challenging to apply traditional notions of product liability.

Under such circumstances, if we impose liability on the authors, it is impossible, because the author gets no income to pay the compensation; it is inefficient, because the author would be discouraged from contributing; and it is also unfair, because the users use the software for free and voluntarily.

Liability of System Owners

Systems can be both targets and tools in attacks. For example in a Distributed Denial of Service attack, the attacks are launched from numerous manipulated computers. The owners of such systems, who use software written and sold by third parties, cannot fully secure their systems, cannot stop unforeseeable outsiders' exploitation, and have no way to reduce the risks. In order to hold the system owners liable, two prerequisites are necessary to be in place: the establishment of a security standard, and the mechanism of insurance. The latter was discussed by Fisk in analogy to vehicle operators who are often legally required to carry insurance against accidents.[38]

Conclusion

This article argues that cybersecurity is a private good and should be provided mainly by the private sector. Regarding cybersecurity as a public good would discourage the private sector to invest in security provision. From this standpoint, an early government intervention would reduce the effectiveness and efficiency of cybersecurity. However, in terms of prevention of security breaches, law enforcement can play an important role in establishing and enforcing liability mechanisms. Although it is still controversial whether and how cybersecurity players should be held liable for their activities, every step made in this direction will bring benefits to the private sector to achieve their goals.

Acknowledgement

The author wishes to express his appreciation to Jenny and Antti Wihuri Foundation, the Department of Law at the University of Joensuu, and the Finnish Cultural Foundation, for their generous financial support for his current research. He also wishes to thank the Finnish Economic Education Foundation for supporting him in the early stage of this research. Certainly, the responsibility for the contents is the author's.

Notes:

[1] National Research Council, *Cryptography's Role in Securing the Information Society* (Washington, DC: National Academy Press, 1996).

[2] John McCormick, "Five Reasons You're not Secure," 5 April 2005, <insight.zdnet.co.uk/internet/security/0,39020457,39193819,00.htm> (14 Dec. 2005).

[3] Dan Farmer, "Shall We Dust Moscow?: Security Survey of Key Internet Hosts & Various Semi-Relevant Reflections," November-December 1996, <http://www.trouble.org/survey/> (14 Dec. 2005).

[4] Jennifer A. Chandler, "Security in Cyberspace: Combating Distributed Denial of Service Attacks," *University of Ottawa Law & Technology Journal* 1 (2003-2004): 231-261, <http://www.uoltj.ca/articles/vol1.1-2/2003-2004.1.1-2.uoltj.Chandler.231-261.pdf> (14 Dec. 2005).

[5] Christopher Coyne and Peter Leeson, "Who Protects Cyberspace?" Working Paper 24 (George Mason University, Department of Economics, Global Prosperity Initiative, 2004), <http://www.mercatus.org/pdf/materials/616.pdf> (14 Dec. 2005).

[6] Benjamin Powell, "Is Cybersecurity a Public Good? Evidence from the Financial Services Industry," Working Paper Number 57 (The Independent Institute, 15 March 2001), <http://www.independent.org/pdf/working_papers/57_cyber.pdf> (14 Dec. 2005).

[7] Torgeir Daler, Roar Gulbrandsen, Birger Melgrd, and Torbjorn Sjølstad, *Security of Information and Data* (Ellis Horwood, January 1989), 15.

[8] Lawrence A. Gordon, Martin P. Loeb, William Lucyshyn, and Robert Richasrdson, *Tenth Annual CSI/FBI Computer Crime and Security Survey* (Computer Security Institute, 2005), 11, <http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2005.pdf> (14 Dec. 2005).

[9] CERT Coordination Center, *CERT/CC Statistics 1988-2005* (2005), <http://www.cert.org/stats/cert_stats.html> (14 Dec. 2005).

[10] Peter G. Neumann, "Information System Adversities and Risks" (paper presented at the Conference on International Cooperation to Combat Cyber Crime and Terrorism, Stanford, CA: Hoover Institution, 1999).

[11] Carl Howe, John C. McCarthy, Tom Buss, and Ashley Davis, "The Forrester Report: Economics of Security," (February 1998).

[12] Gordon, Loeb, Lucyshyn, and Richasrdson, *Tenth Annual CSI/FBI Computer Crime and Security Survey*, 15.

[13] Stephen J. Lukasik, "Protecting the Global Information Commons," *Telecommunication Policy* 24, no. 6-7 (2000): 519-531.

[14] Robert L. Ullman and David L. Ferrera, "Crime on the Internet," *Boston Bar Journal*, no. 6 (November/December 1998).

[15] L. Jean Camp and Catherine Wolfram, "Pricing Security," in *Proceedings of the CERT Information Survivability Workshop* (Boston, Massachusetts, 24-26 October 2000), 31-39, <www.ljean.com/ files/isw.pdf> (14 Dec. 2005).

[16] Camp and Wolfram, "Pricing Security."

[17] Source: "Good (Economics and Accounting)," Wikipedia, the free encyclopedia <http://en.wikipedia.org/wiki/Good_%28economics%29> (15 Dec. 2005).

[18] Paul A. Samuelson, "The Pure Theory of Public Expenditure," *Review of Economics and Statistics* 36 (November 1954): 387-389.

[19] Hal R. Varian, "System Reliability and Free Riding," in *Proceedings of the First Workshop on Economics and Information Security* (University of California, Berkeley, 16-17 May 2002), <http://www.sims.berkeley.edu/resources/affiliates/workshops/econsecurity/econws/49.pdf> (14 Dec. 2005).

[20] Powell, "Is Cybersecurity a Public Good? Evidence from the Financial Services Industry."

[21] Neal Kumar Katyal, "The Dark Side of Private Ordering for Cybersecurity," in *The Law and Economics of Cybersecurity*, ed. Mark F. Grady and Francesco Parisi (Cambridge University Press, November 2005).

[22] Bruce H. Kobayashi, "An Economic Analysis of the Private and Social Costs of the Provision of Cybersecurity and Other Pubic Security Goods," *Supreme Court Economic Review* 14 (2005), <http://law.bepress.com/gmulwps/gmule/art26> (15 Dec. 2005).

[23] Earnest & Young, *Global Information Security Survey 2004*, BYG No. FF0231, <http://www.ey.com/global/download.nsf/International/2004_Global_Information_Security_Survey/$file/2004_Global_Information_Security_Survey_2004.pdf> (14 Dec. 2005).

[24] Ian C. Ballon, "Alternative Corporate Responses to Internet Data Theft," in *17th Annual Institute on Computer Law* 737, 744 (PLI Patents, Copyrights, Trademarks & Literary Prop. Course, Handbook Series No. 471, 1997).

[25] David L. Gripman, "The Doors Are Locked but the Thieves and Vandals Are Still Getting in: A Proposal in Tort to Alleviate Corporate America's Cyber-Crime Problem," 16 *J. Marshall J. Computer & Information Law*, 167 (1997): 174-176.

[26] Michael Hatcher, Jay McDannel, and Stacy Ostfeld, "Computer Crimes," *American Criminal Law Review* 36, 397 (1999): 406.

[27] James Brooke, "Calm Scene Isn't Really, Police Say," *New York Times*, 22 April 2000, C1.

[28] Mary M. Calkins, "They Shoot Trojan Horses, Don't They? An Economic Analysis of Anti-Hacking Regulatory Models," *Georgia Law Journal* 89, no. 171 (November 2000): 214-217.

[29] Convention on Cybercrime 2001.

[30] David Icove, Karl Seger, and William VonStorch, *Computer Crime: A Crimefighter's Handbook* (O'Reilly and Associates, Inc., August 1995): 427.

[31] Icove, Seger, and VonStorch, *Computer Crime.*

[32] Marc D. Goodman, "Why the Police Don't Care about Computer Crime," *Harvard Journal of Law and Technology* 10, no. 3 (1997): 465-494.

[33] Ronald H. Coase, "The Problem of Social Cost," *Journal of Law and Economics* 3 (1960): 1-44.

[34] Ethan M. Preston and John Lofton, "Computer Security Publications: Information Economics, Shifting Liability and the First Amendment," *Whither Law Review* 24, no. 71 (Fall 2002): 130.

[35] Natalee Drummond and Damon J. McClendon, "Cybercrime – Alternative Models for Dealing with Unauthorized Use and Abuse of Computer Networks," (Summer 2001), <http://gsulaw.gsu.edu/lawand/papers/su01/drummond_mcclendon/> (14 Dec. 2005).

[36] E. Gabriel Perle, Mark A. Fischer, and John Taylor Williams, "Electronic Publishing and Software," Part A, *Computer Law* (January 2000).

[37] Mike Fisk, "Causes and Remedies for Social Acceptance of Network Insecurity" (paper presented at Workshop on Economics and Internet Security, University of California, Berkeley, 16-17 May 2002), 3, <http://www.sims.berkeley.edu:8000/resources/affiliates/workshops/econsecurity/econws/35.pdf> (14 Dec. 2005).

[38] Fisk, "Causes and Remedies for Social Acceptance of Network Insecurity."

XINGAN LI, born in 1967, LLB (1989), LLM (1994), is Associate Professor at Inner Mongolia University Law School. He was a visiting scholar at Kyushu University (2000-2001), and researcher at the University of Lapland and the University of Joensuu. His research interests are criminology, criminal psychology, criminal law and criminal procedural law, and particularly, cybersecurity and cybercrime. His publications include the books "Criminal Law of England and Wales," "Principles of Criminal Law," and several papers on economic crime, cybersecurity and cybercrime. *Address for Correspondence*: Sepänkatu 15 C 57, 80110 Joensuu, Finland; *Phone*: +358 044 910 7632; *E-mail*: li@cc.joensuu.fi.