

THREE ESSAYS ON THE LAW AND ECONOMICS  
OF INFORMATION TECHNOLOGY SECURITY

BY

RUPERTO PAGAURA MAJUCA

B.S., University of the Philippines at Diliman, 1991  
J.D., Ateneo de Manila University, 1996

DISSERTATION

Submitted in partial fulfillment of the requirements  
for the degree of Doctor of Philosophy in Economics  
in the Graduate College of the  
University of Illinois at Urbana-Champaign, 2006

Urbana, Illinois

UMI Number: 3250284

### INFORMATION TO USERS

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleed-through, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

**UMI**<sup>®</sup>

---

UMI Microform 3250284

Copyright 2007 by ProQuest Information and Learning Company.

All rights reserved. This microform edition is protected against unauthorized copying under Title 17, United States Code.

ProQuest Information and Learning Company  
300 North Zeeb Road  
P.O. Box 1346  
Ann Arbor, MI 48106-1346

# CERTIFICATE OF COMMITTEE APPROVAL

University of Illinois at Urbana-Champaign  
Graduate College

October 16, 2006

*We hereby recommend that the thesis by:*

**RUPERTO PAGAURA MAJUCA**

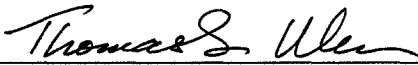
*Entitled:*

**THREE ESSAYS ON THE LAW AND ECONOMICS OF INFORMATION  
TECHNOLOGY SECURITY**

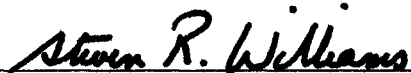
*Be accepted in partial fulfillment of the requirements for the degree of:*

**Doctor of Philosophy**

*Signatures:*

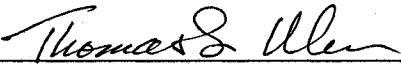


Director of Research - Thomas S. Ulen

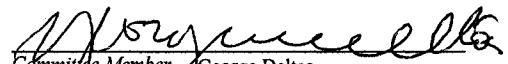


Head of Department - Steven R. Williams

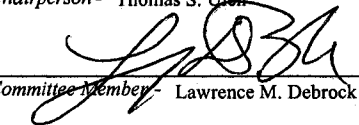
Committee on Final Examination\*



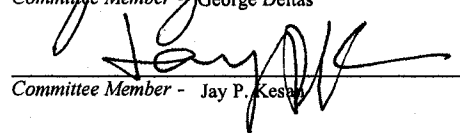
Chairperson - Thomas S. Ulen



Committee Member - George Deltas



Committee Member - Lawrence M. Debrock



Committee Member - Jay P. Kesava

Committee Member -

Committee Member -

\* Required for doctoral degree but not for master's degree

## ABSTRACT

This dissertation contains three essays on the law and economics of cybersecurity. Chapter 1 contains the introduction to the problem and the review of the different technological, economic, and law-based solutions hitherto proposed to combat the problem.

Chapter 2, which contains the first essay, puts forward the idea that cyberinsurance can be a powerful tool to align market incentives toward improving cybersecurity. We present three economic arguments for cyberinsurance as well as conduct time and case studies to trace the evolution of the cyberinsurance industry. We conclude that in theory, there are significant theoretical foundations to support the case for cyberinsurance as a market-based solution to managing Internet security risks. In practice, although some implementation issues remain, cyberinsurers were able to find ways to address what used to be major problems, such as adverse selection, moral hazard, etc.

In Chapter 3, we examine whether firms whose computer systems are under attack should be permitted to hack back, and how the law of self-defense in cyberspace should be designed. We employ a formal, game-theoretic analysis of the strategic interaction between the hacker and the attacked firm/individual. We also include, in our extended model, Bayesian updating to capture the effect of intrusion detection system technology, as well as consider the social planner's perspective and the effect of different liability regimes. We conclude that neither total prohibition nor unrestrained permission of hackback is optimal. Instead, the model results suggest that hackback should be

permitted when: (1) other alternatives, such as police enforcement and resort to courts, are either ineffective or ineffectual; (2) there is a serious prospect of hitting the hacker instead of innocent third parties; and (3) the damages to the attacked firm's (that is, the entity that is hacking back) systems that can be potentially mitigated outweigh the potential damages to third parties.

In Chapter 4, we study a model where cybercrimes are addressed through a combination of private and public measures, as well as study the public goods and externalities aspects of Internet security. We find that the socially-optimal level of security is achieved by equalizing the marginal-benefit-to-marginal-cost ratios of the different security measures. The interrelatedness of Internet risks causes firms to underinvest in private and public security goods. The government decidedly lowers the level of police expenditures to induce firms to invest in more precautions. Under certain conditions, cooperation results in socially-optimal levels of private and public security goods expenditures.

To the Lord God, the King of Ages,  
Immortal and Invisible, the Only God,  
and to the Blessed Mother

## ACKNOWLEDGMENTS

Numerous people have provided invaluable help for the completion of this dissertation and my doctoral degree; it may not be possible to name all of them here. I do hope that I do not forget the most important ones. I would like to thank Bill Yurcik and Jay Kesan for introducing me to the area (of the law and economics of Internet security), and especially the latter for providing me with guidance, co-authorship opportunities, job market recommendations, and financial support for two years. I would also like to thank several people who have read and/or given comments on the papers herein or parts thereof, such as Carl Nelson, Laudo Ogura, and some referees (including anonymous ones) in the conferences/symposia we attended. Special thanks to my committee members Tom Ulen, Jay Kesan, Larry DeBrock, and George Deltas for suggesting numerous improvements and ideas which have greatly enriched my dissertation.

On a personal note, this dissertation would not have been possible without the encouragement and support of several persons. My beloved, Marissa Manlapaz, for the understanding, encouragement and support throughout this tedious process, and my family, especially my parents, for understanding why their son has to study (and not get a real job) for so long. My greatest personal thanks go to my two spiritual directors and most of all to my adviser. Fr. Drs. Fortunatus Bijuras, Ph.D. and Barry Cole, S.T.D., like true fathers, have always been there for me, giving me invaluable sound advice through the ups and downs of the Ph.D. process; without their indispensable help, I honestly don't know how I could have finished my PhD. My greatest thanks go to my adviser, Prof. Ulen, who has always been very helpful and absolutely indispensable to my getting

finished with the Ph.D. and getting a job. Prof. Ulen is one of the best if not the best adviser a Ph.D. student could ever get at the University of Illinois; he is always very generous and magnanimous in his willingness to help throughout the process, from his willingness to be an adviser, to giving his expert senior scholar advice, to giving recommendations for the job market, and even to things like recommendation for visa matters. He is just always selflessly thinking what is for the best of the student/s. If there is any graduate student out there contemplating on getting Prof. Ulen as an adviser, my unqualified advice to you is to go for it. To everyone who has helped me, thank you very much!



## TABLE OF CONTENTS

LIST OF FIGURES.....	xi
LIST OF TABLES.....	xii
CHAPTER 1: CYBERCRIMES AND CYBER-ATTACKS: A REVIEW OF TECHNOLOGICAL, ECONOMIC, AND LAW-BASED SOLUTIONS .....	1
1. INTRODUCTION .....	1
2. TECHNOLOGY-BASED SOLUTIONS .....	5
2.1. Firewalls and Virtual Private Networks .....	6
2.2. Intrusion Detection Systems and Honeypots .....	7
2.3. Encryption Technology and Access Control Mechanisms .....	8
2.4. Vulnerability Scanners, File Integrity Checkers, and Antivirus Software.....	9
2.5. Other Technological Tools.....	11
3. ECONOMICS-BASED APPROACHES.....	11
3.1. Identifying Software Bugs Pre-Release.....	12
3.2. Finding Security Holes Post Product Release .....	12
3.2.1. <i>Market vs. Federal Funding Approach</i> .....	13
3.2.2. <i>Auction for Bug Information</i> .....	14
3.3. Disclosure Policy on Vulnerability Information.....	14
3.4. Interdependence in Cybersecurity .....	15
3.4.1. <i>Externalities in Cybersecurity</i> .....	15
3.4.2. <i>Public Goods Aspect of Cybersecurity</i> .....	16
3.5. Optimal Amount of Security Investment and Cyberinsurance.....	17
4. LAW-BASED SOLUTIONS .....	17
4.1. Criminal Law.....	17
4.2. Regulations.....	18
4.3. Other Law Based Solutions.....	22
5. SUMMARY AND CONCLUDING COMMENTS .....	22
CHAPTER 2: CYBERINSURANCE AS A MARKET-BASED SOLUTION TO THE PROBLEM OF CYBERSECURITY .....	24
1. INTRODUCTION.....	24
2. ECONOMIC ARGUMENTS FOR CYBERINSURANCE.....	25
2.1. Cyberinsurance Increases IT Safety.....	27

2.2. Cyberinsurance Facilitates Standards for Liability to be Set at Socially-Optimal Levels.....	35
2.3. Cyberinsurance Increases Social Welfare .....	41
2.3.1. <i>General Methodology for Measuring Welfare Gains from Cyberinsurance</i> .....	42
2.3.2. <i>An Example: Calculating Welfare Gains for Year 2000 DoS Attacks</i> .....	44
2.3.3. <i>Calculating Cyberinsurance Premiums</i> .....	47
3. THE DEVELOPMENT OF CYBERINSURANCE .....	48
3.1. Traditional Insurance Policies .....	48
3.2. The Advent of Early Hacker Insurance Policies .....	50
3.3. Causal Events: Increasing Risks and Legislation Compliance .....	52
3.4. More Sophisticated Cyberinsurance Policies .....	56
4. HOW CYBERINSURERS WORKED OUT ISSUES IN DEVELOPING COVERAGE .....	59
4.1. Adverse Selection.....	59
4.2. Moral Hazard.....	66
4.3. Other Implementation Issues.....	69
5. SUMMARY AND CONCLUSIONS .....	71
CHAPTER 3: HACKING BACK: OPTIMAL USE OF SELF-DEFENSE IN CYBERSPACE.....	73
1. INTRODUCTION.....	73
2. THE BASIC MODEL .....	80
2.1. The Model Set-up.....	80
2.2. Equilibrium When Police Enforcement is Effective .....	83
2.3. Equilibrium When Litigation is Not Beneficial .....	85
2.4. Equilibrium When Litigation is Beneficial .....	91
3. THE ROLE OF IDS TECHNOLOGY.....	93
4. SOCIALLY-OPTIMAL SOLUTION .....	98
4.1. The Social Planner's Problem.....	98
4.2. The Optimality of Hackback .....	102
5. PROPER LIABILITY RULE FOR DAMAGES TO INNOCENT THIRD PARTIES.....	105
6. WHAT THE LAW ON SELF-DEFENSE IN CYBERSPACE SHOULD BE.....	110
7. CONCLUSIONS.....	115

8. SUMMARY OF NOTATIONS AND PROOF OF PROPOSITIONS .....	117
CHAPTER 4: OPTIMAL MIX OF INDIVIDUAL PRECAUTIONS AND POLICE ENFORCEMENT WHEN RISKS ARE INTERRELATED: THE CASE OF CYBERCRIMES .....	
1. INTRODUCTION.....	129
2. THE MODEL.....	135
3. THE SOCIALLY-OPTIMAL SOLUTION .....	139
4. THE INDIVIDUAL SOLUTION .....	142
5. THE COOPERATIVE SOLUTION .....	148
6. EXAMPLES AND SIMULATIONS .....	152
7. CONCLUSIONS.....	162
8. GENERAL CASE: $n$ FIRMS.....	163
CHAPTER 5: SUMMARY OF CONCLUSIONS AND POSSIBLE AVENUES FOR FUTURE RESEARCH.....	
1. SUMMARY .....	168
2. POSSIBLE AVENUES FOR FUTURE RESEARCH .....	171
REFERENCES.....	174
APPENDIX A: TABLE ON THE SALIENT PROVISIONS OF CYBERINSURANCE POLICIES .....	
CURRICULUM VITAE .....	198

## LIST OF FIGURES

Figure 2-1. Expenditure on cyberinsurance and amount of coverage.....	27
Figure 2-2. Self-insurance and cyberinsurance as substitutes.....	30
Figure 2-3. Cyberinsurance, self-insurance and self-protection .....	31
Figure 2-4. Socially-optimal precaution level.....	36
Figure 2-5. Simple negligence liability rule.....	37
Figure 2-6. Measuring welfare gains.....	43
Figure 2-7. Internet incidents versus relevant laws and cyberinsurance products .....	55
Figure 2-8. Social welfare loss from adverse selection.....	61
Figure 3-1. Game tree, no IDS case .....	81
Figure 3-2. Nash equilibria when litigation is not beneficial (No IDS available) .....	86
Figure 3-3. Nash equilibria when litigation is beneficial (No IDS available).....	91
Figure 3-4. Game tree, IDS case .....	94
Figure 3-5. Nash equilibria when litigation is not beneficial (IDS available) .....	97
Figure 3-6. Nash equilibria of the social planner's problem.....	101
Figure 3-7. Hackback vs. no hackback social welfare comparisons .....	104
Figure 3-8. Nash equilibria of the firm's problem (No liability rule).....	107
Figure 3-9. Divergence of private and socially-optimal equilibria .....	108
Figure 3-10. Nash equilibria of the firm's problem (Due to frictions in enforcing liability rules, only a fraction $1-\pi$ goes to court).....	110
Figure 3-A1. Nash equilibria when litigation is beneficial (IDS available).....	125
Figure 3-A2. Nash equilibria when litigation is beneficial when the IDS signals an intrusion, but not otherwise.....	126
Figure 4-1. Elements of the model .....	131
Figure 4-2. $p(x_1, x_2, z)$ (when $x_1 = x_2 = z$ ).....	154
Figure 4-3. $p(x_1, x_2, z) \cdot L(x_1, x_2, z)$ (when $x_1 = x_2 = z$ ) .....	154
Figure 4-4. $p \cdot L + f(x_1) + y_T + g(z)$ when $x_1 = x_2 = z$ , $y_T = 1$ , $f(x_1) = 4x_1$ .....	156
Figure 4-5. Optimal private precaution: cooperative vs. individual solution.....	157
Figure 4-6. Individual firm's $y_T/x$ as a function of $f'(x)$ .....	158
Figure 4-7. Individual firm's $x$ as a function of $f'(x)$ .....	159
Figure 4-8. Individual firm's $y_T$ as a function of $f'(x)$ .....	159
Figure 4-9. Individual firm's $z$ as a function of $f'(x)$ .....	160

## LIST OF TABLES

Table 2-1. Premiums and Welfare Gains: Year 2000 DoS Attacks (in \$Mn).....	47
Table 2-2. Worldwide Cyberinsurance Premiums and Welfare Gains (in \$Bn).....	48
Table 2-3. Early Hacker Insurance Products.....	51
Table 2-4. Summary Table of Recent Cyberinsurance Policies.....	57
Table 2-5. Different AIG Cyberinsurance Products Reveal Product Differentiation Strategy.....	58
Table 2-6. Exclusions That Address the Moral Hazard Problem in Recent Cyberinsurance Policies .....	68
Table 2-7. Exclusions That Address Externalities in Recent Cyberinsurance Policies ...	70
Table 4-1. Private and Public Goods Aspects of Internet Security .....	130
Table 4-2. Summary of First-Order Conditions and Level of Security Investments (By Type of Agent and Security Investment) .....	152
Table A. Table on the Salient Provisions of Cyberinsurance Policies.....	192

## CHAPTER 1:

### CYBERCRIMES AND CYBER-ATTACKS: A REVIEW OF TECHNOLOGICAL, ECONOMIC, AND LAW-BASED SOLUTIONS

#### 1. INTRODUCTION

The Internet has radically changed the way business is carried out and is increasingly dominating our professional and personal lives (Brown 2001). Although U.S. retail sales increased a mere 5.4 percent in 2003, U.S. e-commerce sales surged 26.3 percent to \$54.9 billion (U.S. Department of Commerce 2004). Overall, global business-to-business e-commerce sales is expected to grow from \$1.93 trillion in 2002 to \$8.53 trillion in 2005 (Clark 2002).

Yet, software vulnerabilities abound. They expose Internet businesses to both risks<sup>1</sup> and liability<sup>2</sup> for property damage, business interruption, defamation, invasion of privacy, theft of credit card numbers, malpractice and consumer fraud. Thus, cybercrime and cyber-attacks on the Internet have increased in recent years. Increasingly available hacking programs (Pascuillo)<sup>3</sup> have made it easier for hackers to mount attacks (Insurance Information Institute 2003). Accordingly, hackers are responsible for:

---

<sup>1</sup> Ernst & Young reported that 34% of the 1400 organizations surveyed admit of less-than-adequate ability to identify if their intrusions in their systems, and 33% admits of lack of ability to respond (Insurance Information Institute 2003).

<sup>2</sup> Potential e-litigation may relate to product liability claims (for example, incorrect configuration or negligent design of hardware and software); computer malpractice suits associated with negligent provision of services; denial-of-service flooding attacks and other security breaches; intellectual property violation; and domain name and meta-tagging controversies (Norman 2001).

<sup>3</sup> About seventy-five percent of security incidents are carried out by unskilled hackers who use well-known exploits (Hensing 2004b).

hacking passwords and authentication codes, computer intrusions,<sup>4</sup> denial-of-service (DOS) attacks,<sup>5</sup> web defacements,<sup>6</sup> the proliferation of worms and viruses,<sup>7</sup> phishing,<sup>8</sup> identity theft (see, for example, Solove 2005), etc. Already, high profile firms such as Microsoft, Amazon.com, eBay, Yahoo, and CNN.com have suffered denial-of-service (DoS) attacks, rendering these firms unreachable for significant period of time (Gohring 2002; Vogel 2002). The CERT/CC reports that the number of cyber-incidents increased from 252 in 1990 to 137,529 in 2003 (CERT Coordination Center 2003).<sup>9</sup> In fact, a survey by the Computer Security Institute (CSI) in May 2003 revealed that 75% of the companies surveyed lost money because of computer security breaches (Insurance Information Institute 2003). Of the companies that reported security breaches, theft of proprietary data resulted in the greatest monetary losses (an average loss of \$2.7 million).<sup>10</sup> Overall, *InformationWeek* magazine estimated that computer viruses and

---

<sup>4</sup> For example, a hacker breached the U.S. Naval Academy computer system in December 1994. Another example is that of a 15-year-old Croatian hacker who intruded into the computer network of Andersen Air Force Base (Guam) in March 1997 (Washington Technology 1998).

<sup>5</sup> For instance, the websites of Microsoft, Amazon.com, eBay, Yahoo, CNN.com have been rendered unreachable over the Internet for significant periods of time because of DOS attacks (Gohring 2002; Vogel 2002).

<sup>6</sup> For example, "Sm0ked Crew" marked websites of Hewlett-Packard, Compaq, Intel and the New York Times, among others (*Information Security* 2001).

<sup>7</sup> For instance, the Love Bug virus (2000) affected 20 countries and 45 million users worldwide, and caused an estimated \$8.75 billion in foregone productivity and software damage (Insurance Information Institute 2003).

<sup>8</sup> "Phishing" means mass e-mailing aimed at duping individuals to go to fake Web sites (see, for example, Christie 2004).

<sup>9</sup> An incident may involve one, hundreds, or thousands of sites (CERT Coordination Center 2003).

<sup>10</sup> The second highest amount of monetary damage was caused by DOS attacks, with a total loss of \$65.6 million (Insurance Information Institute 2003; Fisher 2001). The FBI estimated that the average lost from network security breach in 1999 is \$142,000 (Duffy 2000). Not only intrusions but even internal attacks can be a problem, as employees can obtain credit card data or the firm's proprietary design. Employee-related security losses represent 41 percent of total losses (Duffy 2000). The Love Bug virus (2000) affected 20 countries and 45 million users caused an estimated \$8.75 billion in lost productivity and software damage (Insurance Information Institute 2003).

hacking cost an estimated \$266 billion in the United States (U.S.) and \$1.6 trillion worldwide in 1999 (McDonald 2000; Knight 2000).<sup>11</sup>

Government agencies, as well as businesses, have experienced Internet attacks. The Navy, for one, had its satellite guidance computer control compromised by a hacker who penetrated the Research Laboratory's network and downloaded software used in guiding satellites (*Information Security* 2001). Hackers have also breached the on-line security of other U.S. government agencies including: the Federal Bureau of Investigation (FBI), the Department of Defense (DOD), the Environmental Protection Agency (EPA), the National Aeronautics and Space Administration (NASA), and the U.S. Senate (Vogel 2002). Attacks such as these demonstrate the vulnerability of vital infrastructure controlled by computers.<sup>12</sup>

---

<sup>11</sup> Estimating the damages caused by security breaches is inherently hard; hence, these figures may be subject to debate. The costs associated with security incidents not only involve transitory costs such as lost business, decreased productivity, repair, hacker prosecution and media-related costs, but also long-term effects such as loss of potential new customers, reduced trust of present customers and business partners, higher insurance costs, and other intangible costs (Cavusoglu et al. 2004). In estimating the above figures, InformationWeek and Reality Research and Consulting used company downtime figures of about 50,000 firms they surveyed. They calculated that the 6,822 person-years productivity loss in North American businesses and the 3.3% unanticipated downtime in worldwide businesses translated to \$1.6 trillion in lost revenue. (The principal researcher of Reality Research and Consulting believes that these estimates may in fact be underestimated considering they only represent the impact of viruses on businesses with more than 1,000 employees.)

Aside from surveys, another method used to estimate the cost of security incidents is the event study method (see *infra* note 125 for a description of this method) which is used to measure the impact of security breaches on the firm's market capitalization (for a survey of studies conducting estimates of the cost of security incidents, see generally, Garg et al. [2003]). Cavusoglu et al. (2004) used this technique to estimate that attacked firms lost, on average, \$1.65 billion (or 2.1 percent) of their market capitalization within two days of the security breach occurrence. Other studies corroborate the huge and significant impact of Internet attacks on the stock price of firms (see, for example, Ettredge and Richardson 2002; Garg et al. 2003).

<sup>12</sup> In March 1997, services to the Federal Aviation Administration control tower at the Worcester, Massachusetts airport were paralyzed by malicious codes from a hacker (Washington Technology 1998). Other security events show that major cyber-attacks could easily be executed by someone who just has electronic capability and a broadband connection: (a) in January 1990, a programming mistake in AT&T electronic switching systems software obstructed about 5 million calls; (b) in January 1991, a fiber cut halted air traffic control operations in Boston, Washington and New York; and (c) in September 1997, erroneous uploads into a Signaling System 7 processor resulted in a 90-minute AT&T toll-free telephone service interruption (Washington Technology 1998).



Hacking has evolved from what used to be merely the pastime of mischievous individuals to what is now big business. Organized groups now hack computer systems on a large-scale basis.<sup>13</sup> Spammers send out huge mass-emailings advertising various products.<sup>14</sup> Employees of large companies have stolen sizeable amounts of money by hacking into company databases.<sup>15</sup> Even political activists have resorted to hacking in order to promote their causes.<sup>16</sup>

Another important area of concern relates to privacy issues in the Internet.<sup>17</sup> Organizations and businesses that manage personal information on the Internet have a duty of confidentiality (Meyer 2003), yet few of these organizations and businesses have security sufficient to protect personal information which includes credit card and social security numbers.<sup>18</sup> Thus, specific claims of liability may arise from: (1) tort based on privacy violations; (2) breach of an implied contractual duty; (3) violation of regulations

---

<sup>13</sup> The FBI determined that organized hacking groups (mostly in Russia and the Ukraine) have stolen more than 1 million credit card numbers from Internet locations that have not patched known vulnerabilities (Walsh 2001). Electronic Fund Transfer systems also transmit hundreds of billions of dollars on a daily basis. While bank burglaries involve \$3,000 on average, computer crimes normally cost around half a million dollars in losses (Gold 2002, p. 13, citing Ardis et al. 1985).

<sup>14</sup> It has been estimated that as of November 2003, 56% of  $5.7 \times 10^{10}$  emails sent per day were spam (Laurie and Clayton 2004, citing Radacati Group 2004). Spam has started on instant messaging (IM) ("spim"). The amount of spim quadrupled from 500 million messages in 2003 to 2 billion messages in 2004, and is projected to grow to 3 billion messages in 2005 (Paulson 2004, citing data from Ferris Research). Like spam, spimmers advertise and/or link to products such as prescription drugs and pornographic websites, often with use of bots that generate spim attacks (Paulson 2004).

<sup>15</sup> It has been reported that employee-related security losses average \$1.8 million (see Duffy 2000).

<sup>16</sup> Thus, online activists who wanted to attract attention to their anti-globalization stance had broken into databases, and intruded into private information of 27,000 important participants at the World Economic Forum in 2001, including Microsoft's Bill Gates and former U.S. Secretary of State Madeline Albright (ZDNet 2001).

<sup>17</sup> Courts recognize four types of privacy invasion: (1) intrusion upon a person's solitude or private affairs; (2) revelation of embarrassing private facts; (3) publicity that puts him/her in a false light; and (4) appropriation of his/her name or likeness (Meyer 2003, citing Loesch and Brenner 1998; Smith 1978).

<sup>18</sup> See, for example, ZDNet (2001), reporting that during the 2001 World Economic Forum, crackers who espouse the globalization cause had breached databases acquiring the participants' confidential data, including those of Microsoft Chairman Bill Gates and former U.S. Secretary of State Madeline Albright, and accessed credit card numbers for 1,400 people. See also Insurance Information Institute (2003), citing a 2002 survey by St. Paul Companies of 501 IT and risk managers at 460 U.S. companies which found that only 55 percent of the respondents said that they have reviewed existing coverages for e-risk coverage.

intended to safeguard privacy; and (4) federal legislation intended to safeguard personal data online (Meyer 2003).

Thus, it is clear that cyber-threats merit considerable concern. In this paper, we advocate using technology, economic principles, and law-based solutions simultaneously to combat cybercrime. In Section 2, we examine how organizations can use technology to protect themselves from cyber-attacks. Since software vulnerabilities have contributed a great deal to the rising incidents of cyber-attacks,<sup>19</sup> in Section 3, we investigate methods for reducing security holes in software. In Section 4, we discuss how laws and regulations can provide incentives for businesses to safeguard personal information.<sup>20</sup> In Section 5, we conclude that a combination of technological, economic, and law-based solutions are necessary to effectively combat cybercrime.

## 2. TECHNOLOGY-BASED SOLUTIONS

In the same way as locks, security cameras, and alarm bells help protect physical assets in the brick-and-mortar economy, a good information security infrastructure can help secure digital assets in the information age. In this section, we discuss technology available to protect digital resources and communication over the Internet.

---

<sup>19</sup> Security holes in software enable hackers to develop exploit codes. Note too that it is easy for hackers and script kiddies to get free vulnerability scanners, port scanning tools, rootkits, and other hacker tools. Thus, the rise of security incidents (see *supra* text accompanying note 9), is positively correlated with the rise in vulnerabilities (CERT reports that the number of vulnerabilities reported per year increased steadily from 171 in 1995 to 3,784 in 2003 [CERT Coordination Center 2003]). <http://www.sans.org/top20> lists the 20 most critical Internet security vulnerabilities (last visited 2/14/05).

<sup>20</sup> Ernst & Young reports that more than 34% of 1400 organizations it surveyed recognize that their capability to diagnose intrusions is inadequate, while 33% admit to having insufficient capacity to react to intrusions. Another survey reveals that many U.S. firms are underestimating e-risks and have not trained personnel to deal with them (Insurance Information Institute 2003).

## 2.1. Firewalls and Virtual Private Networks

Firewalls provide the first line of defense against computer intrusions (Cavusoglu, Mishra, and Raghunathan 2002). Firewalls both restrict and authorize admission into specific networks.<sup>21</sup> Simple firewalls, such as packet filters, screen incoming computer traffic using source and destination addresses,<sup>22</sup> while application-level filters allow for finer configuration (Cheswick, Bellovin, and Rubin 2003). For example, an application-level filter for e-mail can be set up to check for dirty words, identify virus-infected software, and remove unsafe attachments.<sup>23</sup> A demilitarized zone (DMZ)<sup>24</sup> can provide an additional layer of defense by preventing a hacker who bypasses the firewall from being able to access the network (Cheswick, Bellovin, and Rubin 2003).

Virtual Private Networks (VPNs) provide companies with the capability to allow their own communications to pass through firewall security. VPNs grant certain computers the permission to pass through a hole in the firewall into the network (Cheswick, Bellovin, and Rubin 2003, p. 237).<sup>25</sup> VPNs also help in environments such as universities and hotels by allowing users in the same location to connect to each other with a secure VPN connection (Schneier 2000, pp. 193-94).

---

<sup>21</sup> A common configuration is to install a two-level firewall: a first firewall protects against DOS attacks, port scans, and IP spoofing, while another (proxy) firewall protects against application-level targets (Juniper Networks 2004).

<sup>22</sup> This is called ingress filtering. The firm can also apply egress filtering to make sure that its site doesn't emit any packets with inappropriate addresses (Cheswick, Bellovin, and Rubin 2003, p. 177, citing Ferguson and Senie 2000).

<sup>23</sup> Other categories of firewalls are circuit-level gateways and dynamic packet filters (Cheswick, Bellovin and Rubin 2003).

<sup>24</sup> Named after the DMZ in Korea (Cheswick, Bellovin, and Rubin 2003).

<sup>25</sup> Technically, a VPN is a protected connection over an open network (Schneier 2000, p. 193). Since it is more costly to install a private network cable, encryption is used to secure communications transmitted over the Internet (University of Illinois at Urbana-Champaign 2006).

## 2.2. Intrusion Detection Systems and Honeypots

Firewalls, however, are not 100% effective in stopping the entry of malevolent software (“malware”) into the network (Hensing 2004).<sup>26</sup> Furthermore, firewalls are unable to prevent attacks from individuals who have access to the network (Cheswick, Bellovin, and Rubin 2003).<sup>27</sup> This is an important consideration because insiders/employees commit a significant number of cybercrimes (Cavusoglu, Mishra, and Raghunathan 2005, citing Escamilla 1998; Russell and Gangemi 1992). Intrusion detection systems (IDSs), therefore, function as an important second line of defense (Cavusoglu, Mishra, and Raghunathan 2001). By alerting network administrators of unusual or suspicious activities on the network, IDSs provide an important defense against hackers who negotiate a system’s firewall (Cavusoglu, Mishra, and Raghunathan 2001).

Two types of IDSs provide the basis for secondary network protection. First, a signature-based IDS compares suspected security breaches to a database of known attacks (Cheswick, Bellovin, and Rubin 2003).<sup>28</sup> Second, anomaly-based detection checks for abnormal behavior, that is, behavior that statistically differs from regular activities (Cavusoglu, Mishra, and Raghunathan 2001).

Honeypot IDSs work best for setting such as the DMZ. Honeypots act as a decoy by allowing the breach of a faux security system in order to deflect attacks against the real systems which house valuable assets and data. Honeypots thus make it less likely for hackers to gain access to the more valuable computer systems (Dornseif and May 2004).

---

<sup>26</sup> There can be false positives (where a valid user is precluded access) and false negatives (where an intruder is granted entry) (Cavusoglu, Mishra, and Raghunathan 2002).

<sup>27</sup> Nor are they designed to stop malicious programs running on an in-house computer (Cheswick, Bellovin, and Rubin 2003).

<sup>28</sup> Since they only recognize what is in the database, they tend to have a lot of false positives (where incidents have come about but the IDS doesn’t report them as intrusions) (Cheswick, Bellovin, and Rubin 2003).

There is also a presumption that users gaining access to honeypots are intruders. Thus, honeypots are useful for acquiring information about hacker behavior (Cheswick, Bellovin, and Rubin 2003, p. 282).<sup>29</sup>

### 2.3. Encryption Technology and Access Control Mechanisms

Encryption technology can transform a message in its original form (“plain text”) into an indecipherable form (“ciphertext”), and back into a readable form using decryption.<sup>30</sup> An example of a decryption system, the Kerberos Authentication System (*Kerberos*), authenticates individual users/computers on a network (Cheswick, Bellovin, and Rubin 2003, p. 315).<sup>31</sup> At the network level, IPsec provides encryption for the Internet (Cheswick, Bellovin and Rubin 2003, p. 318).<sup>32</sup> The common, application-level, encryption technologies are: SSH (Secure Shell), used to secure a remote login (Cheswick, Bellovin and Rubin 2003, p. 322); SSL (Secure Socket Layer), which provides cryptographic protection for transactions on the Web (Cheswick, Bellovin, and Rubin 2003, p. 77 and 323); and S/MIME<sup>33</sup> or PGP,<sup>34</sup> both used for securing e-mail communications (Cheswick, Bellovin, and Rubin 2003, p. 326).

---

<sup>29</sup> Normally, the firm would be more interested on gathering data about intrusions specifically targeting its systems (such as those done by corporate spies), rather than data on random attackers (since the latter can be gathered from more general sources) (Dornseif and May 2004).

<sup>30</sup> Modern encryption is done using cryptography, the art of secret writing (Pfleeger and Pfleeger 2003, p. 35).

<sup>31</sup> PKI (or Public Key Infrastructure) on the other hand is a device used for securely distributing public keys (Kaufman, Perlman, and Speciner 2002, p. 371). If an individual, for instance, wants to send an encrypted email message to another, she needs to securely find out the other’s public key. The PKI trust model provides some mechanism where public keys are known to others in a trustworthy fashion (Cheswick, Bellovin, and Rubin 2003, p. 150).

<sup>32</sup> It includes an encryption mechanism, an authentication mechanism, and a key management protocol (Cheswick, Bellovin, and Rubin 2003, p. 318).

<sup>33</sup> Secure Multipurpose Internet Mail Extensions.

<sup>34</sup> Pretty Good Privacy.

Access controls in the form of good password management can significantly reduce the incidence of security breaches (Cheswick, Bellovin, and Rubin 2003, p. at 106). Common types of password attacks are password hash (for example, sniffing), guessing, and dictionary attacks. A weak password policy can severely jeopardize a company's security because cyberattacks can occur so quickly that a company may not even recognize that an attack has occurred until well after it has lost valuable information. For example, a hash attack on a 1 Terabyte RainbowCrack database takes only subseconds to crack a 6-8-character password (Hensing 2004). On the other hand, it takes 1.9 years to crack an 11-character password; hence, good password practices require at least 12-character passwords and different local administrator passwords. In general, a weak password policy is one of the top security mistakes a company can make (Hensing 2004).

#### **2.4. Vulnerability Scanners, File Integrity Checkers, and Antivirus Software**

Vulnerability scanners such as Nmap ("Network Mapper") rapidly scan large networks to discover what hosts on the network are open, what applications and operating system (OS) versions are running, and what type of firewalls and other obstacles are in use (<http://www.insecure.org/nmap>).<sup>35</sup> Although Nmap is available as free open source code to hackers wishing to infiltrate a network, network administrators can benefit from using Nmap and similar tools to detect and patch security holes and apply critical updates to their systems.<sup>36</sup> Possible indications of a security breach include: slow servers, depleted

---

<sup>35</sup> Nmap also offers advanced capabilities such as remote OS detection, and stealth, parallel, and decoy scanning (*Insecure.org*). It supports most OS including Linux, Windows, FreeBSD, Solaris, Sun OS, etc. (*Insecure.org*). For more detailed information on Nmap (*see* <http://www.insecure.org>).

<sup>36</sup> For example, tools like Microsoft Baseline Security Analyzer 1.2 (MBSA) searches for unpatched holes in Windows, IE, SQL, Office, etc. and patch them (Hensing 2004b). Also, Windows Update (WU) ([www.windowsupdate.microsoft.com](http://www.windowsupdate.microsoft.com)) detects missing OS patches or updates, produces a list of needed updates, and sets up updates chosen by the customer. A similar tool is Microsoft's SUS 1.0, which gives

storage space, irregular bandwidth consumption, irregular event log data, and unexpected process crashes (Hensing 2004a).<sup>37</sup>

File integrity checking tools like Tripwire (<http://www.tripwire.com>) enable quick repairs and restoration of data damaged by successful hackers (Mangla 2004).<sup>38</sup> File integrity checkers detect unusual changes to important system components such as tree structures and files, compare the changes to a baseline digital inventory of good files, log changes, and trigger alerts to administrators (*SecurityWizardry*).<sup>39</sup>

Anti-virus (AV) protection safeguards organizations against viruses and worms that can initially infect a single computer on a network and later spread throughout the other computers on the network.<sup>40</sup> A common configuration places a first layer AV at the desktop level, with a second layer of defense a file/mail server AV. A third layer of AV defense is also available at the gateway level (Juniper Networks 2004). Computer users must regularly update AV software to most effectively protect their computers against virus attacks (Cheswick, Bellóvin, and Rubin 2003, p. 107).

---

administrators control over which patches to set up from WU (Hensing 2004b). Note, too, that Microsoft has just recently released a free Windows XP upgrade “Service Pack 2,” designed to make users more secure against attacks by closing virus entries, repelling spyware, and increasing safeguards for personal information (*CNN.com* 2004a).

<sup>37</sup> Deletion of administrator shares and unexpected installation of security patches are among the signs of a breach because hackers—in protecting their own turf from being invaded by other hackers—patch the security holes through which they enter and delete the administrator shares they control. Also, since rootkits and security patches are normally followed by reboots, unexpected reboots can also be signs that the system might have been breached (Hensing 2004a).

<sup>38</sup> They create a message fingerprint/digest of important files, and regularly check these files to ensure that the hash hasn’t been altered (Mangla 2004).

<sup>39</sup> Tripwire for Linux is free, while versions for Windows and Solaris are available at [www.tripwire.com](http://www.tripwire.com) (Mangla 2004).

<sup>40</sup> Companies can also install anti-spyware programs to help protect against pop-ups ads programs which gather information about computer users (see Christie 2004a). However, administrators should exercise care in using anti-spyware programs since a lot of fake spyware programs have appeared, and some even install spywares themselves (see Dolinar 2004); [http://www.spywarewarrior.com/rogue\\_anti-spyware.htm](http://www.spywarewarrior.com/rogue_anti-spyware.htm) lists fake and suspect spyware programs.

## 2.5. Other Technological Tools

Several other technology-based tools are available for use against cyber-attacks.

Visualization tools such as NVisionIP and VisFlowConnect<sup>41</sup> provide security administrators with situational knowledge of complex computer networks and identify intrusion patterns by allowing security administrators to visualize the devices, traffic, and relationship between the devices in the network (Paulson 2004a). Another tool, ICAT, is a search engine for vulnerabilities and available patches maintained by the National Institute for Standards and Technology (NIST).<sup>42</sup> *Hashcash* proposes charging spammers a fee for every sent message<sup>43</sup> and can also be useful to check other abuses of un-metered Internet resources such as distributed denial-of-service (DDOS) attacks (Laurie and Clayton 2004, citing Mankins et al. 2001).

## 3. ECONOMICS-BASED APPROACHES

In the previous section, we discussed the technology available to prevent cyber-attacks. In this section, we argue that improving software is an important means of preventing cybercrimes. Because faulty software, in and of itself, is costly even if not used to commit cybercrimes,<sup>44</sup> in this section, we discuss an economic analysis of the software vulnerability problem.

---

<sup>41</sup> Both developed by the National Center for Supercomputing Applications (NCSA).

<sup>42</sup> It indexes data from CERT, ISS X-Force, Security Focus, NT Bugtraq, Bugtraq, and other security and patch bulletins (see <http://www.icat.nist.gov>).

<sup>43</sup> The idea is to have the sender solve a cryptographic puzzle and do complex computational work (Laurie and Clayton 2004). The sender computes a CPU cost function (easy enough to verify but costly to calculate) and thus pays “tokens” in terms of burnt CPU cycles (Back; Back 2002). For those legitimate emails that are part of a mailing list, subscribers can put the mailing list address in a postage-free recipients list (Back).

<sup>44</sup> For example, in 1998, buggy software disrupted telephone communication in a couple of cities in the East Coast as well as the New York Mercantile Exchange (Washington Technology 1998). Also, NIST



### **3.1. Identifying Software Bugs Pre-Release**

Among the first steps available to address software quality is finding software problems during pre-release of the software. Problems identified early in the development process are less expensive to fix than later in the development process (National Institute of Standards and Technology 2002, citing Kit 1995). Nevertheless, because software has become increasingly complex,<sup>45</sup> the cost of debugging, testing, and verifying software typically ranges from 50%-75% of the total software development cost. In answering rising software costs, NIST has proposed developing software testing tools that identify problems more quickly (National Institute of Standards and Technology 2002).

According to the NIST, enhanced testing tools will: reduce software development and testing costs; reduce the time needed to introduce new software; and improve software quality. Overall, NIST estimates that improved testing tools could result in software developers saving \$10.6 billion and software users saving \$11.7 billion (National Institute of Standards and Technology 2002).<sup>46</sup>

### **3.2. Finding Security Holes Post Product Release**

Despite the dedicated efforts of software developers to identify problems during pre-release, not all problems are found (National Institute of Standards and Technology 2002, p. 4-2, citing Myers 1979). Software developers release patches to correct problems

---

estimated that the yearly costs of faulty software (in terms of testing resources by software developers and loss prevention activities by software users) was somewhere between \$22.2 to \$59.5 billion (see National Institute of Standards and Technology 2002, p. ES-3). Moreover, the Gartner Group reports a 25% failure rate for notebook computers used in large U.S. companies (National Institute of Standards and Technology 2002, p. 1-2, citing Barron 2000).

<sup>45</sup> Software size now span not only thousands of lines of codes, but millions of lines of code (National Institute of Standards and Technology 2002, p. ES-1).

<sup>46</sup> The cost savings to software users relates to error mitigation and avoidance (National Institute of Standards and Technology 2002).

identified after a program's general release. Accordingly, software developers perform an economic analysis of whether it is more profitable to release a product with problems or delay the product's release until all of its problems are corrected (Arora, Caulkins, and Telang 2003).<sup>47</sup> Moreover, a firm with the ability to fix defects after general release will have incentives to release a product with more problems (thereby allowing the product to maximize its market share) but invest more in after-sales patching support (Arora, Caulkins, and Telang 2003).<sup>48</sup>

### ***3.2.1. Market vs. Federal Funding Approach***

Software designers are undecided as to how best to find vulnerabilities in software released to the general public.<sup>49</sup> Currently, reporting bugs to intermediaries like the CERT is voluntary and does not come with financial rewards (Kannan, Telang, and Xu 2003).<sup>50</sup> Some people have suggested developing a market, similar to those used to trade other commodities, thereby creating incentives for software users to find and report software problems. Others have cautioned that such a move towards an unregulated market-based mechanism may not necessarily lead to a better social outcome because people looking to exploit security weaknesses in the software might exploit the

---

<sup>47</sup> Vendors deal with a trade-off between the benefits and disadvantages of releasing the product early. On the one hand, software that is released earlier can be used by customers sooner; on the other hand, early release may entail that the software has more bugs and that the software firm needs to invest more in after-sales patching support. Right now, many popular software manufacturers regularly release patches: "Sun released more than 200 patches for Solaris 9.0, . . . Microsoft issues patches on an almost daily basis, and Hewlett Packard puts out an average of 60 to 80 HP-UX patches per week." (Arora, Caulkins, and Telang 2003)

<sup>48</sup> As software developers invest more in patching, they tend to release buggier product earlier. Also, it is socially-optimal to release the software sooner and provide broad patching support (Arora, Caulkins, and Telang 2003).

<sup>49</sup> However, some question whether vulnerability finding is a useful activity, arguing that the data do not show any significant measurable effect on the software defect rate (see Rescorla 2004).

<sup>50</sup> When a person comes across a bug, he or she can report such information to an institution like the CERT, which in turn informs the vendor of such problem and gives the vendor sufficient time to create a patch before it discloses the information to the public (Kannan, Telang, and Xu 2003).

vulnerability information.<sup>51</sup> The best mechanism may be a federally-funded CERT-type of institution. This type of institution would reward people who identified vulnerabilities but would not charge a subscription fee to those to whom it released such vulnerability and patching information (Kannan, Telang, and Xu 2003).

### **3.2.2. Auction for Bug Information**

Another possible method for identifying software problems after a product's release is for companies to buy information from product users who find problems with the software. Buying this type of information could take the place of pre/post-release product testing and at the same time assist software vendors in determining the security of their product (Schechter 2002).<sup>52</sup> Auction markets could be used for these purposes (Ozment 2004).

### **3.3. Disclosure Policy on Vulnerability Information**

Conflicting opinions exist as to whether to publicly disclose known software problems. On the one hand, publicly announcing security holes enables hackers to exploit them.<sup>53</sup> On the other hand, publicly announcing security holes creates an incentive for software manufacturers to generate the patches necessary to protect the public against the security holes. Hence, the policy planner must essentially balance the competing interests of

---

<sup>51</sup> Also, the market-based intermediary may have incentive to protect its own subscribers (such as delivering a patch or providing filters to its subscribers) but "leak" the information without adequate safeguards, thereby rendering non-subscribers susceptible to attacks. The non-subscribers then will have incentives to subscribe to its service in order to be protected. In this case, some form of regulation preventing the intermediary from leaking the vulnerability information might be necessary (Kannan, Telang, and Xu 2003).

<sup>52</sup> An initial amount could be set as a reward for finding a product defect and this reward grows over time until it is claimed. The amount, when unclaimed, is the lower limit of the cost to break the product, which is a measure of the product's security (Schechter 2002).

<sup>53</sup> Symantec reports that in 2001 and 2002, around 70% of all vulnerabilities in 2003 are easily exploitable either because they require no exploit code or the exploit code is publicly available (see Symantec Internet Security Threat Report 2004). Also, even if a patch is available, not all customers patch immediately (Arora et al. [2004], citing an InternetNews.com report that 6 months after the DOS attacks in 2000, more than 100,000 machines were still unpatched).

exposing consumers to attacks against reducing the time for vendors to develop and release patches.<sup>54</sup> Neither secrecy nor instant disclosure is optimal. Rather, the optimal timing of the disclosure depends upon the effect of the disclosure on the number of attacks, the mitigation of damages to customers apprised of such holes, and the effect of disclosure on vendor behavior (Arora et al. 2004).<sup>55</sup>

Two opposing factors strongly influence the development of secure software. The first factor is that known security holes are more likely to be the subject of an attack than those left undisclosed.<sup>56</sup> Also, releasing a patch for previously unknown holes increases the number of attacks (Arora, Telang, and Xu 2004). The second factor is that patching a known security hole lowers the frequency of attacks (Arora et al. 2004), and early disclosure pushes software producers to patch earlier (Arora et al. 2004; Arora, Telang, and Xu 2004). An additional consideration is that early disclosure balances the desire of the software vendors to delay releasing patches in software for which they share no liability (Arora, Telang, and Xu 2004). An appropriate disclosure policy would take into consideration each and every one of these factors.

### **3.4. Interdependence in Cybersecurity**

#### **3.4.1. Externalities in Cybersecurity**

Inaction by individuals and firms that are the victims of computer intrusion contributes to the frequency of future intrusions. For example, if a computer virus penetrates the

---

<sup>54</sup> While instant disclosure incentivizes vendors to respond more quickly, keeping the vulnerability information secret may result in fewer attacks (Arora et al. 2004).

<sup>55</sup> Open source and larger firms tend on average to have better patch response. Also, software vendors tend to patch critical security holes sooner (Arora et al. 2004).

<sup>56</sup> Note, however, that although disclosure increases the number of attacks, the total amount of the damages from those attacks could actually be lower if disclosure enables the users to mitigate their losses (Arora et al. 2004).

system through an unprotected machine, it has comparatively easier access to the remaining computers in the system, as in fact a lot of viruses reproduce themselves to all addresses listed in the address book of the compromised computer. In essence, the lack of security in one computer or network can cause damage not only to that single machine or network, but also to all of the computers affected by the network (Heal and Kunreuther 2003).<sup>57</sup> Hackers can also use compromised computers to launch attacks against other computers (Varian 2000), as in the case of DDOS attacks. The issue of how to deal with externalities in computer security is an important one that has arisen recently.<sup>58</sup> Suggested solutions for this problem include both creating Coasian markets for vulnerability credits (see Camp and Wolfram 2000) and imposing liabilities that function as a sort of a Pigouvian tax.<sup>59</sup>

#### **3.4.2. Public Goods Aspect of Cybersecurity**

Protecting system reliability requires cooperative action (see Varian 2002). As such, system reliability is subject to both free-riders and under-providers. Much in the same manner that citizens may build a wall to protect their city, system reliability depends on: the sum of the efforts of the individuals; the minimum effort; or the maximum effort. Fines can influence sub-optimal outcomes resulting from free-riders (Varian 2002). Similarly, collective organizations (such as Information Sharing and Assessment Centers [ISACs]) may help solve the underprovision problem (Kobayashi 2005).

---

<sup>57</sup> This often results in inefficient outcomes since the costs imposed on others are not internalized: the return of the security investment to society is bigger than the private return that the individual or firm takes into account (Heal and Kunreuther 2003).

<sup>58</sup> However, hitherto, we are not aware of any formal study that actually fleshes out a workable solution to these issues, although informal suggestions have been brought forth.

<sup>59</sup> The imposition of liability, say against software vendors, works as a "liability tax" (see our discussions on tort-based liability rules, *infra* at Section 4.2).

### **3.5. Optimal Amount and Mix of Security Measures**

Investment in security diverts societal resources from other uses. Accordingly, the research agenda of this dissertation is to achieve a balance between the gain from additional investment in security equals the cost of extra security, as well as to identify the optimal mix between the different security measures. Thus, in Chapter 2, we explore using cyberinsurance with liability rules to achieve an optimal level of security in society (see, for example, Kesan, Majuca, and Yurcik 2005). In Chapter 3, we study the optimal combination between public approaches to security as well as private measures such as self-help and using technology like IDS and traceroute. In Chapter 4, we study the externalities and public goods aspects of Internet security and model the optimal combination of private and non-rivalrous security investment as well as police enforcement expenditures. Chapter 5 concludes with a summary of our discussions and some directions for future research.

## **4. LAW-BASED SOLUTIONS**

### **4.1. Criminal Law**

Criminal penalties are another useful tool for preventing computer hacking. The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 (18 U.S.C. § 1030)<sup>60</sup> protects computers at the federal level.<sup>61</sup> In the United States, criminal law has

---

<sup>60</sup> Although originally designed to curb the proliferation of computer-related crimes in the financial sector, the law was expanded in 1985 to cover crimes outside financial settings, and further amended in 1986, 1994, and 1996. See generally Adequacy of Criminal Law and Procedure (Cyber): A Legal Foundations Study (Report 7 of 12 to the President's Commission on Critical Infrastructure Protection) (1997) [hereinafter Legal Foundations Study] for legislative history of 18 U.S.C. § 1030. The National Information Infrastructure Protection Act, the USA Patriot Act of 2001, and Section 225 ("The Cyber Security Enhancement Act") of the Homeland Security Act of 2002, H.R. 5710 further strengthened the

generally stayed current with increasing technology.<sup>62</sup> At the state level, Florida, Arizona, and Virginia were the first states to pass legislation (in 1978) addressing computer crimes; California, Illinois, Michigan, New Mexico, North Carolina, Rhode Island, and Utah passed legislation in 1979 (Legal Foundations Study 1997, p. 5). By 1999, all states had computer crime laws.<sup>63</sup>

Aside from using criminal law to prosecute hackers, legislators could also consider using criminal law against corporate entities that compromise confidential data. Some experts even suggest treating confidential data as property that deserves property rights protection.<sup>64</sup> Additionally, these same experts suggest instituting criminal as well as civil penalties on people who violate data privacy (see Brenner 2004).<sup>65</sup>

## 4.2. Regulations

Legislation must necessarily influence the behavior of businesses that hold personal information. This is because large amounts of personal information are stored in readily accessible company databases and network servers (Peek 2004). Because company databases and network servers are readily accessible and easily shared, personal data is susceptible to leaks, intrusions, and identity theft (Solove 2004). In an attempt to correct

---

law. The text of the law, as amended, is available at [http://www.usdoj.gov/criminal/cybercrime/1030\\_new.html](http://www.usdoj.gov/criminal/cybercrime/1030_new.html). For a sample of cases prosecuted under the Act, see <http://www.usdoj.gov/criminal/cybercrime/cccases.html>.

<sup>61</sup> Before the 1980s, there was no federal law specifically designed to cover computer crimes, thus prosecution of computer crimes has to rely on other statutes such as mail fraud (18 U.S.C. § 1341) and wire fraud (18 U.S.C. § 1343) (Legal Foundations Study, p. 6).

<sup>62</sup> Federal and state legislation now cover a wide array of computer crimes, including intrusions and proliferation of malewares (Legal Foundations Study, p. 2.)

<sup>63</sup> For a compilation of U.S. state computer crime law and regulations, see Baker & McKenzie.

<sup>64</sup> Personal information has value both to firms who seek these data for their profit-making objectives and to individuals whose personal information can be mis-used (Brenner 2004).

<sup>65</sup> One possibility toward this end is the use of "public welfare"-offense type of legislation to protect the data confidentiality, similar to the ones used to hold corporate officers strictly and vicariously criminally liable for failure to protect the integrity of food they sold (see Brenner 2004).

this inadequacy, in 1999, President Clinton signed the Gramm-Leach-Bliley (GLB) Act.<sup>66</sup> Section 501<sup>67</sup> of the Act requires certain government agencies to adopt appropriate standards for the financial institutions subject to their control. The GLB Act's security regulations,<sup>68</sup> passed in 2001, require financial institutions to: assess risks; manage and control risks; oversee service provider arrangements; monitor and adjust their information security programs to reflect the changing nature of threats, the available technology, and the financial institutions' changing business requirements; and involve the board of directors in the approval and oversight of the development and implementation of the information security program (GLB Security Regulations, 12 C.F.R. Part 30, Appendix B, Part III).

The HIPAA Security Regulations, issued in 2003, required health plans, health care clearinghouses, and health care providers to basically adopt the same safeguards as those required of financial institutions.<sup>69</sup> Thus, there are currently, specific security regulations governing the financial and health care sectors (Smedinghoff 2004).<sup>70</sup> *National Strategy*

---

<sup>66</sup> Pub. L. 106-102.

<sup>67</sup> Protection of Nonpublic Personal Information.

<sup>68</sup> Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness, 12 C.F.R. Part 30 (Office of Comptroller of the Currency), 12 C.F.R. Parts 208, 211, 225 & 263 (Federal Reserve System), 12 C.F.R. Parts 308 & 364 (Federal Deposit Insurance Corporation), and 12 C.F.R. Parts 568 & 570 (Office of Thrift Supervision), *available at* <http://federalreserve.gov/boarddocs/press/boardacts/2001/20010117/attachment.pdf> [hereinafter GLB Security Regulations].

<sup>69</sup> Specifically it requires covered entities to: "(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits. (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information. (3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required . . . (4) Ensure compliance . . . by its workforce." 45 C.F.R. Parts 160, 162, and 164, *available at* <http://www.cms.gov/regulations/hipaa/cms0003-5/0049f-econ-ofr-2-12-03.pdf> [hereinafter HIPAA FINAL REGULATIONS], §164.306.

<sup>70</sup> Some businesses not covered by the regulations have nonetheless been covered by consent decrees (Smedinghoff 2004 citing *FTC v. Microsoft*, Consent Decree (FTC, August 7, 2002), *available at* <http://www.ftc.gov/os/2002/08/microsoftagree.pdf>; In the Matter of Ziff Davis Media, Inc., Assurance of Discontinuance, *available at* [http://www.oag.state.ny.us/press/2002/aug/aug28a\\_02\\_attach.pdf](http://www.oag.state.ny.us/press/2002/aug/aug28a_02_attach.pdf); In the Matter of Eli Lilly & Co., Decision and Order (FTC, May 8, 2002), *available at* <http://www.ftc.gov/os/2002/05/elilillydo.htm>).



to *Secure Cyberspace*<sup>71</sup> suggests that the other, unregulated, sectors may have a general duty to protect the information under their control.<sup>72</sup>

Liability rules may be useful for fixing problems caused by poor security (Schneier 2002; Varian 2000). Accordingly, some people suggest making software vendors who release insecure codes accountable for damages arising from vulnerabilities in their software (Schneier 2002).<sup>73</sup> Alternately, because ISPs<sup>74</sup> are best able to control their users' activities, some critics believe that the doctrine of vicarious liability<sup>75</sup> dictates that ISPs should be accountable for their users' malicious activity (see Lichtman and Posner 2004).<sup>76</sup>

Economic theory suggests that in setting up liability regulations, society should strike a balance between the gains and the costs associated with specific liability rules.<sup>77</sup>

---

<sup>71</sup> Available at [www.whitehouse.gov/pcipb](http://www.whitehouse.gov/pcipb) [hereinafter National Strategy].

<sup>72</sup> Smedinghoff 2004, citing National Strategy: "All users of cyberspace have some responsibility, not just for their own security, but also for the overall security and health of cyberspace". Also, several commentators believe that there exists a common law duty to protect information under one's custody (Smedinghoff 2004, citing Radin 2001; Kiefer and Sabett 2002; Raul, Volpe, and Meyer 2001; Kenneally 2000). If such a duty exists, its scope is not cut and dried, since laws and regulations on the matter focus more on process, rather than product, and emphasize more what has to be done rather than how it ought to be implemented (Smedinghoff 2004).

<sup>73</sup> See also Chandler (2005): In the case of a DDOS attack the victim could be a good plaintiff, since he or she is not subject to claims of contributory negligence, unlike a consumer who fails to patch his or her system.

<sup>74</sup> Others have also introduced the idea of holding the network administrators liable (see Varian 2000).

<sup>75</sup> Under the principle of indirect liability, a party capable of stopping the act or reducing the damage, can be made liable for acts done by another, if it will be inutile to apply the accountability to the person directly liable (Lichtman and Posner 2004).

<sup>76</sup> Under current U.S. laws, § 230 of the Communication Decency Act (CDA) (47 U.S.C. § 230) shields ISPs from libel claims resulting from defamatory materials posted by subscribers. Also, the Digital Millennium Copyright Act (DMCA) (17 U.S.C. §512(c)) (2003) frees ISPs from liability associated with hosting any form of material which infringes some copyright. Thus, in *Zeran v. America Online (AOL), Inc.*, 129 F.3d 327 (4th Cir. 1997), the court held that AOL is not liable for defamatory messages posted by an unidentified third party. But see *Stratton Oakmont, Inc. v. Prodigy Serv. Co.*, N.Y. Sup. Ct. May 24, 1995).

<sup>77</sup> Another rule in the economics of liability is to assign liability to the party most capable of dealing with the risk (Varian 2000). In general, if the potential victim (but not the injurer) can take precautions, then a "no liability" regime is optimal. If, on the other hand, the injurer (but not the victim) can take precautions, strict liability with perfect compensation results in efficient precautions, by causing the injurer to internalize the marginal costs and benefits of precautions. However, when both the injurer and the victim

Although liability regulations can be used to deter harm and internalize the damages caused by injurers, liability rules also impose “taxes” on suppliers, thereby discouraging the suppliers from innovation (Shapiro 1991).<sup>78</sup> Accordingly, liability should be broad enough to create incentives for precaution, but not so broad as to create disincentives for innovation (Shapiro 1991).<sup>79</sup> The international community has a shared responsibility to secure the Internet against cybercrimes/cybertorts (Crane 2001),<sup>80</sup> because a secure Internet has global benefits.<sup>81</sup> Unfortunately, along with the Internet’s benefits have come disputes over which countries have jurisdiction to resolve Internet-based conflicts (Gold 2002, pp. 9-10). Such conflicts have the potential to bring various legal systems and traditions into play (Legal Foundations Study 1997, p. 9).<sup>82</sup> In the recent years, several multinational organizations have cooperated to increase the harmonization of the substantive and procedural aspects of cybercrime law (see, for example, Organisation for Economic Co-operation and Development 1992a; Organisation for Economic Co-operation and Development 1992b). Nevertheless, more effort is needed in both inter-

---

can take precautions, a negligence rule in which the legal standard is equal to the efficient level of care results in efficient precautions (Cooter and Ulen 2004).

<sup>78</sup> Due to high liability costs, some products or services have simply vanished (Viscusi 1991).

<sup>79</sup> Note also that in the case of software, the stakes are particularly high—the software market was valued at around \$180 billion in 2000 and the industry employs almost 700,000 software engineers and 600,000 programmers (NIST Report 2002).

<sup>80</sup> The hacker could conduct the attack in a place other than his/her home country, and can be hard to track down considering that digital assets can be moved, copied, and the information can be stored in several locations. Moreover, the damages from a virus created in the country can reach many countries, and hackers and their attack tools can be situated in many countries.

<sup>81</sup> To some extent, cybersecurity may be viewed as “global public good”. International cooperation among nations needs to take into account the costs and benefits to the states of the collective effort, since if countries free-ride, this would result in the underprovision of Internet security (Trachtman 2004).

<sup>82</sup> For instance, in the area of tort law, if the tortious information is available to Internet users worldwide, individuals may bring suits in foreign jurisdictions (Gold 2002, p. 3). Also, different jurisdictions can have different standards, for example, the EU Data Protection Directive has restrictions on what non-EU countries can do with information gathered from e-transactions. So too, in the area of criminal law, mutual legal assistance treaties (MLATs) normally require that the act must also be a criminal offense in the locality where the perpetrator is located. Hence, countries have an interest in seeing that other countries also have adequate computer crime laws (Legal Foundations Study 1997).

jurisdictional investigations and the international apprehension and prosecution of cyber-criminals (Legal Foundations Study 1997).<sup>83</sup>

### **4.3. Other Law Based Solutions**

Another solution for protecting the integrity of personal data on the Internet consists of developing a market for controlling personal information rights, and thus allowing for contracting out the control of personal information. Accordingly, contract law provides the rules for managing the control of personal information (Nimmer 2005). However, because personal information is in many cases acquired and shared by disinterested third parties, privity of contract may be unnecessary to establish liability (Peek 2005). Instead, a quasi-contract (Peek 2005) or fiduciary trust (Edwards 2005) may be more appropriate in such situations.

## **5. SUMMARY AND CONCLUDING COMMENTS**

Cybercrimes and cyber-attacks can have a tremendously negative impact on an information-based economy. Clearly, technology alone cannot prevent cybercrime. Similarly, most cybercrimes are not preventable using only cooperation among intergovernmental law enforcement agencies.

We suggest that a holistic approach, incorporating economic incentives with a combination of technology and legal initiatives, would best prevent cybercrime.

Intrusions into IT systems causing damage to companies' digital resources are preventable with good technology management. Similarly, assuming that everything else

---

<sup>83</sup> Among the important items on which countries can work together include improvement the ability to rapidly track down cyber-criminals, as well as procedures relating to extradition, prosecution, and dual criminality requirements (Legal Foundations Study 1997, p. 10).

remains constant, there will be fewer cyber-intrusions if there are fewer vulnerabilities to exploit. Attacks, therefore, are preventable if computer programmers and network administrators address defects in software and vulnerabilities in the Internet.

Additionally, incentives for data custodians can go a long way towards protecting personal information.

In summary, we conclude that in order to effectively address the growing problem of cybercrime, we must focus on the technological, economic, and the legal fronts simultaneously.

## **CHAPTER 2:**

### **CYBERINSURANCE AS A MARKET-BASED SOLUTION TO THE PROBLEM OF CYBERSECURITY**

#### **1. INTRODUCTION**

In the previous chapter, we reviewed several proposed solutions to Internet security and privacy problems from the technological, economic, and legal perspectives. In this chapter, we look in depth into a particular market-based solution for improving Internet security. Specifically, we examine using cyberinsurance as part of the overall solution to Internet security.

As organizations become more dependent on their networked computer assets, the more vulnerable they become to harm from increasing frequent and damaging attacks enabled by connectivity. Protection from harm on any networked computer system will never be 100%. In the past decade, protection techniques from a variety of computer science fields such as cryptography and software engineering have continually made improvements and yet Internet attacks continue to increase (CERT/CC 2005). While some/most Internet security vendors are selling solutions in the form of hardware and software, Internet security protection is a continual process involving people that cannot be solved entirely with products (Schneier 2000). Most relevantly, while most organizations have focused on preventing cyberattacks solely by technical means, this is only part of an overall solution. An overall solution must include accepting and managing the risk from cyberattacks since their occurrence is a reality.

In Section 2, we propose three economic arguments for cyberinsurance, that is, that cyberinsurance: (a) results in higher level of IT security investment; (b) facilitates standards for best practices; and (c) results in increased social welfare. In Section 3, we suggest that traditional insurance policies do not adequately address the new perils of the information economy, and discuss the evolution of cyberinsurance practice, from traditional insurance policies that were inadequate to early hacker insurance policies that developed into more comprehensive cyberinsurance policies. Specifically, we look at the development of cyberinsurance over time since when it was first introduced in the late 1990s through 2005. In Section 4, we discuss how cyberinsurers dealt with issues such as adverse selection, moral hazard, interdependent risks, and other obstacles to the development of the cyberinsurance industry, including discussion of the mechanisms cyberinsurers are adopting to solve these problems. Finally, in Section 5, we conclude our discussions.

## **2. ECONOMIC ARGUMENTS FOR CYBERINSURANCE**

In this section, we present three primary economic arguments for cyberinsurance. First, cyberinsurance increases IT safety. Second, cyberinsurance best facilitates standards for setting practices at socially optimal levels. Lastly, cyberinsurance solves a market failure and thereby increases societal welfare.

Suppose that the firm has an income in good state ( $I_1^e$ ) and there is a probability  $p$  that it will lose  $L^e = I_1^e - I_0^e$  (where  $I_0^e$  is the income in bad state) in the event of a cyber-attack. E-commerce losses may be: (1) direct losses from the attack or intrusion; (2) business interruption (loss of productive time) and reputation losses; or (3) third party liability (suits for damages associated with privacy, defamation, etc.). All of these potential

losses are risks for which the firm would like coverage. The insurer will pay the firm  $s$  in the event that a cyber-loss occurs and the price of insurance is  $\gamma$  per dollar of cover.

Thus, in the good state (occurring with probability  $1-p$ ), the firm has utility,  $U(I_1^e - \gamma s)$ , associated with its income in the good state minus the expenditure on insurance. In the bad state (which occurs with probability  $p$ ), the firm has utility associated with its income in the good state minus the loss and the expenditure for insurance plus the amount the insurer will pay the insured in the event of a loss:  $U(I_1^e - L^e - \gamma s + s)$ . The firm chooses the insurance coverage,  $s$ , such that its expected utility from both the good and bad states is maximized. That is, the firm chooses  $s$  to:

$$\text{Max } EU = pU(I_1^e - L^e - \gamma s + s) + (1-p)U(I_1^e - \gamma s). \quad (2-1)$$

As illustrated in Figure 2-1, by purchasing insurance coverage of amount  $s$ , a firm moves from E to F. A firm spends  $\gamma s$  on insurance premiums so that in the event a loss occurs, the insurer will pay out  $s$ . The firm gains from purchasing cyberinsurance because the firm moves from point E to point F, thereby moving to a higher indifference curve. The first-order (optimality) condition equates the slope of the indifference curves and the “budget lines”:

$$\frac{p}{1-p} \frac{U'(I_1^e - L^e + [1-\gamma]s)}{U'(I_1^e - \gamma s)} = \frac{\gamma}{1-\gamma}. \quad (2-2)$$

$\gamma = p \Rightarrow U'(I_1^e - L^e + [1-\gamma]s) = U'(I_1^e - \gamma s) \Rightarrow L^e = s$ , that is, the firm will fully insure if the insurance company charges an actuarially fair premium. Hence, the firm moves from point E (no insurance) to either point F (full insurance) if  $\gamma = p$  (premiums are actuarially fair), or point P (partial insurance) if  $\gamma > p$  (insurance prices are higher).

## 2.1. Cyberinsurance Increases IT Safety

Firms use different methods to protect themselves against damages. These methods include outsourced insurance (cyberinsurance), self-insurance, and self-

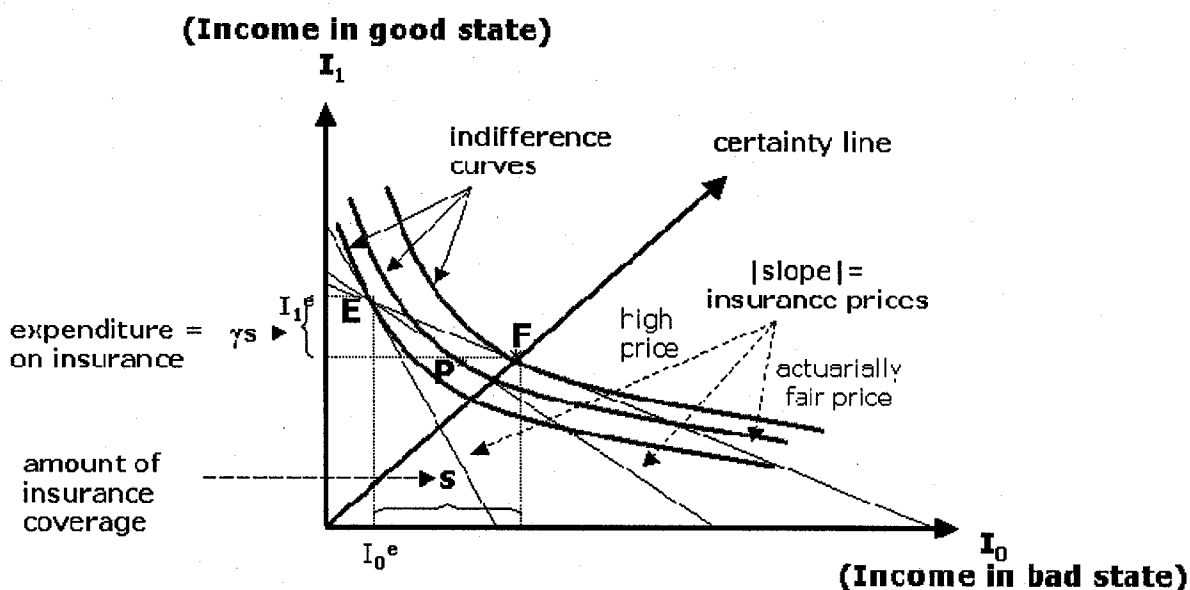


Figure 2-1. Expenditure on cyberinsurance and amount of coverage

protection. Both self-insurance and cyberinsurance protect firms against loss or redistribution of income from “good state” to “bad state”, that is, they are both designed to reduce the *size* of the loss. Cyberinsurance differs from self-insurance in that a firm purchases cyberinsurance from a third party while self-insurance is an internal investment reserved for use only in the event of a loss.

In contrast to both cyberinsurance and self-insurance, self-protection attempts to reduce the probability of losses occurring in the first place. Self-protection, also called loss prevention, is analogous to a burglar alarm that reduces the probability of someone breaking into a house. In cybersecurity, self-protection may manifest in any of the



following forms: authentication processes; anti-virus software; firewalls; virtual private networks; intrusion detection systems; vulnerability scans; and official security policies explicitly stating unacceptable behaviors.

Self-insurance, also called loss protection, is analogous to a sprinkler system that minimizes damage to a burning house. In cybersecurity, self-insurance may manifest in any of the following forms: IT staffs who restore data and normal functions; software backup strategies; disaster recovery planning; and any investment or purchase of equipments or services that reduce the potential loss.

Our intention is to show that: (1) cyberinsurance and self-protection are “complements” (cyberinsurance increases self-protection);<sup>84</sup> (2) cyberinsurance and self-insurance are “substitutes” (an increase in expenditures on one would decrease the amount spent on the other); and (3) self-insurance decreases self-protection (the “moral hazard problem”).<sup>85</sup> An implication of our analysis is that cyberinsurance does not lead to less self-protection, that is, that it does not create a moral hazard.

Cyberinsurance results in higher investment in security, increasing the level of safety for IT infrastructure. Accordingly, new insurance products may make the Internet a safer business environment because cyberinsurers can require businesses to minimize losses

---

<sup>84</sup> Self-protection is encouraged if the price of insurance is negatively related to the amount of self-protection. Overall, the optimal amount of self-protection is likely to be larger with cyberinsurance than without cyberinsurance if  $p$  is not very small (Ehrlich and Becker 1972).

<sup>85</sup> The term “moral hazard”, also known as the *hidden action* or *principal-agent* problem in economics concerns actions of a party that may be unobserved by the other parties which could result in negligence by the former. See Meyer 2003: “[T]he companies may be lax in their security efforts. It may be more cost effective for companies to purchase insurance to cover the risk of security breaches than to continuously improve their computer systems to keep up with the increasing sophistication of [hackers].” However, this may be prevented by cyberinsurers tying the firm’s premium to their level of self-protection.

using economic incentives (Beh 2002).<sup>86</sup> Cyberinsurers are able to base a firm's insurance premium on the insured firm's investment in security processes, thereby creating market-based incentives for e-businesses to increase information security.<sup>87</sup>

In contrast to the moral hazard argument that insurance will result in a reduction of self-protection, investment in IT security occurs at a higher rate in firms that have cyberinsurance than in those firms that don't have cyberinsurance (see Ehrlich and Becker 1972).<sup>88</sup> Because cyberinsurance and loss prevention activities are complements,<sup>89</sup> insurers can insist that software companies deliver safe products and exert pressure on software engineering firms to improve in order to decrease exposure to various claims. In addition, insurance companies have an incentive to monitor hackers in order to minimize the amount of damage the companies would have to pay out to its insured firms. In summary, private enforcement by insurance companies would supplement enforcement efforts of both firms and law enforcement.

As shown in Figure 2-2, a firm has a choice between self-insurance (associated with the bowed-out transformation curve) and cyberinsurance (associated with the straight lines representing the insurance prices). The transformation curve is bowed-out because the "law of diminishing marginal returns" applies to investment in self-insurance

---

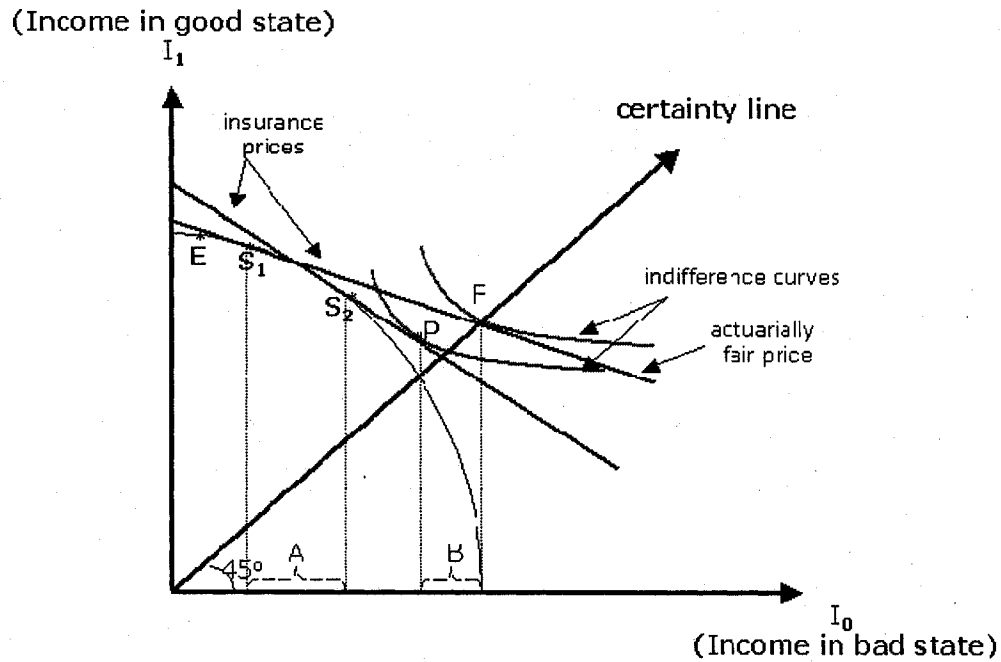
<sup>86</sup> So too, insurers can pool knowledge about risks, identify system-wide vulnerabilities, demand that the insured undergo prequalification audits, and adopt pro-active loss prevention strategies (Beh 2002).

<sup>87</sup> See Kehne (1986): Insurance caused increased safety in fire prevention, aviation, boiler and elevators.

<sup>88</sup> Ehrlich and Becker (1972) have shown that the amount of self-protection can be higher with market insurance than without it, if the premiums are tied to the amount of self-protection. Since the amount of self-protection is negatively related to the probability of the loss, then the presence of market insurance can actually lower the probability of the loss, contrary to the moral hazard argument.

<sup>89</sup> The presence of cyberinsurance increases the amount spent on self-protection as an economically rational response to the reduction of insurance premium, and thus results in higher levels of IT security in society.

products; each additional dollar of good-state income invested on self-insurance is less productive than the previous dollar invested.



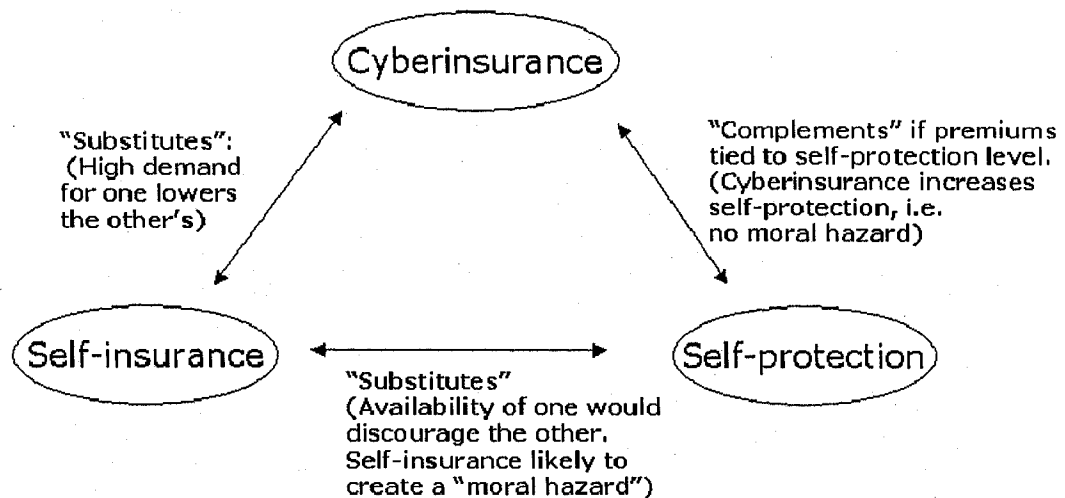
**Figure 2-2.** Self-insurance and cyberinsurance as substitutes<sup>90</sup>

Starting at point E, a firm facing an actuarially fair price would move from E toward  $S_1$  (via self-insurance) or from  $S_1$  to point F (via cyberinsurance). If, however, insurance prices increase, as represented by a steeper price line, the firm would instead have self-insurance up to point  $S_2$  and cyberinsurance up to point F. Thus, as a result of the increase in the insurance prices, the amount of self-insurance increases by the horizontal distance between  $S_1$  and  $S_2$  (represented by A), and the amount of cyberinsurance would decrease by the horizontal distance between points F and G (represented by B) (Ehrlich and Becker 1972). This demonstrates that self-insurance and cyberinsurance are substitutes.

<sup>90</sup> The figure is adapted from Ehrlich and Becker (1972).

Self-insurance, unlike cyberinsurance, is likely to result in a moral hazard in that self-insurance and self-protection act as substitutes.<sup>91</sup> Generally, if the price of insurance is independent of self protection expenditures, the reduction in the probability of the hazard would be exactly offset by the increase in the loading factor. The loading factor, in turn, reduces the demand for self-insurance. Because the price of self-insurance is independent of the probability of loss, there would likely be either a large demand for self-insurance and a small demand for self-protection, or the converse (Ehrlich and Becker 1972).

Cyberinsurers can actually promote self-protection by basing cyberinsurance premiums on the insured's level of self-protection. Figure 2-3 graphically represents these relationships. We conclude that cyberinsurance is better than self-insurance in increasing Internet security.



**Figure 2-3.** Cyberinsurance, self-insurance and self-protection

<sup>91</sup> With market insurance available, since self-insurance and market insurance are substitutes, the loss reduction due to self-insurance would decrease. However, since the insured is now covered by the market insurance, from the point of view of the insured, it doesn't really matter since the loss is reduced correspondingly by the amount of insurance coverage,  $s$ , compensated it by the insurer.

Cyberinsurance does not merely benefit firms. Rather, consumers realize increased privacy and safety. Additionally, customers of firms who purchase third-party liability cyberinsurance receive coverage against fraudulent transactions in cyberspace.<sup>92</sup> By using cyberinsurance, firms benefit consumers in several distinct ways.

First, insurers that offer third-party cyberinsurance will pressure firms to fix security problems<sup>93</sup> such as data leaks.<sup>94</sup> Insurers can make software providers provide secure products by incentivizing the insured firms either via premium discounts or coverage limitations to choose more secure software. For one, insurers can choose to give their seal of approval to specific software. Thus, Wurzler Underwriting Managers has offered clients 5 percent to 30 percent premium break if they use Linux or Unix servers rather than Windows NT because these systems are less susceptible to attack. Security software vendor Tripwire, Inc. has offered 10 percent premium discount on Lloyd's of London's e-Comprehensive cyberinsurance policy to customers who use their product (Savage 2000; Gralla 2001; Lee 2001).<sup>95</sup> Also, cyberinsurers exclude from their policy coverages

---

<sup>92</sup> This is analogous to the third-party coverage for motor-vehicle accidents, where the third-party liability coverage of the injurer contributes directly to the security of the potential victim.

<sup>93</sup> Right now, there exist specific security regulations requiring firms in the financial (see Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness) and health care (45 C.F.R. Parts 160, 162, and 164) sectors, to ensure the security and confidentiality of customer data. For other industries not covered by these regulations or consent decrees, the *National Strategy to Secure Cyberspace* (White House 2003) as well as several commentators suggest that there is a general duty to protect the information under their control (Smedinghoff [2005], citing Radin [2001]; Kiefer and Sabett [2002]; Raul, Volpe, and Meyer [2001]; and Kenneally [2000]).

<sup>94</sup> Note that consumers' prices will increase since part of the insurance costs will be passed on to them by the insured companies. Exactly how much will be passed on to the consumers and how much will be borne by the firm depend on the elasticities of the supply and the demand curve. Security, in this case, is "internalized", that is, it is incorporated as part of the product's or service's price.

<sup>95</sup> AIG have also given its seal of approval to the security sensors developed by a partnership of a dozen IT vendors and the FBI's InfraGard by offering rate reduction to insureds that deploy such technology (Vernon 2003; Vijayan 2005). Safeonline also agreed to provide premium discounts of 10 to 20 percent to customers of Recourse Technologies (Walsh 2001). Recourse offers Manhunt (which provides advanced

losses arising from the inability to use or lack of performance of software programs. For example, AIG's NetAdvantage Security provides that "[t]he insurer shall not be liable for: ... any loss or claim arising out of the inability to use, or lack of performance of, software programmes: ... that have not been released from their development stage; or ... that have not passed all test runs or proved successful in applicable daily operations; or ... due to installation or failure to install software; or ... due to configuration problems".<sup>96</sup> In sum, insurers can pressure software providers to provide more secure products, by choosing risks.<sup>97</sup> By incentivizing the insured firms to choose certain software, either via premium discounts or via coverage limitations excluding software products susceptible to programming malfunctions or have not passed test runs, insurers potentially hold tremendous power in determining which products survive in the marketplace.<sup>98</sup>

---

intrusion detection techniques) and ManTrap (which provides deception host in a decoy environment). According to some industry sources, "Safeonline is able to offer Recourse customers preferred rates because of the effectiveness of Recourse products." (*Business Wire* 2001). Other than these examples, it is also conceivable that insurers can pressure software providers to provide secure products by providing premium discounts or via coverage limitation, by preferring insureds who employ software with some safety features (for example, OS with firewalls, AV, etc.), or software which pass the Common Criteria certification (see *infra* note 122 for a discussion of the Common Criteria), since we know that cyberinsurers such as AIG have used international information security standards such as ISO 17799 in assessing the security of the insured (see Walsh 2002).

<sup>96</sup> Likewise, e-Comprehensive excludes any "malfunction or error in programming errors or omissions in processing" (in computer programs). So too, since lack of performance of software programs is not part of "qualifying clause" in Webnet's policy, it is impliedly excluded. By providing such coverage limitations, insurers make the insured choose only software that are less likely to suffer the abovementioned malfunctions.

<sup>97</sup> See James (1948, pp. 561-62) for various examples of this in other insurance domains such as elevators, boilers, machinery, and air safety.

<sup>98</sup> We have also considered the possibility that third-party can warrant results. Right now, software providers generally do not grant warranty of merchantability for their products. Given that Section 406 of the Uniform Computer Information Transactions Act ("UCITA") (available at <http://www.law.upenn.edu/bll/ulc/ucita/2002final.htm>) approved in 2002, allows for the disclaimer of the warranty (thereby validating the common practice of providing the software on an "as is" basis without warranties), virtually everyone purchasing a software is greeted with shrink-wrap agreements containing among others a disclaimer of the warranty of merchantability. (A google search of "software warranty of merchantability" meets the researcher with results mostly of products terms specifying the disclaimer, including those of Cisco, Verisign Managed PKI, software distributed with Dell products, Apple Mac OS X, Google Desktop, etc.) Software developers almost routinely include the disclaimer because they are

Second, even in the absence of legislation expressly holding firms liable for data leaks,<sup>99</sup> competition pressures will cause firms to develop more secure websites to protect their reputations vis-a-vis other firms.<sup>100</sup>

Third, cyberprotections positively affect third party websites by not allowing compromised systems to serve as a platform for attacking other systems. In addition to reducing the risks of intrusion into other firms' IT infrastructure, customers' personal information residing in those other firms' databases is safer.<sup>101</sup>

In short, not just the insured firm, but also other networks and customers derive safety benefits from cyberinsurance.

---

uncertain of what they are promising with that and how large the concomitant liability could be (Gomulkiewicz 1997). (In fact, some researchers think that applying the warranty of merchantability to software is like fitting a square peg into a round hole [see, for example, Durney 1984]. Software has peculiar characteristics that cause such to be so, including (a) the fact that the warranty do not apply to unique or custom-made products or new inventions in experimental stage (Prosser, at p. 166), of which software is; (b) the nature of software as "diverse collections of ideas that cannot be compared to one another"; and (c) the difficulty of having courts determine what is standard within the trade (Gomulkiewicz 1997). With the difficulty of finding minimum quality standards for software comes the difficulty of applying the Uniform Commercial Code (UCC)'s rule that it must be of a quality comparable to that of similar products (Gomulkiewicz 1997). Moreover, whether a software is a sale of goods (the coverage of the UCC's warranty of merchantability) or a sale of service, or both, is not so straightforward (Carver 1988).)

However, there have been instances when insurers have partnered with third party security technology providers. For example, Safeonline may subcontract technology risk assessment to companies like IBM and others; Marsh uses Internet Security Systems (ISS) as its partners; AIG's technology partners include IBM, RSA Security, and Global Integrity Corp. And some sort of warranty of the security product's effectiveness have been provided by insurers in some of these partnerships. Thus, AIG have provided warranty backing to Citadel's vulnerability remediation product (Vijayan 2005). Other well-known examples of such technology company – insurance firm partnership are Counterpane/Lloyd's of London (Harrison 2000), IBM/Sedgwick (Duvall 1998; Greenemeier 1998); and Cigna Corp/Cisco Systems/NetSolve (Moukheiber 1998; Clark 1998; Davis 1998).

<sup>99</sup> In reality, absent any express legal provision exempting the firm from liability, cyberinsurers have incentives to be cautious and require firms to adopt safety measures since there are privacy common law tort principles that injured customers may potentially resort to. It is to the interest of the insurer to have clearly-defined liability obligations and resolve any ambiguity in favor of precaution.

<sup>100</sup> An analogous idea is when local governments compete for consumers who "vote with their feet" in the choice of local community to live in (see Tiebout 1956).

<sup>101</sup> See Kesan and Majuca (2005): Compromised computers can be used to launch attacks against other systems, as in the case of distributed DoS attacks.

## 2.2. Cyberinsurance Facilitates Standards for Liability to be Set at Socially-Optimal Levels

Liability laws provide efficient incentives for product safety<sup>102</sup> by functioning as a Pigouvian tax that deters harm or internalizes damages caused by the injurer to the victim.<sup>103</sup> Conversely, a liability tax imposed on suppliers of risky goods may discourage the suppliers from developing new, safer products out of a fear of exposing themselves to liability.<sup>104</sup> Lawmakers, therefore, must correctly answer the question of when liability has become too expansive (Shapiro 1991).

As is true with other goods, there is an optimal amount of security. Figure 2-4<sup>105</sup> below shows the socially optimal-level of precaution. Thus, if  $p$  is the probability of a cyber-attack,  $x$  the amount of precaution,  $L$  the monetary value of the loss from a cyber-attack, and  $w$  the cost of precaution (per dollar of unit), the expected social cost equals the costs of precaution plus the expected cyber-loss.<sup>106</sup>

$$SC = wx + p(x)L. \quad (2-3)$$

The line  $p(x)L$  is downward-sloping because increased precaution decreases expected losses. Extra precaution, however, also increases costs (that is why the line  $wx$  is upward-sloping). The socially-optimal level,  $x^*$ , in Figure 2-4 (where the total social costs are at minimum), is achieved by striking a balance between the gain from the additional investment in security and the cost associated with extra security.<sup>107</sup>

---

<sup>102</sup> Another objective of liability laws is to compensate the victim (Shapiro 1991).

<sup>103</sup> When one party is made liable for injury caused to another, an externality has been internalized.

<sup>104</sup> For instance, it has been estimated that liability costs represent 17 percent of the Philadelphia mass transit fares and from 15-25 percent of a ladder's cost. With this, some products or services (such as some park rides and swimming pool diving boards at motels) have just vanished (Viscusi 1991).

<sup>105</sup> This graph and subsequent discussions are drawn from Cooter and Ulen (2004). See also Shavell (1987).

<sup>106</sup> The expected cyber-loss includes all types of cyber-losses to society including spill-over (external) losses, loss of faith in e-commerce, loss of privacy for individuals, etc.

<sup>107</sup> One cost of IT security is its trade-off with convenience. The rule in IT is that security is inversely proportional to convenience (Brush 2001).



$$\begin{matrix} w \\ \text{(marginal social cost)} \end{matrix} = \begin{matrix} -p'(x^*)L \\ \text{(marginal social benefit)} \end{matrix} \quad (2-4)$$

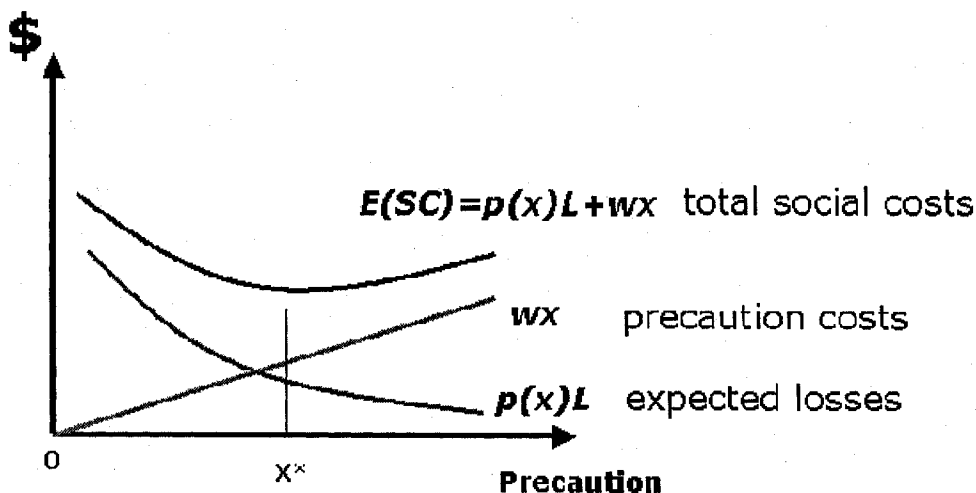


Figure 2-4. Socially-optimal precaution level

The government can encourage firms to implement a socially-optimal level of precaution using three distinct liability regimes: (1) no liability;<sup>108</sup> (2) strict liability; and (3) negligence rule.<sup>109</sup> In general, if the potential victim, but not the injurer, can take precaution, the no liability regime is optimal (Cooter and Ulen 2004).<sup>110</sup> If, on the other hand, the injurer, but not the victim, can take precaution, strict liability with perfect compensation results in efficient precaution where the injurer internalizes the marginal

<sup>108</sup> § 230 of the Communication Decency Act (CDA) (47 U.S.C. § 230) protects Internet Service Providers (ISPs) from libel claims resulting from defamatory materials posted by subscribers and the Digital Millennium Copyright Act (DMCA) (17 U.S.C. §512(c) (2003)) shields ISPs from liability associated with hosting any form of material which infringes some copyright. Thus, in *Zeran v. America Online (AOL), Inc.*, 129 F.3d 327 (4th Cir. 1997), the court held that AOL is not liable for defamatory messages posted by an unidentified third party. But see *Stratton Oakmont, Inc. v. Prodigy Serv. Co.*, N.Y. Sup. Ct. May 24, 1995).

<sup>109</sup> In some sense, both no liability and strict liability are just special cases of the negligence rule: in the latter the due care is set so high that no injurers can meet it, while in the former the due care is set so low that all injurers meet it (see Shapiro 1991).

<sup>110</sup> The victim chooses the level of precaution that minimizes his/her total costs which occurs when his/her marginal costs is equal to his/her marginal benefit. “[T]he rule of no liability causes the victim to internalize the marginal costs and benefits of precaution, which gives the victim incentives for efficient precaution.” If only the victim can take precaution, a strict liability rule with perfect compensation results in zero precaution (Cooter and Ulen 2004).

gains and costs of precaution.<sup>111</sup> However, when both the injurer and the victim can take precaution, neither the no liability nor the strict liability standard can cure the problem of inefficient incentives. In this case, a negligence rule where the legal standard is equal to the efficient level of care results in efficient precaution (Cooter and Ulen 2004).

In the case of a simple negligence rule (illustrated in Figure 2-5 below), the optimal level of precaution is  $x^*$ . Society can set the rule that the injurer is at fault whenever  $x_i$  falls below  $x^*$ . This is the forbidden zone in Figure 2-5 where precaution by the potential injurer is deficient. Thus, whenever  $x_i < x^*$ , the injurer is liable. Otherwise, if  $x_i$  is equal to or greater than  $x^*$ , the injurer is not at fault, and hence, the injurer is not liable.<sup>112</sup>

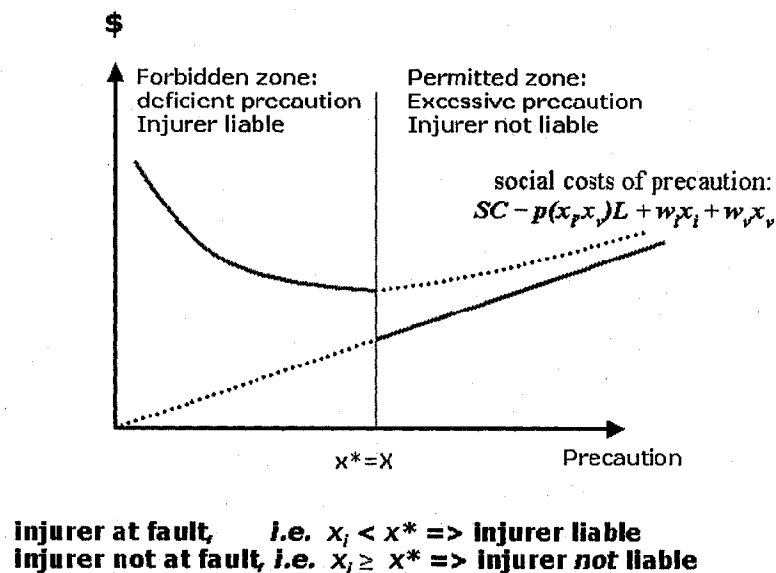


Figure 2-5. Simple negligence liability rule<sup>113</sup>

<sup>111</sup> If the injurer (but not the victim) can take precaution, a *no liability* rule yields zero precaution. The injurer externalizes the gains from precaution. A rule of *strict liability* with deficient compensation results in the injurer externalizing part of the harm and does not provide incentives for optimal precaution (Cooter and Ulen 2004).

For an example of strict liability regime, see Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA), 42 U.S.C. §§ 9601-9627, 9651-9675, 6911a (1988 & Supp. IV 1992); 26 U.S.C. §§ 4611-4612, 4661-4662 (1988 & Supp. IV 1992) (enacting a retroactive strict liability regime to address concerns pertaining to the formation and disposal of hazardous wastes) (Meyer 2003).

<sup>112</sup> This corresponds to the permitted zone in the figure.

<sup>113</sup> The figure is adapted from Cooter and Ulen (2004, p. 327).

Because both the potential injurer and victim can take precautions to strengthen cybersecurity, a negligence rule with a legal standard equal to the efficient level of care results in efficient precaution.<sup>114</sup> In theory, the liability system results in efficient precaution if  $x^*$  is set at just the right amount. Also, because the cost of bringing a liability suit is high (Shapiro 1991),<sup>115</sup> liability rules also do not work for many injuries where losses are smaller than the costs of bringing an action (Kehne 1986). Litigation costs may be especially high for cybersecurity because the question of whether a victim of a computer intrusion can be held liable for subsequent damage initiated from his system is an unsettled issue.<sup>116</sup> Another danger is that the expansion of liability can coincide with increased regulatory standards, particularly when liability and regulatory rules are not coordinated (Viscusi 1991). There are also problems associated with a regulatory regime, not the least of which is the information requirement necessary to quantify the risks in order to set the regulatory standard at the proper level.

---

<sup>114</sup> See Chandler (2005), suggesting the imposition of negligence-based liability against the manufacturer of a software that falls below the standard of security.

<sup>115</sup> There is some empirical evidence – for example in the health care industry – suggesting substantial costs related to enforcement of liability rules: less than half of money paid for liability insurance actually reached the victims, while 80 percent of the premiums are returned to the insured in the form of benefits (Shapiro 1991).

<sup>116</sup> For instance, in the case where e-commerce sites are being targeted by hacktortionists, some believe that the real party at fault are the firms not patching their systems. If network administrators kept tabs on security alerts and routinely patch their systems, the impact of these vulnerabilities would be lessened (see Walsh 2001). Some others believe that the real culprit is Microsoft's software holes that needed patching because the hacktortionist targeted U.S. e-commerce sites using unpatched NT and IIS Web servers (Brush 2001). However, some argue that it may not be reasonable for a court to hold Microsoft liable in a tort claim for damages caused by Code Red II worm if the system administrator failed to patch a system after Microsoft made such a patch publicly available (Vogel 2002). A counter-argument to blaming the victim is that patches demand extensive resources and it is often physically not possible for an administrator to patch all machines in an organization in a responsible manner (such as testing patches to make sure they do not break other business applications which often happens) before exploits against the specific vulnerability are released (the so-called "window-of-opportunity").

Lawmakers do not feel market pressures for precise risk categorization and therefore are not always exact in their appraisal of long-term latent risks (Kehne 1986). This causes a problem in that if regulation overshoots the estimate (that is, sets a standard higher than the socially-optimal level), innovation can suffer. If, on the other hand, lawmakers set the standard too low, injurers responsible for accidents and product defects will not recognize a sufficient deterrence. Furthermore, regulatory agencies may be susceptible to lobbying by powerful interest groups opposed to stricter standards.<sup>117</sup>

The administrative costs of updating regulations are far higher than the costs of adjusting premium rates (Kehne 1986). This is where market-based deterrence can offer definite advantages. Because insurers pool information and are experts at assigning proper prices to risk and developing safety standards, insurers are thus better than regulators at determining an optimal level of insurance.<sup>118</sup> Also, because precise risk categorization requires a predictable relationship between safety practices and liability, it is best for insurers to use their superior information to create a level of reasonable care that causes firms to set loss prevention measures to efficient levels.<sup>119</sup> One way of accomplishing this is by cyberinsurers requiring insured firms to set their loss prevention activities equal to the level that will bring about the socially optimal level of care.<sup>120</sup> In sum, because of the high transaction costs associated with the liability system, as well as

---

<sup>117</sup> See Kehne (1986), citing Noll (1971); Quirk (1981): "Well organized opponents of controls may 'capture' the agencies that regulate them and exert direct pressure on the content of regulations. [They] may also ... influenc[e] the information that the agency chooses to collect and the problems it chooses to investigate".

<sup>118</sup> Kehne (1986): "To operate profitably, insurers must maintain strong incentives for underwriters to assess risks accurately."

<sup>119</sup> Thus, market-based pricing of risk and precaution can at least augment regulatory standards and can internalize the costs and benefits associated with IT security better than a case-by-case application of the "Learned Hand" formula. See *U.S. v. Carroll Towing Co.*, 159 F.2d 169 (2d Cir. 1947). Judge Learned Hand's rule can be reformulated as: the injurer is negligent if the marginal cost of his/her precaution is less than the resulting marginal benefit (Cooter and Ulen 2004, pp. 333-35).

<sup>120</sup> Thus, for instance, insurers have lobbied considerably for mandatory air bags in automobiles and pressured the government to force industries to change (Beh 2002, citing Kneuper and Yandle 1994).

the problems associated with a regulatory regime,<sup>121</sup> market-based incentives such as cyberinsurance are a better alternative than either a liability regime or regulatory system at deterring harm and setting IT security at the socially-efficient level.<sup>122</sup>

---

<sup>121</sup> Insufficient expertise in characterizing risk, political lobbying, and high administrative costs.

<sup>122</sup> Right now, a benchmarking program exists for rating the security of different IT products such as operating systems, switches and routers, anti-virus, firewalls, intrusion detection systems, etc. The Common Criteria (see <http://niap.bahialab.com/cc-scheme/>) provides a standardized evaluation assurance for IT security functionality and serves as a scheme for software security evaluation, certification and accreditation (Common Criteria Introduction, p. 3). The idea, which could perhaps be likened to the Food and Drug Administration (FDA)'s certification which gives a stamp of approval of a drug's efficacy and safety (see, for example, Peltzman 1973, at p. 1051.), is to give IT owners a confidence that security countermeasures are both "sufficient for their intended purpose" (CC Part 3, ¶ 93) and have no exploitable vulnerabilities (see Common Criteria Part 1, Figure 2, at p. 27). It provides a numerical rating of the assessment in the form of "Evaluation Assurance Levels" (EALs) with the assurance ratings ranging from a low of 1 to a high of 7. (The EALs are: EAL 1 (functionally tested), EAL2 (structurally tested), EAL3 (methodically tested and checked, EAL4 (methodically designed, tested and reviewed), EAL5 (semiformally designed and tested), EAL6 (semiformally verified design and tested), and EAL7 (formally verified design and tested) (Common Criteria Introduction, p. 11). Higher EALs indicate more assurance than lower EALs (Common Criteria v3 Part 3, ¶ 225). Thus, EAL1 is the entry level EAL (Common Criteria Introduction, p. 12) and it "provides a meaningful increase in assurance over unevaluated IT" (Common Criteria v3 Part 3, ¶ 236). "Up to EAL4 increasing rigour and detail are introduced, but without introducing significantly specialized security engineering techniques. EAL1-4 can generally be retrofitted to pre-existing products and systems. Above EAL4 increasing application of specialized engineering techniques is required." (Common Criteria Introduction, p. 12). To date, there is no IT product that was validated for EAL6, and only one product, the Interactive Link Data Diode Device Ver. 2.1 by Tenix Datagate Inc., a company that caters to government, defense and commercial organizations.)

However, caveat must be exercised in interpreting the Common Criteria certification. First, "testing can never prove the absence of fatal flaws in software [and] ... can at best [only] establish that the program is not likely to fail under certain uses" (Gemignani 1981). Thus, the fact that a software product has passed the evaluation is not a guarantee against future vulnerabilities; the tests are generally only for things that are known. (The Common Criteria instead prescribes that:

"measures should be adopted that reduce the likelihood of vulnerabilities, the ability to exercise (i.e., intentionally exploit or unintentionally trigger) a vulnerability, and the extent of the damage that could occur from a vulnerability being exercised. Additionally, measures should be adopted that facilitate the subsequent identification of vulnerabilities and the elimination, mitigation, and/or notification that a vulnerability has been exploited or triggered." (CC Part 3, ¶ 94)

and that protection profiles "be reviewed periodically to determine if the requirements are still acceptable in the face of rapidly changing technology, increasing threat levels, and other conditions." (CC Part 3, ¶ 93))

Also, it is extremely hard to predict which of the myriad number of ways a hacker will exploit a software flaw not detected *ex ante*. Moreover, because software is a rapidly developing industry, it is hard for the government to codify technology and/or maintain the standards at such rapid pace of development (Hahn and Layne-Farrar 2006). Thus, the Common Criteria is primarily a certification process aimed at addressing the asymmetric information problem.

Second, the coverage of the Common Criteria certification is limited to the "protection profile" which states under what conditions the evaluation hold. For example, in interpreting Microsoft Window's EAL4, the consumer must be aware that the applicable controlled access protection profile:

### 2.3. Cyberinsurance Increases Social Welfare

The current level of uncertainty associated with traditional insurance policies results in an under-investment in insurance, thereby causing an insufficient amount of profit-smoothing by firms and an inefficient level of risk-sharing throughout society. Similarly, the absence of markets for bearing of new Internet risks lowers the welfare of those who find it advantageous to transfer those risks, as well as those who, because of pooling and superior expertise, are willing to assume such risks (Arrow 1963). In short, a market failure exists because of the absence of markets.<sup>123</sup> By creating markets for the trading of Internet risks, this shortcoming is overcome and the market solution is allowed to work, resulting in greater societal welfare.

The amount of welfare society gains from cyberinsurance is a measurable amount.

This value can be calculated in dollars for varying levels of risk aversion and the

---

“provides for a level of protection which is appropriate for an assumed non-hostile and well-managed user community requiring protection against threats of inadvertent or casual attempts to breach the system security. The profile is not intended to be applicable to circumstances in which protection is required against determined attempts by hostile and well funded attackers to breach system security. The [protection profile] does not fully address the threats posed by malicious system development or administrative personnel.”

which may not be enough to make the system secure except under those narrow conditions (Shapiro).

In sum, we think that although caveat must be exercised in interpreting the results, the Common Criteria rating scheme is a step forward in addressing the problem of information asymmetry in software security. This helps consumers to address somehow the problem of “security by obscurity” as well help address asymmetric information problems, similar to how Carfax help address the information asymmetry problem in the used cars sector. Other helpful developments in this area include the emergence of third party evaluators such as ICSA Labs (firewalls and Internet security products certification) and BITS Financial Services Security Lab (for banking and financial related software and hardware certification) (Hahn and Layne-Farrar 2006).

<sup>123</sup> In general, a market failure exists if any of the three conditions for the equivalence of competitive equilibria and social-optimality fail to hold. These conditions are: (a) existence of markets (that is, “marketability” of all goods and services relevant to costs and utilities); (b) existence of some set of prices which will clear all markets (that is, existence of competitive equilibrium); and non-increasing returns. *Id.* at 942-44. In this case, the absence of markets for the bearing of Internet risks results in a violation of condition (a) and results in a reduction in welfare below that fully-obtainable by society.

probability of a cyber-attack occurring. The market value of income, which, in Figure 2-6 below, is the y-intercept of the “budget line” tangent to the indifference curve, can be used as a measure of welfare. Thus, by comparing the market value of income in the first-best case with full cyberinsurance to the situation when there is no cyberinsurance, we are able to provide dollar estimates of society’s welfare gains from cyberinsurance.<sup>124</sup>

In the next section, we develop a general methodology for calculating welfare gains from cyberinsurance and perform calculations for specific examples.

### **2.3.1. General Methodology for Measuring Welfare Gains from Cyberinsurance**

Figure 2-6 illustrates that the firm starts at point E (without cyberinsurance), which is associated with the lower indifference curve. If there is a cyberinsurance market, the firm can go to point F by buying insurance at the price  $\gamma$  per dollar of coverage. In Figure 2-6, the firms pay the insurer  $I^e - I^*$  and if the attack occurs, the cyberinsurer pays the insured firms  $I^* - I^o$ . By entering into this trade, the firm is able to attain a higher indifference curve by fully insuring. The measurement of the change in welfare is the line  $\overline{AB}$  (the difference between the y-axis intercepts of the “budget lines” tangent to those level curves).

Note that the level surfaces are maximized exactly at the intersection of the “budget lines” with the 45°-line, as a particular characteristic of expected utility optimization:

$$\frac{\partial U / \partial I_0}{\partial U / \partial I_1} = \frac{p \, du / dI_0(I_0)}{(1-p) \, du / dI_1(I_1)}, \quad (2-5)$$

---

<sup>124</sup> This is similar to the international macroeconomic approach of measuring welfare gains from trade (see Grinols and Wong 1991; Grinols 1984; Irwin 2005; Bernhofen and Brown 2005; Feenstra 2003).

which implies that  $\frac{\partial U / \partial I_0}{\partial U / \partial I_1} = \frac{p}{(1-p)}$  at  $I_1 = I_0$ . Also, if we assume constant relative risk

aversion, the utility function are homogenous, which means that the lines tangent to the utility curves are parallel. Thus, the following steps indicate how to measure welfare gains  $\overline{AB}$  :

Step 1: Get data on income in good ( $I^0$ ) and bad ( $I^1$ ) states.

Step 2: Get data on  $p$  (the probability of an attack) and  $\gamma$  (premium per dollar of cover), and calculate A. Here, we assume actuarially fair premiums.

Step 3: Assume a particular parametric form of the utility function, and then calculate  $\overline{U}$  (the expected utility of the lower indifference curve). Assume a constant relative risk aversion among firms. Calculate the gains for varying levels of risk aversion coefficient.

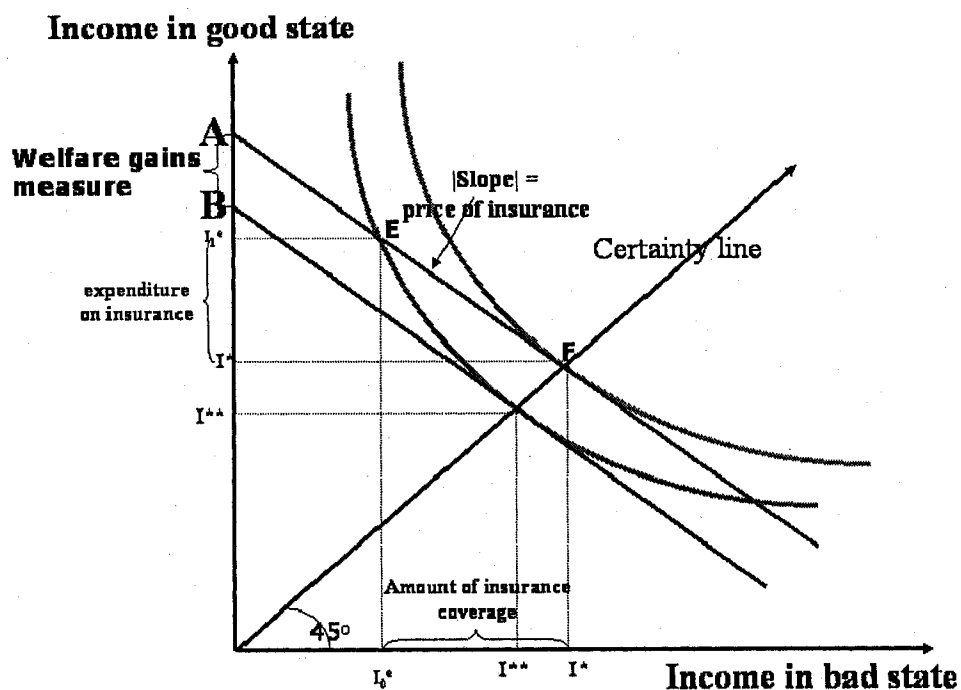


Figure 2-6. Measuring welfare gains



Step 4: Calculate  $I^{**}$ .

Step 5: Calculate  $B$  and subtract from  $A$ . This is our measure of welfare gains (the distance of line  $\overline{AB}$ ).

### 2.3.2. An Example: Calculating Welfare Gains for Year 2000 DoS Attacks

Step 1:

#### Gross Profit (2000) From Yahoo!Finance

Yahoo	\$ 951,759,000
Ebay	335,971,000
Amazon	655,777,000
Total	<u>\$ 1,943,507,000</u> <= we use this figure as $L_0$

From The Yankee Group: The companies' lost revenues, lost market capitalization due to plunging stock prices, and the cost of systems security upgrades due to the DoS attack resulted in more than \$ 1.2 billion (Banham 2000; Gohring 2002)<sup>125</sup>. This means that  $L_I = \$ 3.143$  billion ( $L_0$  + the \$ 1.2 billion damages).

Step 2: Because industry reports indicate that cyberinsurers charge premiums that range from \$5,000 to \$ 60,000 per \$ 1 million of coverage (depending on the extent of the risk and the assets and protection extended [see Mader 2002]), we calculated for  $p=\gamma = 0.005, 0.01, .002, 0.03, 0.04, 0.05,$  and  $0.06$ . As an example,

---

<sup>125</sup> A security incident's impact on the stock prices are usually estimated using event study analysis, a method used extensively in finance, accounting and management science to measure an event's (for example, mergers, regulatory changes, etc.) impact on the stock price of firms (see generally, Cavusoglu et al. [2004] for an application of this technique to computer security events). In general, the market value of the firm's equity following the attacks is subtracted from its market value immediately prior to the attack, and the calculated return is adjusted by subtracting the market's return. This technique relies on the assumption that markets are efficient, in which case the new public information (for example, on the security breach) is immediately incorporated into the stock price (see Fama et al. 1969). The DoS attacks lends itself to this type of analysis since the attacks are a landmark in the catalog of Internet attacks and the relevant time period for capturing the new information flow can be shrunk arbitrarily to capture to specific security event (unless of course if the researcher did not carefully eliminate all other factors that may affect the firm's market valuation). Other studies corroborate the huge and significant impact on the DoS attacks to the stock market price of firms, particularly for substantially Internet-only firms like Yahoo, Ebay, and Amazon, whose market returns are much more affected by security breach announcements than conventional firms (see Ettredge and Vernon Richardson 2002; see also Garg et al. [2003] which estimates an even higher market capitalization loss associated with the Yahoo, Ebay, and Amazon DoS attacks).

in the case where  $p = \gamma = .06$ ,  $I_1^e = A - 0.06 I_0^e \Rightarrow \$ 3.1435 \text{ Billion} = A - 0.06 * \$ 1.9435 \text{ Billion} \Rightarrow \underline{A = \$ 3.2407 \text{ Billion}}$ .

Step 3: As mentioned, it is common in the asset-pricing and macroeconomics literatures to assume a constant relative risk aversion (CRRA) utility function:

$$u(I) = \begin{cases} \frac{I^{1-\sigma}}{1-\sigma} & \text{for } (\sigma > 0, \sigma \neq 1) \\ \log(I) & \text{for } (\sigma = 1) \end{cases} \quad (2-6)$$

This suggests that the firm's willingness to take risks (in *percentage* terms) is constant for all income levels. In other words, the firm doesn't become relatively more or less risk-averse across different levels of income.

The firm's willingness to assume risk is determined by the curvature of the utility

function,  $\sigma = -\frac{u''(I)}{u'(I)} I$ , the Arrow-Pratt (Pratt 1964) coefficient of (relative) risk

aversion. Note that for  $\sigma=1$ , the CRRA utility function is simply the log-utility function, which means the level curves are Cobb-Douglas utility function. Also, in a two-“good” case, the level surfaces of CRRA utility function are constant elasticity of substitution (CES) utility, where the elasticity of substitution  $1/(1-\rho)$  is equal to the reciprocal of the risk aversion coefficient, and the log-utility case ( $\sigma=1$ ) correspond to the Cobb-Douglas level sets:

$$\underline{\text{CRRA:}} U = p \frac{I_0^{1-\sigma}}{1-\sigma} + (1-p) \frac{I_1^{1-\sigma}}{1-\sigma} = \bar{K} \quad (2-7a)$$

$$\underline{\text{CES:}} [a_1 I_0^\rho + a_2 I_1^\rho]^{\frac{1}{\rho}} = K \Rightarrow a_1 I_0^\rho + a_2 I_1^\rho = \bar{K}. \quad (2-7b)$$

Literature suggests that reasonable levels of risk aversion are such that  $\sigma$  is between 1 and 3. We, therefore, calculate the welfare gains (and the premiums) for varying levels of risk aversion within the range such that  $\sigma = 1, 1.5, 2, 2.5, 3$ .

As an example, for  $\sigma = 2$  and  $p = \gamma = .06$ , we calculate

$$\bar{U} = .06 \frac{1.9435^{(1-2)}}{1-2} + (1-.06) \frac{3.1435^{(1-2)}}{1-2} = -0.33.$$

Step 4: For our example ( $\sigma = 2$  and  $p = \gamma = 0.06$ ), we have

$$\bar{U} = .06 \frac{I^{**(1-2)}}{1-2} + (1-.06) \frac{I^{**(1-2)}}{1-2} = -0.33 \Rightarrow I^{**1} = -\bar{U}$$

$$\Rightarrow I^{**} = -\frac{1}{\bar{U}} = \$3.0312 \text{ billion}.$$

Step 5: For the same example ( $\sigma = 2$  and  $p = \gamma = .06$ ), we have  $I^{**} = B - 0.06 \cdot I^{**}$

$$\Leftrightarrow B = 1.06 (I^{**}) = 1.06 * \$3.0312 \text{ billion} = \underline{\underline{\$3.2131 \text{ billion}}}$$

$$\Leftrightarrow \text{Welfare gains} = A - B = \underline{\underline{\$47,040,870.76.}}$$

We performed the same calculations for  $\sigma = 1, 1.5, 2, 2.5, 3$  and  $p = \gamma = 0.005, 0.01, 0.02, 0.03, 0.04, 0.05, 0.06$  with the results presented in Tables 1 and 2 below. We calculated the welfare gains for both (a) DoS attacks against Yahoo, Ebay, and Amazon.com, and (b) worldwide virus and hacking attacks. As Tables 2-1 and 2-2 show, the welfare gains from the presence of a cyberinsurance market can be quite substantial. For instance, assuming constant relative risk aversion and actuarially fair prices, we calculated that in the case of the DoS attacks against Yahoo, Ebay, and Amazon, the availability of cyberinsurance would have resulted in welfare gains to the insured firms of as much as \$78.7 million for a firm with a high degree of risk aversion ( $\sigma=3$ ) facing a high probability of an attack ( $p=\gamma=0.06$ ). Overall, we calculate that if cyberinsurance

were available, the welfare gains associated with insuring worldwide security breaches and virus attacks in 2000 could have approached \$13.16 billion.<sup>126</sup>

### 2.3.3. Calculating Cyberinsurance Premiums

We also calculated the total premium that the insured would be willing to pay for varying levels of risk aversion and attack probabilities. Following Cochrane (1997), the premiums may be calculated as follows:

$$(I_m - \Pi)^{(1-\sigma)} = p \cdot I_0^{e(1-\sigma)} + (1-p) \cdot I_1^{e(1-\sigma)} \quad (2-8)$$

where  $\Pi$  is the total amount of premium paid and  $I_m = p \cdot I_0^e + (1-p) \cdot I_1^e$ . Solving for  $\Pi$ , we have:

$$\Pi = I_m - \left[ p \cdot I_0^{e(1-\sigma)} + (1-p) \cdot (I_1^{e(1-\sigma)}) \right]^{\frac{1}{1-\sigma}} \quad (2-9)$$

Like the welfare gains calculations, we calculated the premiums for  $\sigma = 1, 1.5, 2, 2.5, 3$  and  $p = \gamma = 0.005, 0.01, 0.02, 0.03, 0.04, 0.05, 0.06$  (see Tables 2-1 and 2-2 below).

**Table 2-1. Premiums and Welfare Gains: Year 2000 DoS Attacks (in \$Mn).**

<b>Risk Aversion Parameter <math>\sigma =</math></b>	<b>1</b>	<b>1.5</b>	<b>2</b>	<b>2.5</b>	<b>3</b>
<b>Premiums</b>					
<b>p=<math>\gamma</math>=</b>					
<b>0.005</b>	\$1.55	\$2.54	\$3.67	\$5.03	\$6.62
<b>0.01</b>	\$3.08	\$5.02	\$7.29	\$9.96	\$13.10
<b>0.02</b>	\$6.09	\$9.90	\$14.34	\$19.54	\$25.60
<b>0.03</b>	\$9.03	\$14.64	\$21.17	\$28.75	\$37.54
<b>0.04</b>	\$11.90	\$19.25	\$27.76	\$37.60	\$48.93
<b>0.05</b>	\$14.69	\$23.72	\$34.14	\$46.10	\$59.79
<b>0.06</b>	\$17.42	\$28.07	\$40.30	\$54.26	\$70.15

<sup>126</sup> Our calculations of the welfare gains are broken down for various levels of risk aversion and probabilities of cyber-attack occurring. For our calculations of worldwide welfare gains, we used worldwide gross domestic product (GDP) data (see The World Bank Group 2004) as the income in bad state and \$1.6 trillion as the worldwide loss from hacking and viruses (*see supra* text accompanying note 11).

<b>Welfare Gains</b>						
<b>p=γ=</b>	<b>0.005</b>					
		\$1.59	\$2.57	\$3.73	\$5.09	\$6.69
	<b>0.01</b>	\$3.23	\$5.19	\$7.49	\$10.18	\$13.35
	<b>0.02</b>	\$6.69	\$10.58	\$15.12	\$20.41	\$26.60
	<b>0.03</b>	\$10.37	\$16.17	\$22.89	\$30.70	\$39.75
	<b>0.04</b>	\$14.28	\$21.95	\$30.80	\$41.03	\$52.81
	<b>0.05</b>	\$18.41	\$27.92	\$38.85	\$51.41	\$65.79
	<b>0.06</b>	\$22.76	\$34.08	\$47.04	\$61.84	\$78.69

**Table 2-2. Worldwide Cyberinsurance Premiums and Welfare Gains (in \$Bn)**

<b>Risk Aversion</b>						
<b>Parameter <math>\sigma =</math></b>		<b>1</b>	<b>1.5</b>	<b>2</b>	<b>2.5</b>	<b>3</b>
<b>Premiums</b>						
<b>p=γ=</b>	<b>0.005</b>	\$0.20	\$0.30	\$0.41	\$0.51	\$0.62
	<b>0.01</b>	\$0.40	\$0.60	\$0.81	\$1.02	\$1.23
	<b>0.02</b>	\$0.79	\$1.19	\$1.60	\$2.01	\$2.43
	<b>0.03</b>	\$1.17	\$1.76	\$2.37	\$2.98	\$3.61
	<b>0.04</b>	\$1.54	\$2.33	\$3.12	\$3.94	\$4.76
	<b>0.05</b>	\$1.90	\$2.88	\$3.86	\$4.86	\$5.88
	<b>0.06</b>	\$2.26	\$3.41	\$4.58	\$5.77	\$6.98
<b>Welfare Gains</b>						
<b>p=γ=</b>	<b>0.005</b>	\$0.24	\$0.34	\$0.45	\$0.55	\$0.66
	<b>0.01</b>	\$0.56	\$0.77	\$0.97	\$1.19	\$1.40
	<b>0.02</b>	\$1.44	\$1.85	\$2.27	\$2.69	\$3.12
	<b>0.03</b>	\$2.64	\$3.26	\$3.88	\$4.51	\$5.16
	<b>0.04</b>	\$4.16	\$4.98	\$5.81	\$6.65	\$7.51
	<b>0.05</b>	\$6.00	\$7.02	\$8.06	\$9.11	\$10.18
	<b>0.06</b>	\$8.16	\$9.38	\$10.62	\$11.88	\$13.16

### 3. THE DEVELOPMENT OF CYBERINSURANCE

#### 3.1. Traditional Insurance Policies

The insurance policies firms have traditionally relied upon are: (1) business personal insurance (first-party policies); (2) business interruption policies; (3) commercial general liability (CGL) or umbrella liability insurance policies covering damages to third parties (including those arising from privacy violation); and (4) errors and omissions insurance

policies available to professionals to cover losses arising from the performance of the insured's professional services (Lee 2001). These insurance policies traditionally cover fires, floods, and other forces of nature and do not expressly cover Internet risks.

Many disputes arise between insurance companies and policy holders over the scope and breadth of insurance policies. As an example, because cyber-properties do not have a physical form, attacks on them do not result in any physical damage. Accordingly, there are disputes between insurers and firms as to what constitutes "tangible" property and "physical" damage.<sup>127</sup> Additionally, although most CGLs (Commercial General Liability policy) do not have worldwide coverage, most cyber-torts are international.<sup>128</sup> On one hand, CGL policies commonly designate both a specific coverage area and the location from where an action must arise. In contrast, the question of which court or state or country has jurisdiction over Internet-related events is left open (Gold 2002). In summary, traditional insurance policies use terminology linking physical damage and tangible property and do not consider damage from non-physical, intangible property such as lost data (Beh 2002).

---

<sup>127</sup> In *Retails Systems, Inc. v. CNA Insurance Companies*, 469 N.W.2d 735 (Minn. App. 1991), the court ruled that computer taps and data are tangible property under the CGL since the data had permanent value and was incorporated with the corporeal nature of the tape. In *American Guarantee & Liability Insurance Co. v. Ingram Micro, Inc.*, Civ. 99-185 TUC ACM, 2000 WL 726789 (D. Ariz. April. 18, 2000), the Arizona court ruled that the loss of programming in a computer's RAM constituted physical loss or damage. Also, in *Centennial Insurance Co. v. Applied Health Care Systems, Inc.* (710 F.2d 1288) (7th Cir. 1983), the court ruled in favor of the insured in a dispute concerning defective data processing and system failure which resulted in data loss. However, in *Lucker Mfg. v. Home Insurance* (23 F.3d 808 [3d Cir. 1994]), the Third Circuit ruled that the insured liability for the loss of design use was not loss of tangible property use. So also, in *Peoples Telephone Co., Inc. v. Hartford Fire Insurance Co.*, 36 F. Supp. 2d. 1335 (S.D. Fla. 1997) the Florida District Court ruled that Electronic serial numbers and mobile telephone identification numbers are not 'tangible' property.

<sup>128</sup> See Crane (2001): "Cybertorts particularly difficult to reconcile with standard insurance policies." Different countries have differing standards. For instance, the EU Data Protection Directive has limits on what non-EU countries can do with data gathered online. Moreover, even if a firm's insurance policy expressly stipulate risk coverage, it is uncertain if this encompasses international torts (Crane 2001).

Traditional insurance policies do not explicitly cover Internet risks. Moreover, insurance policy holders desiring coverage for their Internet businesses must challenge insurers consistently insisting on excluding cyber-losses from coverage.<sup>129</sup> This has resulted in: (1) costly litigation between insurers and their policyholders; (2) insurers drafting more ironclad exclusions;<sup>130</sup> and (3) insurers developing new insurance policies to prevent inclusion of cyber-losses.<sup>131</sup> The inability of traditional insurance to deal with the new cyber-threats underscores the need for new insurance products specifically designed to cover the Internet.

### **3.2. The Advent of Early Hacker Insurance Policies**

Although specialized coverage against computer crime first appeared in the late 1970s, these policies were an extension of the traditional crime insurance to electronic banking, and designed mainly to cover against an outsider gaining physical access to computer systems. It was not until the late 1990s that hacker insurance policies designed the Internet first appeared. The earliest known hacker insurance policies were first introduced in 1998 by technology companies partnering with insurance companies to offer clients both the technology services and first party insurance to either back up the technology company's technology or to provide a comprehensive total risk management solution to client firms.

---

<sup>129</sup> See Norman (2001), p. 15: "Many insurance carriers already have gone on record as saying that Love Bug losses are not covered under traditional insurance products."

<sup>130</sup> See Duffy (2002): "As of January 2002, the majority of insurers eliminated virus-related exposures from traditional property insurance because the reinsurance industry is concerned with a cyberhurricane affecting thousands of companies simultaneously with no geographic locus."

<sup>131</sup> See Beh (2002), pp. 77-80: A court may justifiably conclude that the insured did not intend to purchase that type of coverage if a new policy clearly provides particular coverage.

Being a new and unexplored area, these companies started out with small coverage. Thus, the International Computer Security Association (ICSA), the earliest group known to have offered hacker-related insurance as sort of warranty that its service is reliable, started out with only \$250,000 maximum coverage per year. Furthermore, almost all of these early hacker insurance policies covered only the insured firm's own (first party) loss. Table 2-3 illustrates how early hacker insurance started from simple and small amount coverage from losses against hacker attacks, to more differentiated products.

**Table 2-3. Early Hacker Insurance Products**

<b>Year</b>	<b>Company</b>	<b>Description</b>	<b>Coverage</b>
1998	ICSA TruSecure (Poletti 1998; Nelson 1998)	product warranty	1 <sup>st</sup> party coverage: max \$20K per incident; max \$250K per year
1998	Cigna Corp/ Cisco Systems/ NetSolve (Moukheiber 1998; Clark 1998; Davis 1998)	partnership of insurance/benefits company with technology firms; client must buy security assessment and monitoring services	1 <sup>st</sup> party (hacker damage and business interruption); \$10M
1998	J.S. Wurzler Underwriting (Bryce 2001)	insurance broker	1 <sup>st</sup> party
1998	IBM/Sedgwick (Duvall 1998; Greenemeier 1998)	partnership between technology company and insurance firm	\$5-15M
2000	Counterpane/ Lloyd's of London (Harrison 2000)	partnership of security company with Lloyd's insurance	1 <sup>st</sup> party; \$1-10M
2001	Marsh McLennan/AT&T (Salkever 2002)	clients who purchase from AT&T Internet data center receive a discount from insurance company	1 <sup>st</sup> party
2000	AIG (Greenberg 2000)	start of more comprehensive and sophisticated forms of insurance	1 <sup>st</sup> & 3 <sup>rd</sup> party (infringement, libel, slander, privacy, invasion, errors & omissions); \$25M



### **3.3. Causal Events: Increasing Risks and Legislation Compliance**

Perception of risk changed dramatically on September 11<sup>th</sup>, 2001. There had been many Internet security events prior to 9/11 but afterward risks have been considered differently. Three of the most serious Internet worm attacks took place during a three month period around 9/11 – Code Red in July 2001, Nimda in September 2001, and Klez in October 2001. The Slammer Internet worm appeared in January 2003. Prior to 9/11 in February 2000, a series of coordinated denial-of-service (DoS) attacks were launched against major US corporations. Not only did the attacks prevent 5 of the 10 most popular Internet websites from serving its customers but the attacks also slowed down the entire Internet - Keynote Systems measured a 60% degradation in the performance of the 40 other websites that had not been attacked (Nelson 2000).

Clearly, as discussed in Chapter 1, Internet risks have increased during 2000-2003 resulting in a need for individuals and organizations to manage this increased risk. And simultaneous with the increasing risk from Internet attacks has been regulation about the legal use and retention of electronic information, which was started with the need for updated standards given computerized records and then driven by large corporate fraud events for example in Enron and Worldcom (see, for example, the Sarbanes-Oxley Act).

There has also been a recent growing clarity in cyberliability law. Both recently enacted criminal and civil legislation and regulations governing the cyberspace, as well as developing case law, have contributed to the growing clarity of standards and liability rules for the Internet-based economy. For example, both federal and state law now deal with a host of computer crimes (for an example of such federal law, see the Counterfeit

Access Device and Computer Fraud and Abuse Act of 1984 (18 U.S.C. § 1030). Also, practically all states have passed legislation protecting computers (see <http://www.bakernet.com/ecommerce/legis-s.htm> for a compilation of state-level computer laws and regulations).

So also, in order to prevent data residing in financial company databases and network servers from being leaked out, intruded into, or used for identity theft, the Gramm-Leach-Bliley (GLB) Act (Pub. L. 106-102) was passed in 1999. This is because company databases and network servers are readily accessible and easily shared, personal data is susceptible to leaks, intrusions, and identity theft (Solove 2005). Several security regulations were passed in 2001 in pursuance of Section 501 of the Act which mandated certain government regulatory agencies to adopt regulations protecting nonpublic personal information.<sup>132</sup> So too, the Health Insurance Portability and Accountability Act (HIPAA) was passed in order to regulate the electronic transmittal and access to health data of patients and to provide them with more control over the dissemination of their personal information. As mentioned in Chapter 1, the HIPAA Security Regulations, issued in 2003, required health care providers to institute practically the same safeguards GLB security regulations.

Some firms not encompassed by the abovementioned regulations have nonetheless been covered by consent decrees (Smendinghoff 2005 citing *FTC v. Microsoft*, Consent Decree (FTC, August 7, 2002); *In the Matter of Ziff Davis Media, Inc.*, Assurance of

---

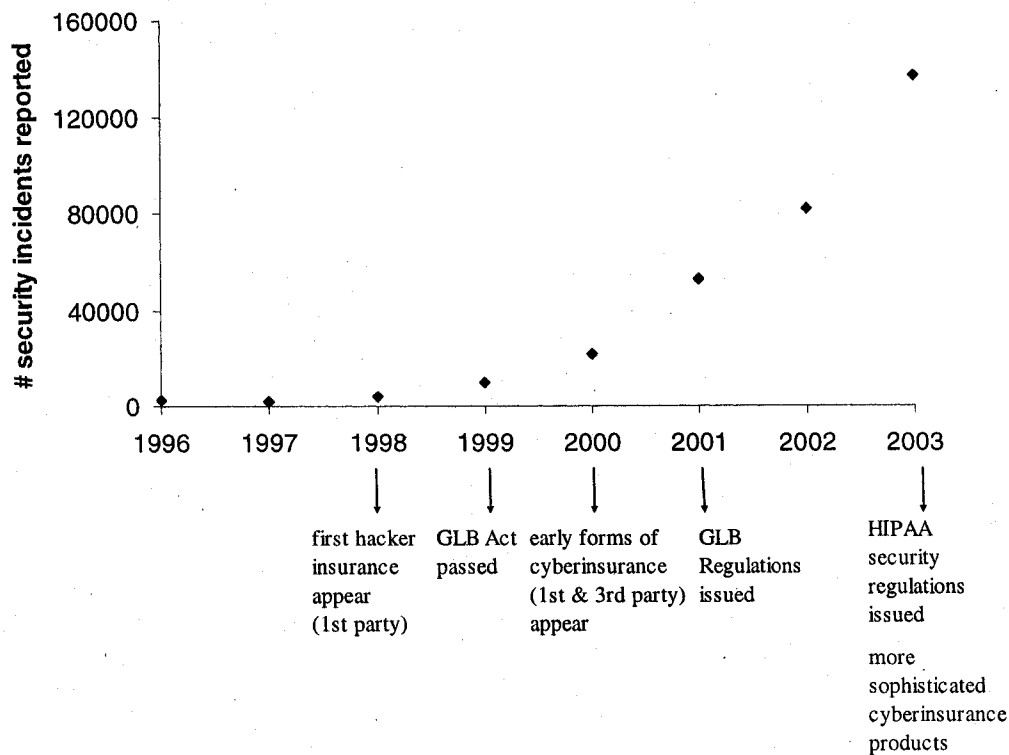
<sup>132</sup> See GLB Security Regulations. These interagency regulations passed in 2001, oblige financial entities to assess, manage and control risks, oversee service provider arrangements, monitor and adjust information security program to take in to account the existing changing technology, the firm's business requirements, and the changing nature of threats, as well as involve the board of directors in the approval and oversight of the information security program (12 C.F.R. Part 30, Appendix B, Part III).

Discontinuance; In the Matter of Eli Lilly & Co., Decision and Order (FTC, May 8, 2002)). Also, there are other criminal or civil liability legislation that businesses with Internet presence must comply with. These include the Digital Millennium Copyright Act of 1998 (P.L. 105-304, 112 Stat. 2860), the Communications Decency Act of 1996 (P.L. 104-104, Title V, 110 Stat. 133), the Electronic Communications Privacy Act of 1986 (P.L. 99-508, 100 Stat. 1936), the Controlling the Assault of Non-Solicited Pornographic and Marketing Act of 2003 (P.L. 108-187, 11 Stat. 2699), the Children Online Privacy Protection Act of 1998, P.L. 105-277, Division C, Title XIII, 112 Stat. 2681-728), the Anti-Cybersquatting Consumer Protection Act of 1999 (P.L. 106-113, § 1000(a)(9), 113 Stat. 1536), the Economic Espionage Act of 1996 (P.L. 104-294, 110 Stat. 1213), and the Sarbanes-Oxley Act of 2002 (P.L. 107-204, 116 Stat. 745) (particularly the internal control provisions of Section 404, which are designed to ensure the integrity of financial reporting).

Hence, we can glean from a review of the growing body of cyberspace law some definite emerging pattern. A higher standard of compliance is required of firms engaged in certain activities: financial and credit report institutions, as well as health care providers have duty to protect personal data residing in their databases; firms that gather data relating to children to duty to safeguard such personal information; firms that employ email to market their products or services need to comply with restrictions relating to non-solicited pornographic and marketing; firms that maintain websites with privacy policy must comply with legal provisions against unfair fraudulent or deceptive practices; publicly held companies must comply with internal controls and reporting standards. Other firms not specifically covered by laws, regulations, or consent decrees,

are charged with general duty to safeguard data under their control (National Strategy to Secure Cyberspace [www.whitehouse.gov/pcipb];<sup>133</sup> Smendinghoff 2005, citing Radin 2001; Kiefer and Sabett 2002; Raul, Volpe, and Meyer 2001; Kenneally 2000).

As shown in Figure 2-7, because of the combination of increased risks and compliance requirements, insurance products specifically targeting the cyberspace have recently sprouted. Insurance products specifically designed for the Internet matured from rudimentary early insurance policies prior to 9/11 to more sophisticated cyberinsurance products post-9/11.



**Figure 2-7.** Internet incidents versus relevant laws and cyberinsurance products (Incident data from CERT/CC, 2005)

<sup>133</sup> Which states that “[a]ll users of cyberspace have some responsibility, not just for their own security, but also for the overall security and health of cyberspace”.

### 3.4. More Sophisticated Cyberinsurance Policies

The new cyberinsurance products can cover several areas including losses arising from (a) DoS attacks (b) e-business interruption; electronic theft of sensitive information; (d) cyberextortion; (e) cybersquatters who occupy domain names; (f) consultants giving wrong recommendation; (g) product liability suits such as improper processing or reporting of data; (h) sensitive data falling into the wrong hands, contaminated or destroyed data resulting in financial loss to consumers; (i) content defamation; (j) copyright and trademark infringement; and (k) privacy suits (Gralla 2001). Some examples of these products include NetSecure by Marsh (see *ZDNet* [2001]); American International Group (AIG), Inc.'s NetAdvantage Security (covering damages arising from hacking, viruses, cyber-extortion, loss of revenue, and damage to intangible property), NetAdvantage (for copyright infringement, libel, and content liabilities); and NetAdvantage Pro (for professional liability for companies with services provided over the Internet); J.H. Marsh & McLennan's NetSecure; Sherwood's e-Sher (see Lee [2001], p. 89); Chubb's SafetyNet; Lloyds of London's e-Comprehensive or Computer Information and Data Security Insurance, Fidelity and Deposit's E-Risk Protection Program (see Brown 2001, p. 33), and products by St. Paul Companies, CNA, InsureTrust.com (see Lee [2001]), and Zurich North America (see Wiles 2003). Premiums can range from \$5,000 to \$60,000 per \$1 million of coverage (or from 0.5% to 6%), depending on the type of business and the extent of insurance coverage.

As can be gleaned from Table 2-3 below, the recent cyberinsurance products have become more sophisticated compared to the early hacker insurance products. Unlike the first hacker insurance products which focused on first-party losses, recent cyberinsurance

products cover both first party and third party insurance, and offer higher coverage. First party coverage typically cover destruction or loss of information assets, internet business interruption, cyberextortion, loss due to DOS attacks, reimbursement for public relation expenses, and even fraudulent electronic fund transfers. Third party coverage typically cover claims arising from Internet content, Internet security, technology errors and omissions and defense costs.

**Table 2-4.** Summary Table of Recent Cyberinsurance Policies

<b>COVERAGE</b>	<b>Net Advantage Security</b>	<b>e-Comprehensive</b>	<b>Webnet Protection</b>
<b>First Party Coverages</b>			
Destruction, disruption or theft of info assets	Y	Y	Y
Internet Business Interruption	Y	Y	Y
Cyberextortion	Y	Y	Y
Fraudulent electronic transfers	N	Y	N
Denial of service attack		Y	Y
Rehabilitation expenses		Y	Y
<b>Third Party Coverages</b>			
Internet Content	Y	Y	Y
Internet Security	Y	Y	Y
Defense Costs	Y	Y	Y

Another noticeable feature of recent cyberinsurance products is that they have narrowly coverages designed to target different kinds of consumers. One reason for this practice is that, by narrowly defining the insurance coverage, insurers are able to exclude coverage of unforeseeable events (Baer, 2003). Another rationale is that by defining coverage more specifically, cyberinsurers are able to engage in product differentiation and thus offer their products to specific markets. For example, cyberinsurers have created products that are specifically meant to target firms concerned about damage to

their own systems, products designed for firms who only want third party liability coverages, or products designed to cover media liability.

In Table 2-5 gives an example of how cyberinsurers engage in product differentiation to capture different segments of the market. In Table 2-5, we see that AIG has offered different types of cyberinsurance products to capture different segments of the market with varying insurance needs. As an example, the enactment of HIPAA resulted in healthcare companies being specifically covered by liability legislation, and hence cyberinsurers have now designed cyberinsurance products specifically targeting this sector. Also some policies cover some specific risks (for example, loss or claim associated with breach of patents or trade secrets, or bulletin boards), which other products exclude.

**Table 2-5.** Different AIG Cyberinsurance Products Reveal Product Differentiation Strategy

<b>COVERAGE \ Net Advantage Product</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>	<b>6</b>	<b>7</b>
Network Security Liability			Y	Y		Y	Y
Web Content Liability	Y	Y	Y	Y		Y	Y
Internet Professional Liability		Y		Y			Y
Network Business Interruption					Y	Y	Y
Information Asset Coverage					Y	Y	Y
Identity Theft			Y	Y	Y	Y	Y
Extra Expense					Y	Y	Y
Cyber-extortion			Y	Y	Y	Y	Y
Cyber-terrorism	Y	Y	Y	Y	Y	Y	Y
Criminal Reward Fund					Y	Y	Y
Crisis Communication Fund					Y	Y	Y
Punitive, Exemplary and Multiple Damages	Y	Y	Y	Y		Y	Y
Physical Theft of Data on Hardware/ Firmware			Y	Y		Y	Y

AIG Product Name: 1 NetAdvantage; 2 NetAdvantage Professional; 3 NetAdvantage Commercial; 4 NetAdvantage Liability; 5 NetAdvantage Property; 6 NetAdvantage Security; 7 NetAdvantage Complete (AIG 2005)

Current industry estimates reveal a growing demand for cyberinsurance products. IT-related policies, for instance, form 30%-40% of the policy mix for InsureHiTech. Firms who recently bought new cyberinsurance products cite as among its advantages: (a) cyberinsurance allows the firm to transfer the risk to an insurers so they feel sheltered with the robust protection; (b) cyberinsurance not only offers monitoring but allows the e-insurer to take fast action against a threat; (c) the benefit of having its systems monitored 24/7/365 by a knowledgeable professional; (d) expediency, since traditional insurance do not provide adequate protection against hacking and other e-risks.

#### **4. HOW CYBERINSURERS WORKED OUT ISSUES IN DEVELOPING COVERAGE**

The newly-introduced cyberinsurance schemes are not without problems. Cyberinsurers had several important implementation issues to address. In this section, we examine these implementation issues and the mechanism cyberinsurers are dealing with them.

##### **4.1. Adverse Selection**

In many circumstances, one party may possess less than full information on the nature of the product being contracted. In insurance settings, these problems arise when insurers are unaware of whether an applicant is high-risk or low-risk. Theory suggests that, in these situations, insurers would offer two types of contract: a low premium, low coverage contract designed to cover the low risk firms, and a high premium, high coverage contract to target the high-risk ones. In equilibrium, the high risk firms choose a contract that has full insurance coverage, while the low risk ones chose a contract that has only partial coverage. That is, the low risk firms suffer, because while the high risk



firms get full coverage, low risk firms do not (Rothschild and Stiglitz 1976). And since some firms (that is, the low-risk firms) are not able to fully insure, the first best solution is not achieved. Only the second best solution – that is, the best solution under information constraint – is feasible. Adverse selection problems therefore result in dissipative social welfare lost. Drawing again from the international trade literature (Grinols and Wong 1991; Grinols 1984; Irwin 2002; Bernhofen and Brown 2003; Feenstra 2003), we can calculate the welfare loss due to adverse selection in dollar amounts.

We use Figure 2-8 to show this calculation of welfare loss. The market value of income is the  $y$ -intercept of the “budget line” tangent to the indifference curve, can be used as a measure of welfare. By comparing the market value of income in the first-best case with full cyberinsurance to the situation where asymmetric information lowers social welfare, we can provide dollar estimates of society’s welfare loss due to the asymmetric information problem. If there are two types of insured in the economy (high risk and low risk ones), and if the insurer cannot distinguish between these two types, the insurer will offer contract  $F_H$  (full insurance contract) to high risk applicants but will not be able to offer  $F_L$  (full insurance) to low risk applicants. In that case, the high risk applicants will have incentive to mimic the low risk applicants and purchase  $F_L$  also. That is, the equilibrium solution must be such that the high risk firms have no incentive to imitate the low risk firms, and the low risk firms do not have incentive to present themselves as high risk firms. This occurs when the insurer offers two types of contract: a high premium, high coverage contract  $F_H$  for the high risk firms, and a low premium, low coverage contract  $P$  for the low risk ones (Rothschild and Stiglitz 1976).

Therefore, under asymmetric information, the first best solution – full insurance contract  $F_L$  to low-risk applicants and full insurance contract  $F_H$  to high-risk applicants – is not attainable. Instead, only the second best solution – where insurers offer partial insurance coverage  $P$  to low-risk applicants and full insurance coverage  $F_H$  to high-risk ones – is achieved. Consequently, social welfare is reduced with the inability of some firms (that is, the low-risk firms) to fully insure. This welfare lost due to the adverse selection problem can be computed as the amount  $A - A'$  in Figure 2-8. As an example, we can calculate the welfare lost for the DoS attack case under risk aversion  $\sigma = 2$ , as follows.

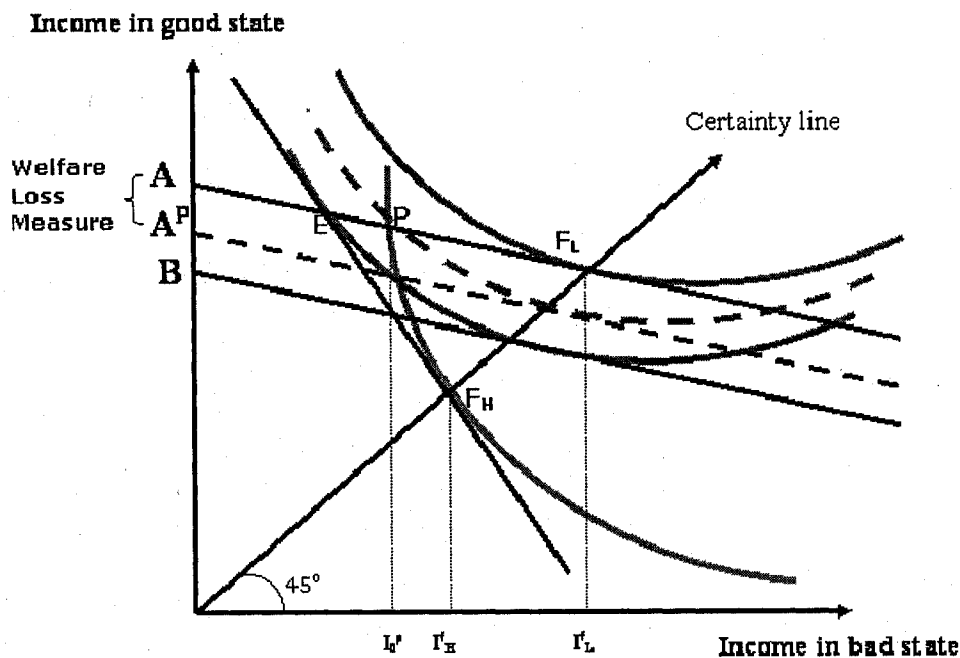


Figure 2-8. Social welfare loss from adverse selection

Step 1: Calculate  $I_H^f$ :  $I_1^e - p_H \cdot (I_H^f - I_0^e) = I_H^f \Rightarrow I_H^f = \$3.076$  billion.

Step 2: Calculate  $EU_H^f$ :  $EU_H^f = \frac{I_H^f (1-2)}{1-2} = -0.32514$ .

Step 3: Calculate  $I_0^p$  and  $I_1^p$ :  $I_1^p = I_1^e - p_L \cdot (I_0^p - I_0^e) = 3.15322 - 0.005 \cdot I_0^p$ .

$$EU_H^f = p_H \cdot \frac{I_0^p \cdot (1-2)}{1-2} + (1-p_H) \cdot \frac{I_1^p \cdot (1-2)}{1-2} \Rightarrow I_1^p = \frac{0.94 \cdot I_0^p}{0.32514 \cdot I_0^p - 0.06} \cdot \text{This implies that,}$$

at  $P$ ,  $I_0^p = \$2.31334$  billion, and  $I_1^p = \$3.1417$  billion.

Step 4: Calculate  $EU_L^p$  and  $I_L^p$ .  $EU_L^p = p_L \cdot \frac{I_0^p \cdot (1-2)}{1-2} + (1-p_L) \cdot \frac{I_1^p \cdot (1-2)}{1-2} = -0.31887$

$$\Rightarrow I_L^p = \$3.136 \text{ billion.}$$

Step 5: Calculate Social Welfare Loss,  $A - A^p$ .

$$A^p - p_L \cdot I_L^p = I_L^p \Rightarrow A^p = \$3.1517 \text{ billion} \Rightarrow A - A^p = \underline{\underline{\$1,500,985}}.$$

The predictions in Section 2.1 above are consistent with the emerging practice in the new cyberinsurance market. To address this adverse selection problem, cyberinsurers require applicants to undergo thorough, detailed, and extensive risk assessments. As a condition to developing coverage, cyberinsurers evaluate the applicant's security through a myriad of offsite and on-site activities with a view of reviewing the applicant's vulnerabilities.

Traditionally, cyberinsurers developing coverage policies have required applicants to provide costly top-to-bottom physical and technical analysis of security, networks, and procedures.<sup>134</sup> Alternatively, some cyberinsurers require applicants to fill in a detailed online questionnaire,<sup>135</sup> to assess the applicants' security risks and cyberprotections.<sup>136</sup>

<sup>134</sup> How a typical step-by-step formal assessment may be done is shown in this PDF document <http://common.ziffdavisinternet.com/download/0/2274/Baseline-NetDiligenceMap.pdf> (last visited April 24, 2004), in Mullin (2002). The strict assessment procedure can be very costly for firms. For example, AlphaTrust Corp.'s (insured by Insuretrust) security assessment cost about \$20,000, while Marsh's security assessment cost \$25,000 (Banham 2000).

<sup>135</sup> Realizing that a detailed top-to-bottom physical analysis can be onerous for buyers, some insurers have simplified their underwriting procedures. For example, Insuredotcom.com developed an online questionnaire, while AIG adopted a three-level underwriting process -- online application, online

For example, a typical cyberinsurer like American International Group (AIG), Inc., Marsh, or Insuretrust would categorize an applicant firm into one of several risk classifications and tie the premiums to the level of the firm's security, giving discounts to firms that have installed a professional security system.<sup>137</sup> Insurers also utilize monitoring of the firm's security processes,<sup>138</sup> third-party security technology partners,<sup>139</sup> rewards for information leading to the apprehension of hackers,<sup>140</sup> and expense reimbursement for post-intrusion crisis-management activities.<sup>141</sup>

The risk assessment starts with the applicant filling in an application form with the detailed security questionnaire, some consisting of about 250 queries, to assess the applicants' 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

---

assessment based on the questionnaire and a remote evaluation of the firm's security, and physical assessment (Banham 2000).

<sup>136</sup> This has also allowed firms to assess their risks and become better aware of their security needs and has also allowed insurers to engage in an ongoing dialogue with the firms about their security risks.

<sup>137</sup> Insuredotcom.com also places its applicant into 1 or 30 risk classifications. For instance, a new dot-com with no credit card transactions is categorized differently from Amazon.com (Banham 2000).

<sup>138</sup> Engaging in dialogue between insurer and insured about their risks is important to developing coverage.

<sup>139</sup> For example, Safeonline may subcontract technology risk assessment to companies like IBM and others; Marsh uses Internet Security Systems (ISS) as its partners; AIG's technology partners include IBM, RSA Security, and Global Integrity Corp.

<sup>140</sup> AIG's NetAdvantage Security offers up to \$50,000 for leads which result in the apprehension and conviction of a cybercriminal (Duffy 2000).

<sup>141</sup> Security software vendor Tripwire, Inc. offers 10 percent premium discount on Lloyd's of London's e-Comprehensive cyberinsurance policy to customers who use their product. Wurzler Underwriting Managers also offered clients 5 percent to 30 percent premium break if they use Linux or Unix servers rather than Windows NT because these systems are less susceptible to attack (Savage 2000; Gralla 2001; Lee 2001). Safeonline also agreed to provide premium discounts of 10 to 20 percent to customers of Recourse Technologies (Walsh 2001).

Internet activities conducted (for example, email and web browsing, production and internal processes integration, e-commerce, VPN, third party hosting services, consulting, etc.). More specific underwriting questions include information relating to:

content: whether the applicant is monitoring its website's content; whether it has qualified intellectual property attorney and/or a written policy for removing controversial items;

what professional services are offered: whether the applicant's services include systems analysis, publishing, consulting, technology professional services, data processing, chatroom/bulletin boards, etc.; whether the applicant sells/licenses software or hardware; and whether there are hold and harmless clauses with subcontractors; and

network security: whether there are company policies on IT security, privacy, and allowable email/Internet use; whether employees are informed of possible disciplinary actions for violation; whether third party security assessment and/or intrusion test were carried out; whether the high priority recommendations of the insurer were put into practice.

The applicant needs to attach, among others, the firm's written policy on IT security, written policy for deleting offensive or infringing items, copy of appraisal of IT security controls and intrusion test outcomes, resumes of senior officers including the director of IT, and audited financial statements. Finally, the application form cites state laws reminding applicants that knowingly supplying false information is a crime in many states. This provides a direct incentive for applicants not to misrepresent their type of risk, at the risk of imprisonment (AIG 2003; InsureTrust.com 2001)

After examining the applicant's detailed application form, insurers then conduct a top-to-bottom physical and technical analysis of security, networks, and procedures. The baseline risk assessment starts with information requests on:

physical security (including where the computer equipments are located, whether the location has single or multiple occupancy or multiple tenants, or whether the facility is a multi-story building, in a corporate campus or city, etc.);

network diagram (which shows the locations of operating systems, remote access devices, placement of routers, firewalls, web, database and email servers; which of systems reside in space leased from ISP; where each IP is located and what machines; and if hard drive or server space is leased); and

description of network activities (for example, list of IP addresses; list of managed devices like switches, hubs, routers, firewalls; platforms and OS including proxy servers, security scanners, anti-virus software, remote computer maintenance, main frame data protocols, firewall tunneling, wireless communications; etc.)

Then follows physical reviews, including checks on applicant's personnel and hiring procedures, physical security review, review of incident response, disaster recovery, and security education programs, as well as technical assessment of the network's external vulnerability, using vulnerability scans, digital sweeps, network monitoring for internal and external malicious users, and a review of firewalls, routers, network configuration. These results are analyzed and a report compiled listing recommendations for upgrades and fixes in order to ensure a more secure network (InsureTrust.com)

This is the mechanism cyberinsurers use to work around the adverse selection problem. The rigorous *ex ante* security assessment allowed insurers to distinguish between high and low risk applicants. By employing a clever mechanism of checking the applicants' security, insurers are able to avert a market failure that results from adverse selection and thus prevent the dissipation of social welfare arising from the asymmetric information problem. Furthermore, such mechanism works directly to benefit the low risk firms, since the security health checks enable them to distinguish themselves from the high-risk firms. With the ability of insurers to differentiate the risk types of

applicants, high-risk applicants can no longer present themselves as low risk types and thus, the corresponding social welfare lost is averted.

#### **4.2. Moral Hazard**

The second major problem that insurers need to address in developing cyberinsurance coverage is the moral hazard problem. This occurs, for example, when firms covered by insurance slack in their security work. That is, they may either not invest in security infrastructure or they may not have incentive to maintain or upgrade their existing level of security.

A well-known device to work around the problem is for insurers to observe the level of care that the insured takes to prevent the loss and tie the insurance premium to that amount of self-protection care. This way, the presence of insurance can in fact increase the level of self-protection that the insured takes rather than decrease it (Ehrlich and Becker 1972; Shavell 1979). If the security level can be perfectly observed either *ex ante* (before writing the insurance contract) or *ex post* (during the effectivity of the coverage), the presence of cyberinsurance increases the amount spent on self-protection by the insured firms as an economically rational response to the reduction of insurance premium, and thus results in higher levels of IT security in society. Hence, the detailed risk assessment conducted by insurers in developing cyberinsurance coverage works both to identify the risk type of the insured (and thus addresses the adverse selection problem), and insofar as tying the risk classification to premium incentivizes the insured to adopt a higher level of security, it also addresses the moral hazard problem.

In examining current industry practice as well as several of the provisions of the cyberinsurance policies, we find that insurers are able to address the moral hazard

problem by instituting several mechanisms in the cyberinsurance contract. By requiring applicants to undergo *ex ante* security assessment, cyberinsurers are able to charge premiums according to risk classifications. For example, insurance coverage to firms with less cyberprotections, with a greater percent of its business online, or in a highly-regulated business subject to high penalties like financial firms, are considered to be higher risk (Mullin 2002).

*Ex post*, cyberinsurers also conduct surveys of insured's information infrastructure, either as part of regular annual surveys of the insurers premises, as part decision to continue and/or modify their coverage, or in processing of a loss or a claim. Several other provisions incorporated in the standard insurance policies are designed to address the moral hazard problem are shown in Table 2-6. First, insurers stipulate in the contract that they are not liable for losses or claims arising from the insured's failure to maintain a level of security equal to or superior to those in place at the inception date of the policy.<sup>142</sup> Second, insurers also explicitly state that no coverage will be given to firms who fail to back up their files. By unanimously excluding loss or claim based on failure to back-up from insurance coverage, cyberinsurers give insured firms incentives to regularly back-up their e-files. Third, once breach has occurred, insurers incentivize insured firms to mitigate the loss. For instance, under Lloyd's e-Comprehensive policy, expenditures incurred by the insured in employing the services of the underwriter's information risk group in order to mitigate the extent of the loss are expressly covered as

---

<sup>142</sup> Thus, e-Comprehensive always include the following provision in its different coverages: "Provided always that the Insured Company maintain System Security levels that are equal to or superior to those in place as at the inception of this Policy" (Lloyd's of London 2002). A similar provision can be found in the Webnet sample policy, thus: "You agree to protect and maintain your computer system and your e-business information assets and e-business communications to the level or standard at which they existed and were represented..." (InsureTrust.com 2003).



a first party loss (Lloyd's of London 2002). AIG's netAdvantage, on the other hand, include as part of its first-party coverage a criminal reward fund to be rewarded to individuals who give information resulting in conviction of the cybercriminal, while Webnet expressly covers investigative expenses incurred by the insured (InsureTrust.com 2003).<sup>143</sup>

**Table 2-6.** Exclusions that address the Moral Hazard Problem in Recent Cyberinsurance Policies

<b>EXCLUSIONS</b>	<b>Net Advantage Security</b>	<b>e-Comprehensive</b>	<b>Webnet Protection</b>
Failure to back-up	Y	Y	Y
Failure to take reasonable steps to maintain and upgrade security	Y	Y	Y
Fraudulent, dishonest and criminal acts of insured	Y	Y	Y
Ordinary wear and tear of insured's info assets	Y	Y	Y
Claim arising out of liability to related parties	Y	Y	Y
<b>OTHER RELEVANT PROVISIONS</b>			
Retentions	Y	Y	Y
Liability Limits	Y	Y	Y
Criminal Reward Fund/Investigative Expenses Covered	Y		Y
Services by Information Risk Group to mitigate the impact of 1 <sup>st</sup> party loss, covered		Y	
Representations Relied Upon	Y	Y	Y
Regular/Annual Surveys of Insured's Facilities	Y	Y	Y

In the case where perfect observation of the insured firms' level of security is not possible, other incentive mechanisms designed to check the moral hazard problem are

<sup>143</sup> Also, Webnet requires the insured to "[n]otify the police if a law is broken" and to "[i]mmediately take all reasonable steps and measures necessary to limit or mitigate the loss, claim, or defense expenses" (InsureTrust.com 2003). E-comprehensive also requires in covering first party losses arising from malicious copying, recording, or sending of the insured's trade secret" that the insured should have "taken reasonable measures to prevent such copying, recording or sending of such Information" (Lloyd's of London 2002).

incorporated in standard cyberinsurance policies. Thus, for example, retentions and liability limits are designed to make the insured somewhat a co-insurer interested in preventing the occurrence of the loss (Shavell 1979). Thus, the insured covers the first losses (retentions) as the insurance covers only amount over which the coverage will apply. Note also that the retentions generally apply to each loss. Other provisions designed to check on the moral hazard problem are the exclusion from coverage of losses and claims caused by fraudulent or dishonest acts committed by the insured, as well as claims arising out liability to related parties. Thus, by observing the level of precaution by the insured, cyberinsurers are able to base a firm's insurance premium on the insured firm's investment in security processes, thereby creating market-based incentives for e-businesses to increase information security.

#### **4.3. Other Implementation Issues**

Internet security externalities arise because of interdependencies from interconnectivity. Computer systems have interdependent security such that an event on one system may affect all its peers even if they are under different administrative control. Thus, if malicious code penetrates a system through a compromised machine, it can use this machine as a platform for further attacks (Heal and Kunreuther 2003). For example, if an individual or firm does not use anti-virus software, if infected it may propagate infections of other systems under different administrative control. Because of this possibility of aggregating cyber-risk exposures, a major concern in developing cyberinsurance coverage is the potential of single Internet security events causing damage to many policy holders simultaneously (Böhme 2005; Ogut et al. 2005). Insurers have put in place several mechanisms designed to alleviate the problem of interrelated risks. As shown in

Table 2-7, insurers may exclude events from coverage in order to protect themselves from large scale losses associated with interrelated risks. For example, a common exclusion relates to losses due to failures of electric and telecommunication facilities. These exclusions are designed to shield insurers from exposure to a single event resulting in a large-scale failure.

**Table 2-7. Exclusions that Address Externalities in Recent Cyberinsurance Policies**

<b>EXCLUSIONS</b>	<b>Net Advantage Security</b>	<b>e-Comprehensive</b>	<b>Webnet Protection</b>
Inability to use or lack of performance of software programs	Y	Y	Y
Electric and telecommunication failures	Y	Y	Y

There are also other problems with the developing cyberinsurance industry. First, high costs, where premiums can range from \$5,000 to \$60,000 per \$1 million of coverage, make it extremely difficult for small and medium-sized companies to purchase cyberinsurance.<sup>144</sup> Second, underwriting qualifications lack standardization and remain complex and time-consuming. Unlike traditional insurance where decades of information are available, there is little history to guide firms looking to minimize Internet risks (Gohring 2002).<sup>145</sup> Because insurers rely on measurements of predictability to forecast probable risk and set prices, the absence of enough historical and actuarial data for Internet risks makes it more difficult to determine premiums (Martin 2002; Walsh 2001).

One possible solution to the risk-assessment problem is partnering insurance brokers with security service providers (Walsh 2001). Another possibility is coordinating

<sup>144</sup> Insurance coverage is not offered to individuals although they can purchase identity-theft coverage (Wiles 2003).

<sup>145</sup> Lack of actuarial or event data on all types of losses uncertainty as well as information about the potential worst-case damage liability presents problems associated with calculation of risks and premium pricing.

regulation and standardizing the policies for computer-related coverage with the help of the National Association of Insurance Commissioners (NAIC), a private, non-profit organization of insurance regulators (Lee 2001). The Critical Infrastructure Protection Board (CIPB), established by President Bush in October 2001, has developed a partnership with insurers to pool the data that exists in many sources within government and insurance industry to develop actuarial tables, a process that is likely to continue into 2005 (Duffy 2002). Federal subsidies are an additional option for encouraging firms to purchase cyberinsurance (Lee 2001, p. 90, citing NAIC's model regulations and guidelines for such areas as accident and health insurance, and the intervention of the government for such areas as floods and nuclear power plant accidents).

## **5. SUMMARY AND CONCLUSIONS**

The Internet has created new risks that traditional insurance policies do not satisfactorily cover. The creation of new insurance products that specifically deal with Internet problems has resulted in: (1) better IT safety infrastructure and increased Internet security; (2) standards based on the optimal amount of care; and (3) overcoming the market's failure thereby increasing overall societal welfare. These results are consistent with the results we found in our survey of the nascent and immature cyberinsurance market.

In this paper, we conducted time and case studies and traced the evolution of cyberinsurance from traditional insurance policies to early cyber-risk insurance policies to current comprehensive cyberinsurance products. We conclude that the cyberinsurance industry has matured from primitive "hacker insurance policies" offering largely first-party policies with low coverages, to more sophisticated, product-differentiated policies

offering first- and third-party insurance products with substantially higher coverages. We also find that cyberinsurance companies are able to deal with implementation issues. For instance, insurers are addressing adverse selection and the moral hazard problem by rigorously classifying the risk level of the insured, and stipulating provisions on the care expected of the insured. We present a methodology for calculating the amount of social welfare loss that was averted by addressing problems such as adverse selection.

We conclude that cyberinsurance products are making the Internet a safer environment because cyberinsurers are requiring businesses to minimize losses using economic incentives and individuals/organizations are increasingly seeing cyberinsurance in their own self-interest. Insurers can pool knowledge about risks, identify system-wide vulnerabilities, demand that the insured undergo prequalification audits, and adopt proactive loss prevention strategies (Beh 2002). This is similar to what has happened in other industries where insurance increased safety in fire prevention, aviation, boiler and elevators (Kehne 1986). In addition to compliance with federal legislation for protecting networked infrastructure, federal subsidies are an additional option for encouraging firms to purchase cyberinsurance following NAIC's model regulations and guidelines for such areas as accident and health insurance, and the intervention of the government for such areas as floods and nuclear power plant accidents (Lee 2001).

**CHAPTER 3:**  
**HACKING BACK: OPTIMAL USE OF SELF-DEFENSE  
IN CYBERSPACE**

**1. INTRODUCTION**

One approach emerging in dealing with the problem of Internet security is the notion of self-help – using reasonable force in self-defense against hackers.<sup>146</sup> At present, counterstrike technology is ready for deployment, as in fact, some organizations have already used it<sup>147</sup> and some commercial products are already available for sale.<sup>148</sup>

However, hitherto, the law has not taken a clear position on the legality of hackback, and among legal scholars the jury is still out whether or not counterstrike should be allowed

---

<sup>146</sup> In real space, various instances of self-help have been recognized by the law, ranging from the use of reasonable force in self-defense or in defense of property in criminal law (see American Law Institute [1985], secs. 3.04 and 3.06), to recovery of property and summary abatement of nuisance in tort law, to repossession and commercial arbitration in commercial law, to the right of restraint and self-help eviction remedies in landlord-tenant relations (see Brandon et al. 1984), and even to such areas as the first amendment, trade secret law, copyright law, and patent law (see Lichtman 2005).

<sup>147</sup> One famous example of hackback that actually took place involved the World Trade Organization (WTO)'s server. Conxion, Inc., which hosted WTO's server was subjected to a DoS attack by an online activist group, Electrohippies (E-hippies). Having traced the IP trail to the E-hippies server and saw postings exhorting the mail-bombing of the WTO, Conxion "returned the mail to sender", swamping the E-hippies server for hours (Radcliff 2000). Another computer counterstrike incident involved the Pentagon. When the activist group Electronic Disturbance Theater attacked the Pentagon's website with a flood of requests, the Pentagon redirected the requests and sent graphics and messages back to the group's system to cause it to crash (Schwartau 1999). An officer of Ernst & Young's information security practice has been quoted as saying that he has knowledge of firms in finance, insurance and manufacturing business that have either set up or are building capability to have aggressive defense capabilities (Schwartau 1999).

<sup>148</sup> Symbiot, Inc., an Austin, Texas-based network security company claims to be the first company to commercially offer for sale a security system with the capacity to strike back (Oram 2004). It offers a solution that not only can repel attacks but also "identify the malicious attackers in order to ... fight[ ] fire with fire." (Symbiot, Inc. 2004b). Symbiot follows the military method of employing a "graduated response" against hackers (Symbiot, Inc. 2004b). The levels of response range from identification of hostile acts, reconnoitering, determining hostile intent, surveillance, to direct and indirect countermeasures such as blocking the act, degradation of the quality of network service, returning fire, invasive techniques (which may either be non-destructive, destructive but recoverable, or destructive and non-recoverable), blacklisting of upstream providers, distributed denial-of-service [DDoS] counterstrikes, special operations, disinformation and psychological warfare (Symbiot, Inc. 2004a).

in cyberspace. Here, we try to understand the optimality of hackback and articulate what the law on self-defense in cyberspace ought to be. In particular, we seek to answer the following questions: Should society permit hackback? How should the law on self-defense in cyberspace be designed? Which among the tools of combating cybercrimes – law enforcement, court litigation, hacking back the hacker – should be used to most effectively address cybercrimes? What optimal mix of these alternatives should be used to combat cyber-attacks? What role does technology play?

The issue of whether or not hackback should be permitted has polarized legal scholars as well as the online community. One major argument for hackback is that traditional law enforcement schemes simply do not work in cyberspace because of the speed by which attacks cause great damage to e-commerce sites and also because hackers can stage attacks from multiple jurisdictions with varying cybercrime laws and procedures for prosecuting Internet crimes. As Smith (2005), for example, point out, while forensic investigation takes time, a virus or worm spreads quickly, underscoring the need to act right away in order to mitigate the grave damage that security incidents can cause. Epstein (2005) believes that even when legal remedies are available, self-help still plays a role because of the numerous instances when the judicial remedy is inadequate or too slow. Thus, Lichtman (2005) points out the importance of bringing together, and capitalizing on the interchangeability between, public and private means, particularly when legal remedies respond slowly to technological risks.

However, some commentators also point out the potential dangers associated with hackback. Kerr (2005), for example, is concerned about counter-strikers hitting innocent third parties rather than the hacker since, in his view, it is easy to conceal the real source

of the attack in the Internet. For instance, one hypothetical scenario that can occur is a hacker using compromised university hospital computers to stage an attack against a firm. If the firm attacks back, it may disable the life supports functions of the hospital, resulting in the loss of the patient's life (Christiansen 2003; Agora Workshop 2003). Because of this consideration, Himma (2004) argues on moral grounds that since the direct and indirect effects of hackback cannot be accurately anticipated, it is not easy to evaluate the pros and cons of hackback to know whether the relevant ethical considerations are satisfied.<sup>149</sup> Katyal (2005), on the other hand, argues that private self-help methods not only raise distributional issues (since the rich would be more able to afford themselves of the private measures than the poor), but also fragment the community spirit by weakening the connectivity between people.<sup>150</sup> He thus proposes methods toward community action against cybercrimes.

---

<sup>149</sup> Himma (2004) argues that permitting hackback may be wrong from a moral standpoint because "we [can't] reliably predict all the direct consequences of digitalized actions ... For example, a set of zombies network could ... have the direct effect of impairing the performance of the life-support system and hence could result in death of any number of innocent bystanders". If such argument is correct, would driving a car be morally wrong because of a remote probability that the driver can fatally hit somebody?

<sup>150</sup> In Professor Katyal's (2005) view, individual self-help can cripple interconnectivity and destroy reciprocity:

"A private precaution ... expresses a view of fear... Bars on windows and other target hardening scares people away, fragmenting the community and the development of an ethos that promotes order... Gated communities ... reduc[e] access ... [and create] poor opportunities for social interaction... [W]alls, street patterns and barricades that separate people from one another reduce the potential for people to understand one another and commit themselves to any common or collective purpose... Gated enclaves tend to be nothing more than an assemblage of individuals lacking any communal spirit... Under a self-help regime, ... the internet could begin to resemble a ... community where people stay indoors because they are afraid of crime."

In our view, however, the community spirit is in many circumstances already fragmented by other factors (such as, in the case of the Internet, the anonymity of the actors). And although individual self-help may contribute to the fragmentation, it may be not be entirely fair to withhold such option to individuals since it may be the rational response to opt for individual self-help remedies rather than to wait for the community to address the problem, especially when the community action is not forthcoming.

The building of community spirit is potentially a fruitful endeavor and thus needs to be pursued more, with the nuts and bolts of the proposal further tightened. (For instance, how does one deal with free riders and shirkers? How are groups formed? How are the responsibilities and costs allocated among the group members? How does one implement and enforce the obligation of each individual in the community?) We



Those aforementioned papers articulate well the arguments for and against hackback. We think, however, that most of these authors take one polar view or the other. On the one hand, you have Smith (2005), who, using historical analogy of the use of spring guns by eighteenth and nineteenth century game owners in England, argues for the use of counterstrike technology in cyberspace without due concern about its potential negative consequences nor specify what appropriate safeguards must be instituted to address potential abuses. On the other hand, we have authors like Himma (2004), Kerr (2005), and Katyal (2005) who looked at issue from ethical considerations and whose concern for the negative consequences of hackback led them to let the pendulum swing the other way. In this paper, we use a law and economics approach to arrive at the middle position. For us, there are benefits for allowing the self-help remedy in *certain* situations, but in other cases, the exercise of the remedy could lead to negative consequences. However, the possibility of abuse does not necessarily mean that the remedy ought to be proscribed, but rather, the exercise of privilege should be regulated.

Thus, we differ in methodology and position from the more polar views of Himma (2004), Kerr (2005), Katyal (2005) and Smith (2005). Our approach and position are closest to that of Epstein (2005) in that with him we think that neither blanket permission nor total prohibition of hackback is the right solution, and Lichtman (2005) in that we deem it important to use public means and private methods like self-help to combat cybercrimes. Unlike Epstein (2005) and Lichtman (2005) who do not lay down the criteria for the valid exercise of hackback however, here we actually formulate what are

---

agree with Professor Katyal that community-based solutions are probably fruitful pursuits, but this need not entail that individual self-help should be banned outright. In fact, the two may very well go hand-in-hand, particularly in cyberspace where the quickness of the attacks, for instance, may entail that individuals should defend themselves until the community is able to act.

the requirements for a valid exercise of self-help in cyberspace, as well as propose what regulations are necessary to guide actual conduct during hackback, in the same manner that Posner (1971) proposed the conditions for the use of deadly force in real space.

However, unlike Posner (1971), we employ formal modeling to generate our criteria and regulations.<sup>151</sup>

Hence, in this paper, we employ formal game theory to model the strategic interaction between the firm and the hacker. This allows us to study the behavior of the hacker given the effectiveness of law enforcement and the potential counter-actions of the firm, and vice versa, and also capture the interaction between law enforcement, court remedies, and self-help remedies. From the Nash equilibria that flow from the model, we observe that the firm will find police enforcement works best in certain instances, while in some cases, resort to the courts based on civil liability litigation will be the better approach, and in still other situations, self-defense and self-help will best address the cybercrimes problem.

Furthermore, from the social planner's perspective, we show under what conditions social welfare is higher when hackback is permitted in society versus when it is not. Also, by identifying the divergence between the private and the socially-optimal solutions, we are able to formulate regulations that are needed in order to bring the private solution closer to the socially-optimal outcome. Thus, explicit modeling enables us to develop litmus tests and criteria that determine if hackback is the proper remedy in

---

<sup>151</sup> Formulating bright-line rules that guides parties when hackback can be resorted to as well as what safeguards must be adopted when conducting hackback is important because (a) lack of clear guidance when hackback can be exercised can result in the underprovision of hackback in society considering that firms may fear exposure to criminal (for example, violation of the Computer Fraud and Abuse Act [18 U.S.C. § 1030]) and/or civil liability, and (b) lack of regulations governing product conduct during hackback may cause firms not to internalize the damage to the third parties' and hackers' systems and result in an excessive amount of hackback.

certain cases, as well as formulate regulations governing proper conduct during hackback.

The model results generate the following criteria for the valid exercise of self-defense in cyberspace: (1) accounting for trace back costs, the damage to the attacked firm's (that is, the entity that is hacking back) systems that can be potentially mitigated outweigh the potential damage to third parties; (2) there is a relatively high chance of hitting the hacker, instead of innocent third parties; and (3) recourse to police enforcement or civil-action based litigation is either ineffective or impractical. The results also underscore the importance of using good technology (that is, intrusion detection systems (IDS), and trace back technology) in order for hackback to be effective as a deterrent against cyber-attacks.

When such criteria are satisfied, resort to hackback would be justified, and the rules governing proper conduct during counterstrike would come into play: (i) counter-strikers should not cause undue damage to the hacker's computer systems and use only reasonable and proportionate means to defend themselves; and (ii) counter-strikers would be held liable for whatever damages may be suffered by innocent third parties caught in the crossfire. These added regulations are necessary in order to move the firm's Nash equilibrium outcome towards the socially optimal result. For example, making firms liable for third-party damages will cause them to internalize in their decision-making the potential damage to others and behave closer to the socially-optimal outcome.<sup>152</sup>

---

<sup>152</sup> Thus, our regulation clearly prohibits retaliation or vigilante justice. Thus, under our proposed rules, a third party hit in the middle of hackback cannot simply hackback the original attacked party in retaliation. The main idea of active self-defense is that it is an action meant to minimize damage to ones' self and not to inflict damage on the other, so that if the third party exercises active defense in order to reduce damage to him, then we envision that to be a valid exercise of hackback; but on the contrary, if such 3<sup>rd</sup> party simply hacks back in retaliation, then such is prohibited. The rules then are also meant to address such possibility. Thus, valid active self-defense should generally be exercised while the attack is ongoing and

As it turns out, these conditions resemble the traditional formulation of the “just war” doctrine,<sup>153</sup> which requires the following necessary elements for a valid counterstrike: (1) there is grave damage (greater than the damage that might result from the action) that will be inflicted to the defender unless it counter-strikes, (2) there is a serious prospect of success, and (3) other means for stopping the evil are either impractical or ineffective (see United States Catholic Conference 1997, ¶ 2309). Interestingly, our requirement that counterstrikers should not wantonly damage the hacker’s system and use only necessary force echoes the classical authors’ position that war must not be waged for “revengeful cruelty” (Augustine 400, ¶ 74) and that only necessary and proportionate force ought to be used (Grotius 1625).

Since our reasonableness conditions were generated from the social planner’s optimization of social welfare, they are consistent with the economic approach to tort law which balances the rights of firms seeking to mitigate damages to their systems and of third parties not being forced to suffer economic harm.

Section 2 presents the basic model. The Nash equilibria of the extensive form game show how the hacker’s behavior depends on the effectiveness of law enforcement and the possibility of being hit back by the firm, as well as how the strategy of the firm depends on the hacker’s behavior, the probability of hitting the hacker, the potential damages to

---

not an after thought after the fact, at the time that there is no more damage to mitigate. At that stage, it is the authorities who take over and the privilege to exercise active defense ceases.

<sup>153</sup> Aurelius Agustinus (354-430), generally acknowledged as the first to have articulated the “just war” doctrine, points out that war must be exercised by the sovereign (¶ 75), and must be waged in order to achieve peace and not for “love of violence, revengeful cruelty, fierce and implacable enmity, wild resistance, and the lust of power, and such like” (¶ 74) (Augustine 400, XXII, ¶¶ 73-79; see also Augustine 423, XIX, chap. 7). Aquinas (c.1271, II, II, Q.40, Art. 1) contributed to the discussion by identifying the three necessary elements for a war to be just: authority of the sovereign waging the war, just cause, and rightful intention. Hugo Grotius, generally known as the father of modern international law, articulated that a just war must contain these basic elements: immediate danger to the nation, necessity of the force employed used is necessary to adequately defend the nation’s interests, and proportionality of the force employed to the threatened danger (DeForrest 1997, citing Grotius 1625).

third parties, and the law enforcement effectiveness. In Section 3, we introduce intrusion detection system (IDS) into the model and examine the role of technology in deterring the hacker and the effectiveness of hackback. Section 4 considers the social planner's perspective and analyzes the divergence between the private and social motive to engage in hackback. Section 5 discusses the proper liability rule for damages to innocent third parties. Based on the model results, Section 6 summarizes what the law of self-help in cyberspace should be. Section 7 concludes our discussions together with some final comments.

## **2. THE BASIC MODEL**

### **2.1. The Model Set-up**

In Kesan and Majuca (2005), we pointed out that in order to effectively combat cybercrimes, society needs to simultaneously focus on the technological, economic, and the legal fronts, since each of these methods alone are insufficient. The question now is how to optimally mix these measures in order to best address the cybercrimes problem. In this paper, we use game theory to explicitly model the interaction between several measures – IDS and traceback (technology), criminal law enforcement and liability-based court litigation (legal remedies), and costs/benefits associated with hackback (economic incentives) – in order to shed light on this question. We start with the basic model of hacker and firm interaction when IDS is not available, and in the next section consider the role of IDS technology.

There is a fraction  $\theta$  of hackers in this model. At period 1, a hacker decides whether to hack or not, and simultaneously, the firm decides whether to monitor or not. Let the

probability that the hacker hacks be  $\delta$  and the probability that the firm monitors be  $\mu$ . If the firm monitored the hacking incident, at period 2, it decides whether to hack back, to file a civil liability-based suit, or simply to recover damages. Denote the probability that it attacks back by  $\sigma_1$ , and the probability that it goes to court by  $\sigma_2$  (with probability  $1 - \sigma_1 - \sigma_2$ , the firm decides to simply recover damages). The game tree is summarized in Figure 3-1 below.

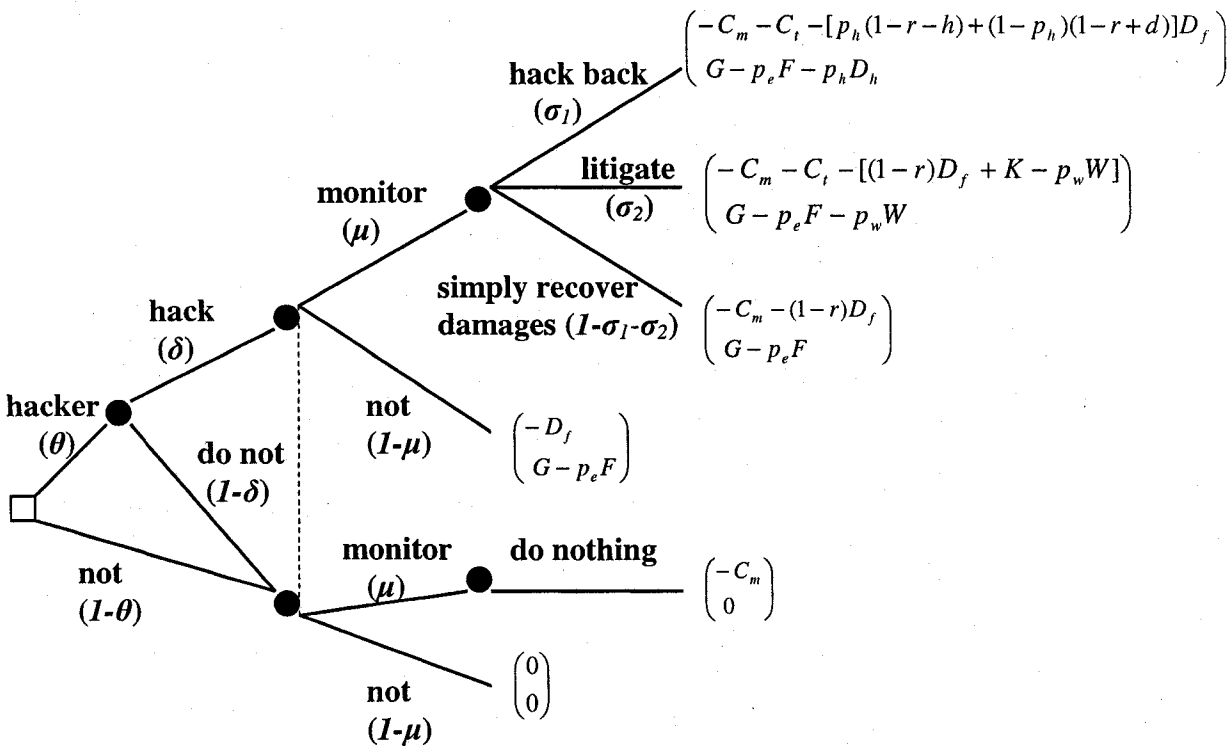


Figure 3-1. Game tree, no IDS case

The hacker gains  $G$  from hacking the firm's computer system, but he pays a fine  $F$ <sup>154</sup> if he gets caught by the police (which happens with probability  $p_e$ ). If the firm decides to monitor and attack back ("hack back"), the hacker suffers damage  $D_h$  when hit (which

<sup>154</sup> We can also consider,  $M$  = monetary equivalent to the hacker of disutility from imprisonment. For notational simplicity, we include this value in  $F$ .

occurs with probability  $p_h$ ). If, however, the firm decides to monitor and bring a suit in court (“litigate”), with probability  $p_w$ , it wins and gets paid the amount  $W$  by the hacker (see Section 8 for a summary of notations). Overall, the hacker must balance his expected gain from hacking with the probability times the magnitude of the fine plus the costs he can suffer in case the firm decides to hack back or litigate. Hence, the hacker’s expected pay-off from hacking is:

$$H(\mu, \sigma_1, \sigma_2, \delta) \equiv \delta(G - p_e F - \mu \sigma_1 p_h D_h - \mu \sigma_2 p_w W). \quad (3-1)$$

The firm, on the other hand, suffers damage  $D_f$  from intrusions into its systems. If the firm decides to simply recover damages, it can recover a fraction  $r$  of the damage. If, instead, the firm decides to attack back, it hits the hacker with probability  $p_h$  and mitigates an additional fraction  $h$  of damage. However, with probability  $1 - p_h$ , it hits innocent third parties instead. We assume, for now, that counter-strikers are liable for damages to innocent third parties,<sup>155, 156</sup> which means that the firm incurs an additional  $dD_f$  expense whenever it hacks back and misses. If, on the other hand, the firm decides to sue, it has to pay the court costs  $K$ , and with probability  $p_w$ , it succeeds and is awarded  $W$ . The firm’s pay-off from hacking back is therefore

$-C_m - C_t - [p_h(1 - r - h)D_f + (1 - p_h)(1 - r + d)D_f]$ , where  $C_m$  is the cost of monitoring and  $C_t$  is the cost of tracing the hacker,<sup>157</sup> and its payoff from litigation and simply

---

<sup>155</sup> In Section 5, we discuss this assumption in more detail, and consider the change in the equilibrium results if firms are instead not liable for third-party damages.

<sup>156</sup> For notational convenience, we express the third-party damages as a fraction  $d$  of the firm’s own damage.

<sup>157</sup> For simplicity, we assume the cost of tracing the hacker to be the same for both hackback and litigation actions.

recovering damages are, respectively,  $-C_m - C_t - [(1-r)D_f + K - p_w W]$  and

$-C_m - (1-r)D_f$ . If the firm decides to not monitor, it suffers the entire damage,  $D_f$ .

The total expected pay-off of the firm is thus:

$$F(\mu, \sigma_1, \sigma_2, \delta) \equiv -\mu C_m - \theta \delta \mu (\sigma_1 + \sigma_2) C_t - \theta \delta (1-\mu) D_f - \theta \delta \mu \left\{ \begin{array}{l} \sigma_1 [p_h (1-r-h) D_f + (1-p_h)(1-r+d) D_f] \\ + \sigma_2 [(1-r) D_f + K - p_w W] \\ + (1-\sigma_1 - \sigma_2)(1-r) D_f \end{array} \right\}. \quad (3-2)$$

The first three terms represent, respectively, the expected monitoring cost, the expected cost of tracing the hacker, and the expected cost of not monitoring. The terms inside the curly bracket are as follows: the first term represents the net cost associated with hacking back, the second term represents the net cost associated with going to court, and the third is the net unrecoverable damage to the firm if it adopts a purely defensive strategy. The hacker chooses  $\delta$  to maximize (1), while the firm chooses  $\mu$ ,  $\sigma_1$  and  $\sigma_2$  to maximize (2).

Thus:

$$\frac{\partial F}{\partial \mu} = -C_m - \theta \delta (\sigma_1 + \sigma_2) C_t + \theta \delta \left\{ \begin{array}{l} \sigma_1 [p_h h - (1-p_h) d] D_f \\ + \sigma_2 [p_w W - K] \\ + r D_f \end{array} \right\} \quad (3-3)$$

$$\frac{\partial F}{\partial \sigma_1} = -\theta \delta \mu C_t + \theta \delta \mu [p_h h - (1-p_h) d] D_f \quad (3-4)$$

$$\frac{\partial F}{\partial \sigma_2} = -\theta \delta \mu C_t + \theta \delta \mu [p_w W - K] \quad (3-5)$$

$$\frac{\partial H}{\partial \delta} = G - p_e F - \mu [\sigma_1 p_h D_h + \sigma_2 p_w W]. \quad (3-6)$$

## 2.2 Equilibrium When Police Enforcement is Effective

**Lemma 3-1.**  $G < p_e F \Rightarrow \delta = 0, \mu = 0 \Rightarrow \mu \sigma_1 = \mu \sigma_2 = 0$ .



**Proof.** From equation (3-6),  $\frac{\partial H}{\partial \delta} < 0$  since  $G < p_e F$ ,  $\sigma_1 p_h D_h \geq 0$ , and  $\sigma_2 p_w W \geq 0$ , implying that  $\delta = 0$  in equilibrium. Substituting  $\delta = 0$  into equation (3-3), we have  $\frac{\partial F}{\partial \mu}(\delta = 0) = -C_m < 0$ , which implies that  $\mu = 0 \Rightarrow \mu\sigma_1 = \mu\sigma_2 = 0$ .

Lemma 3-1 states that if the probability of catching the hacker times the magnitude of the penalty,  $p_e F$ , is bigger than what the hacker gains from hacking,  $G$ , the hacker will not hack, and there is no need for the firm to hack back or to litigate. (This corresponds to area A of Figures 3-2 and 3-3 below.) Thus, when the expected punishment exceeds the expected benefit to the hacker, cyberintrusions will be completely eliminated, and there is no need for the firm to resort to hackback or litigation. Effective cybercrime laws and police enforcement therefore act as a broad deterrent against cybercrimes.

However, law enforcement is costly (Stigler 1970) and society needs to optimally balance the costs and benefits associated with enforcing crime laws (Becker 1968).<sup>158</sup> Accordingly, it may be optimal for society to permit that some offenders go unpunished and “[t]he optimal amount of enforcement depends on, among other things, the cost of catching and convicting offenders ... and the responses of offenders to changes in enforcement” (Becker 1968, p. 170). Particularly in the Internet where hackers can situate themselves in different and several jurisdictions with varying computer crime laws of several jurisdictions, the costs associated with the discovery and prosecution of hackers can be prohibitive, and hence, traditional law enforcement measures cannot be

---

<sup>158</sup> The issue of law enforcement and the optimal probability and magnitude of fines has also been discussed in, for example, Stigler (1970), Shavell (1991), and Mookherjee and Ng (1992).

entirely relied upon to address cybercrimes.<sup>159</sup> In this situation, firms can provide additional deterrence by resorting to litigation and/or counterstrike.

We discuss in Propositions 3-1 to 3-5 the optimal behavior of the firm when law enforcement is inadequate, in accordance with the following scenarios:

Proposition 3-1: No IDS available; litigation is not a beneficial option

Proposition 3-2: No IDS available; litigation is a beneficial option

Proposition 3-3: IDS available; litigation is not beneficial, whether or not the IDS signals an intrusion

Proposition 3-4: IDS available; litigation is beneficial, whether or not the IDS signals an intrusion

Proposition 3-5: IDS available; litigation is beneficial when IDS signals an intrusion, but not otherwise. (Note that, as Lemma 3-2 in Section 8 shows, there cannot be situations where litigation is beneficial when IDS does not signal an intrusion, but not otherwise.)

### 2.3 Equilibrium When Litigation is Not Beneficial

**Proposition 3-1.** When  $[p_w W - K] < C_l$ , litigation is not beneficial, and the following Nash equilibria obtain:

---

<sup>159</sup> In fact, in an August 2001 survey by CIO Magazine, 88 percent of 450 chief information officers surveyed do not think that existing law enforcement agencies are ready to address cybercrimes (*CIO Magazine* 2001).

Probability times  
Magnitude of Fine,  $p_e F$

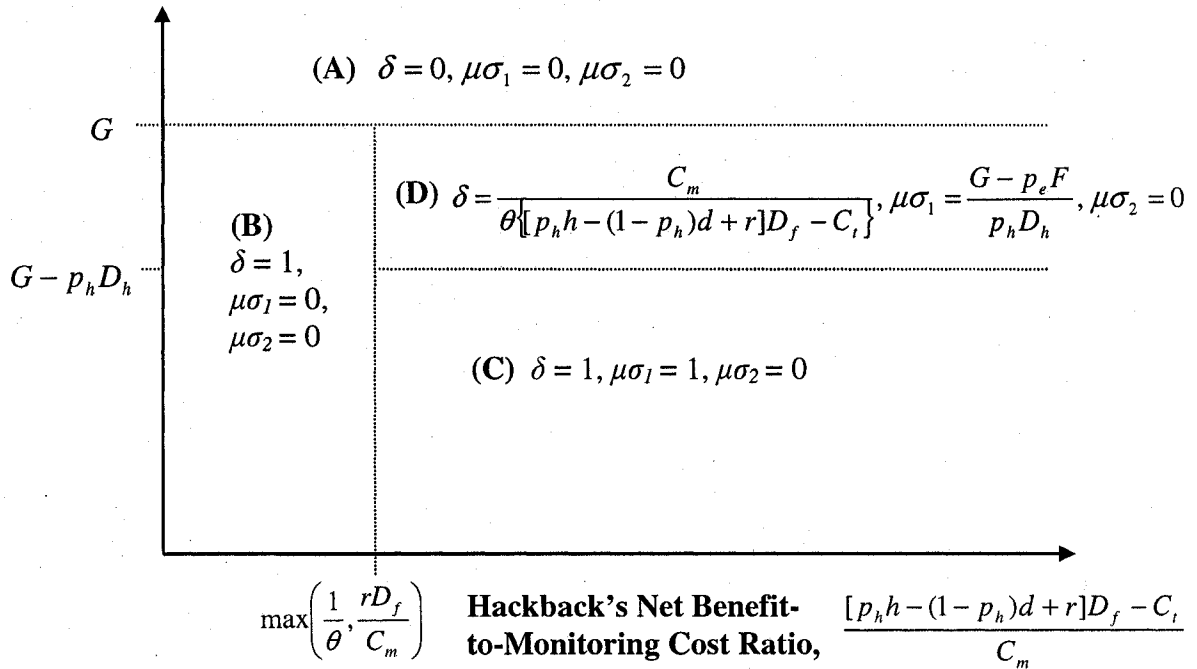


Figure 3-2. Nash equilibria when litigation is not beneficial  
(No IDS available)

**Proof.**

$[p_w W - K] < C_t \Rightarrow \frac{\partial F}{\partial \sigma_2} < 0 \Rightarrow \sigma_2 = 0$  in all equilibria here. *Equilibrium B:* For

the case  $\frac{rD_f}{C_m} > \frac{1}{\theta}$ :  $\frac{[p_h h - (1 - p_h)d + r]D_f - C_t}{C_m} < \frac{rD_f}{C_m} \Rightarrow$

$\frac{[p_h h - (1 - p_h)d]D_f - C_t}{C_m} < 0 \Rightarrow \frac{\partial F}{\partial \sigma_1} < 0 \Rightarrow \sigma_1 = 0$ . For the case  $\frac{1}{\theta} > \frac{rD_f}{C_m}$ :

$\frac{\partial F}{\partial \mu} = -C_m + \delta\theta\sigma_1 \{ [p_h h - (1 - p_h)d + r]D_f - C_t \}$  is less than zero in the range

$\theta \{ [p_h h - (1 - p_h)d]D_f - C_t \} < C_m$  or  $\frac{[p_h h - (1 - p_h)d + r]D_f - C_t}{C_m} < \frac{1}{\theta}$ , that is,  $\mu = 0$ .

Thus,  $\mu\sigma_1 = 0$  for either case. This implies that  $\frac{\partial H}{\partial \delta} = G - p_e F$ , which is positive in the

region; thus,  $\delta = 1$ . *Equilibrium C:*  $\frac{[p_h h - (1 - p_h)d + r]D_f - C_t}{C_m} > \frac{rD_f}{C_m} \Rightarrow$

$$\frac{\partial F}{\partial \sigma_1} > 0 \Rightarrow \sigma_1 = 1. \text{ Given } \sigma_1 = 1 \text{ and } \sigma_2 = 0,$$

$$\frac{\partial F}{\partial \mu} = -C_m + \theta \delta \{ [p_h h - (1 - p_h)d + r]D_f - C_t \} > 0 \text{ for the region}$$

$\theta \{ [p_h h - (1 - p_h)d + r]D_f - C_t \} > C_m$  if  $\delta = 1$ .  $\delta = 1$  because  $\frac{\partial H}{\partial \delta} > 0$  in the region.

*Equilibrium D:* Since  $\frac{[p_h h - (1 - p_h)d + r]D_f - C_t}{C_m} > \frac{rD_f}{C_m}$ , then  $\frac{\partial F}{\partial \sigma_1} > 0 \Rightarrow \sigma_1 = 1$ .

Also, we know by Nash (1950) that if  $G \geq p_e F > G - p_h D_h$  and

$\theta \{ [p_h h - (1 - p_h)d + r]D_f - C_t \} > C_m$ , an equilibrium in mixed strategies exists. Setting

$$\frac{\partial F}{\partial \mu} = 0 \Rightarrow \delta = \frac{C_m}{\theta \{ [p_h h - (1 - p_h)d + r]D_f - C_t \}}. \text{ Thus, } H = \delta(G - p_e F - \mu p_h D_h).$$

Hence,  $\frac{\partial H}{\partial \delta} = 0 \Rightarrow \mu = \frac{G - p_e F}{p_h D_h}$ . Thus,  $\delta = \frac{C_m}{\theta \{ [p_h h - (1 - p_h)d + r]D_f - C_t \}}$ ,

$\mu\sigma_1 = \frac{G - p_e F}{p_h D_h}$ , and  $\mu\sigma_2 = 0$  are equilibrium strategies.

When the net payoff from going to court is lower than the trace costs, going to court would not be beneficial for the firm.<sup>160</sup> In such a situation, when both police enforcement

<sup>160</sup> For example, the hacker may be situated in a country with weaker computer laws than the country where the firm is from. Also, even if the firm is able to get hold of and legally make the hacker liable to pay, the hacker may not have the means to pay, thus the firm may not find going to court an attractive option.

and litigation are ineffective or impractical, self-help can be useful in mitigating the damage to the firm's e-assets.

The firm's choice between a passive self-help remedy (that is, simply recovering damages) and a more active defense (that is, hackback) would depend on their relative pay-offs. If the net pay-off from active defense is less than that of simply recovering damages then the firm will not hack back. That is, the firm will simply recover damages if  $[p_h h - (1 - p_h)d]D_f < C_i$ . That is, the firm's decision to hack back will crucially depend on the damage that can be mitigated to firm's systems relative to those that can potentially be caused to third parties. The firm will find it advantageous to counter the attack only when it calculates that the damage that it can mitigate by counter-striking would be considerably greater than the potential liability.<sup>161</sup> Thus, extreme conditions like stopping an ongoing major denial-of-service (DoS) or distributed denial-of-service (DDoS) attack may require knocking down the master machine lest considerable damage would be incurred.

Because of the discipline induced by the liability rule, the firm's objective in hacking back will be limited to mitigating damages to its systems and due care will be exercised in order to lessen the damages inflicted to third parties. That is, the liability rule induces the firm to internalize the potential damages that it may cause others. Also, since the net pay-off from hackback depends crucially on the probability of hitting the right person instead of innocent ones, from the firm's perspective, the decision to hackback depends on the available traceback technology: hackback will make sense only if the probability

---

<sup>161</sup> Hacking back makes more sense the bigger the potential damage that the firm can prevent its own system and the smaller the potential damage to innocent third parties.

of successfully tracing and hitting the hacker exceed a certain threshold level.<sup>162</sup> If the probability is below this level, then active defense is not optimal. The firm will thus hack back only if there is “serious prospect of success”.

In effect, our model shows that the concern of other authors about innocent parties getting hit (see, for example, Himma 2004; Kerr 2005; Katyal 2005) is alleviated by liability rules. Liability for damages to innocent third parties causes the firm to strike back only if the probability of hitting the hacker (instead of innocent third parties) is large enough relative to the amounts of damages involved. The fact that the firm would be liable makes it cautious in calculating its chances of (and benefits from) success as compared to the potential liability. This may in fact induce technical developments in the precision of traceroute technology as more firms demand precise devices that can help them trace the hacker more accurately.<sup>163</sup> Nonetheless, regardless of the state of the current traceback technology, strong enough liability rules will induce firms to hack back only when optimal since, depending on the ratio of damages involved, if the probability of hitting the hacker is so small, firms will choose not to hack back.

Figure 3-2 also shows that the propensity to hack back decreases with the effectiveness of law enforcement. Thus, increasing either the probability or the magnitude of the fine has two important effects. First, it reduces the hacker’s intrusion

---

<sup>162</sup> This threshold level of probability depends on ratio of third-party damages to the sum of the mitigated damages and third-party damages, that is,  $p_h > \frac{d}{h+d} + \frac{C_m}{\theta(h+d)D_f}$ .

<sup>163</sup> Significant strides have recently been made in the area of traceback research. IDSs and firewalls acquire data about inbound IP addresses that can be employed to initiate a trace (Jayawal, Yurcik, and Doss 2002). If the hacker uses a valid source address, techniques such as the traceroute utility can be used to identify with reasonable accuracy the attack’s path (Moriarty 2003). In the case of attacks from spoofed address or when hacker logs-in through a chain of hosts, other techniques such as packet filtering and flow analysis can be utilized to track the source (Moriarty 2003). The path of the traffic can also be reconstituted using network routers if detailed logging is employed. Also, sleepy watermark tracing can also be employed to inject watermarks into the path of the attack (Jayawal, Yurcik, and Doss 2002).

rate (compare, for example, the hacker's equilibrium strategy for regions (C), (D) and (A)). Hence, an investment in more police resources and international coordination of enforcement efforts, for example, can reduce hacking activity. Second, better police enforcement also reduces the firm's propensity to hack back, as the firm perceives a higher level of protection that law enforcement affords (compare, for example, the firm's strategy for regions (C), (D) and (A)). This emphasizes the substitutability between self-help and law enforcement. This also reduces the force of the argument that since hackers are anonymous in the Internet, hackback should be prohibited (see, for example, Kerr 2005). True, the fact that hackers can attack anonymously in the Internet could mean that innocent third parties may be caught in the crossfire.<sup>164</sup> But that fact, as well as the fact that hackers can situate themselves in different jurisdictions, also mean that cybercriminals are harder for the police to pin down thus lowering the efficacy of traditional police enforcement measures, and increasing the need for self-help measures to substitute in for the slack by providing additional remedy and deterrence against intrusions.

Thus, equilibrium D illustrates the deterrent effect of hackback when law enforcement per se is not sufficient to completely eliminate cybercrimes. When effective police enforcement,  $p_e F$ , lies in between  $G$  and  $G - p_h D_h$ , in region D, the hacker adopts a mixed hack strategy in response to the firm's adopting a mixed hackback strategy. In contrast, in the same region of police enforcement, if the firm does not hack back, the hacker will definitely hack (region B).<sup>165</sup> Thus, when the probability times the magnitude

---

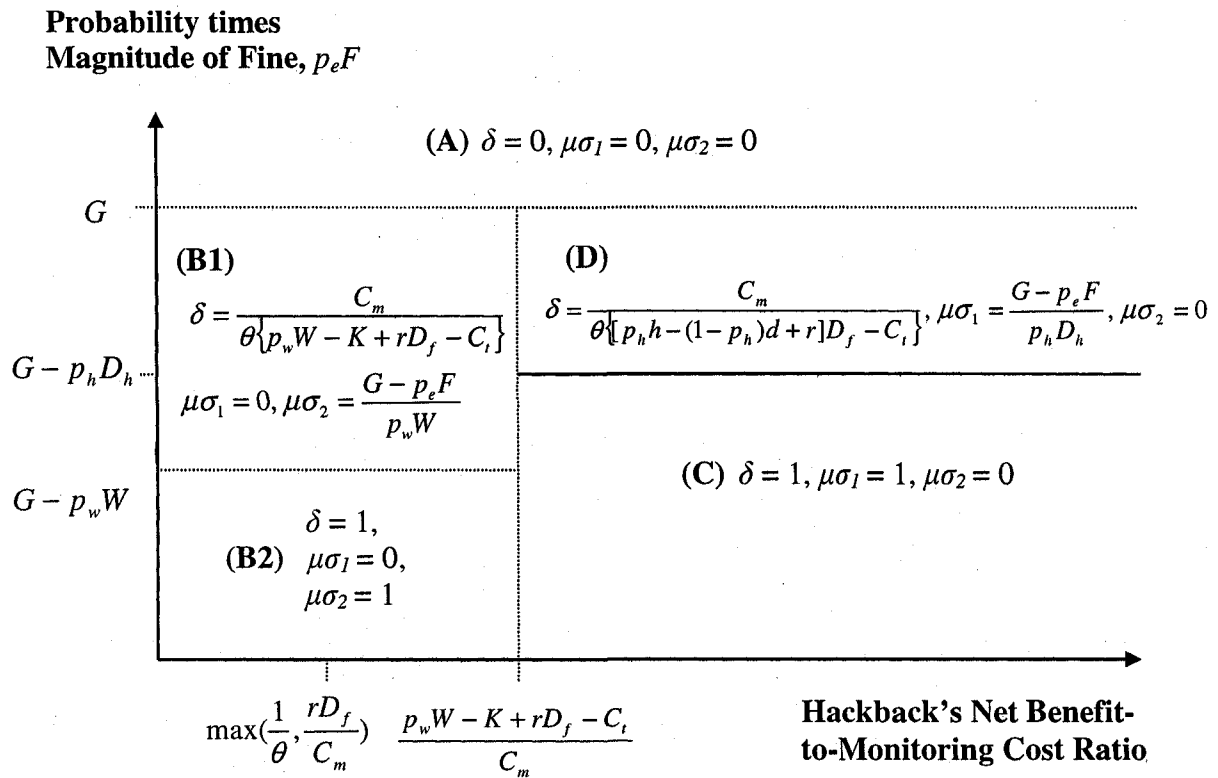
<sup>164</sup> This concern though, as mentioned, could be handled by liability rules holding firms responsible for the consequences of their actions.

<sup>165</sup> This region where hackback has a deterrent role thus depends on  $p_h D_h$ , that is, current traceback technology's ability to identify the hacker multiplied by the damage that the hacker suffers as a result of the

of the fine falls below the gain from hacking, self-help can supplement law enforcement because the hacker incorporates in his decision-making the potential damage a counterstrike can inflict on its system.

## 2.4 Equilibrium When Litigation is Beneficial

**Proposition 3-2.** When  $C_t < [p_w W - K]$ , litigation is beneficial, and the following Nash equilibria obtain:<sup>166</sup>



**Figure 3-3.** Nash equilibria when litigation is beneficial  
(No IDS available)

counterstrike. This result confirms the conventional belief that “[k]nowledge of the source of [an] attack via traceback capability has the possibility to ... deter ... DOS attacks .. with counter-attack” (Jayawal, Yurcik, and Doss 2002).

<sup>166</sup> Proof of this and subsequent lemmas and propositions are presented in the Appendix.



When the proportion of hackers times the net pay-off from litigation exceeds the trace costs, litigation is a beneficial option for the firm. In this case, the firm will choose between litigation or hackback, depending on whether the net pay-off from litigation exceeds that of hackback's (equilibria B1 and B2 on the left side of Figure 3-3) or vice versa (equilibria C and D on the right).

The firm will prefer to rely on active defense if its net pay-off,  $[p_h h - (1 - p_h)d]D_f$ , exceeds that of litigation,  $p_w W - K$ . Thus, if active defense will allow the firm to save further damage, or if there are high transaction costs of going court, self-help will be the more effective remedy.<sup>167</sup> When it is more beneficial for the firm to engage in self-help remedies (equilibrium C and D), the law should perhaps not compel the firm to go to court.<sup>168, 169</sup>

However, self-help is not the better remedy in all situations. Equilibria B1 and B2 illustrate cases where the benefits from self-help are small compared to the more effective relief afforded by the courts. In these cases, self-help measures are not cost-effective, and the courts should be provided as an alternative that the firm can resort to. This illustrates why there would still be a need for the legal system to provide formal legal protections since in certain instances, self-help remedies do not provide complete

---

<sup>167</sup> Comment e of Section 218 of the Restatement takes away from the chattel owner the option of bringing a suit for nominal damages for harmless interferences, and instead mandates the use of self-help remedies. The "mitigation of damages" rule principle also obligates parties to exercise reasonable self-help measures (such as protecting one's property from further intrusions) in order to minimize the damages, and failure to prevent a tort or to minimize the severity of its harm by exercising the privilege is contributory negligence that will bar recovery of damages for the portion attributable to the neglect (Brandon et al. 1984, p. 871 and n. 146).

<sup>168</sup> Among the advantages of hackback compared to litigation, for example, is speed of the remedy. Hackback can prevent, for example, worms or DDoS attacks from further inflicting damage. Thus, sometimes the way to effectively address an attack is to defend one's self rather than first gather evidence and go through court processes, since measures taken after-the-fact may not work.

<sup>169</sup> See, for example, the case of *Intel Corporation v. Hamidi* (71 P.3d 296 [2003]), where the legal remedy of injunction based on a defamation suit is available, but it is not in the firm's interest to avail of it (Epstein 2005).

assistance (see Epstein 2005; Lichtman 2005). The law should thus permit hackback as an option, but not force it as a requirement (see Brandon et al. 1984, p. 870 *et seq.*, for examples of judicially required self-help).

### 3. THE ROLE OF IDS TECHNOLOGY

The model in Section 2 assumes that firms are not assisted by technology to help detect whether its computer systems are under attack or not. In this section, we study the case where the firm employs an intrusion detection system (IDS) technology to help spot intrusions in its network,<sup>170</sup> and analyze the role that technology like IDS play against cyber-attacks.<sup>171</sup>

Suppose that the firm installs an IDS in its security architecture. The timing of the game is then modified as follows:

Period 0. Nature determines if an individual is a hacker or not.

1. The hacker decides whether to hack or not.

1'. The IDS sends a signal on whether or not there is an intrusion. A well-known feature of IDSs is that their signals are not perfect. There are usually false positives (where intrusions occur but the IDS fail to detect them) and false negatives (where the IDS falsely reports an intrusion). Denote  $1-q_1$  to be the probability that the IDS misses an attack, and  $1-q_2$  to be the probability that the IDS sends a false alarm.

2'. Depending on whether or not the IDS signals an intrusion, the firm decides whether to hack back, to go to court, or simply to recover damages. Denote the

---

<sup>170</sup> IDSs act like security cameras that monitor suspicious activities in a network and alert administrators about unusual activities, by either comparing suspected security breaches to a database of known attacks or checking for abnormal behavior.

<sup>171</sup> For other IDS models, see, for example, Alpcan and Basar (2004) and Cavusoglu, Mishra, and Raghunathan (2005). Our model differs from these models in that we focus on hackback, as well as the interaction between private and court-assisted remedies.

probability that the firm will hack back given an intrusion signal by  $\alpha_1$ , the probability that it goes to court given such signal by  $\alpha_2$ , the probability that it hacks back even if the IDS doesn't signal an intrusion by  $\beta_1$ , and the probability that it goes to court absent the signal by  $\beta_2$ ; the firm simply recovers damages with residual probabilities  $1-\alpha_1-\alpha_2$  and  $1-\beta_1-\beta_2$ . Figure 3-4 below summarizes the modified game tree.

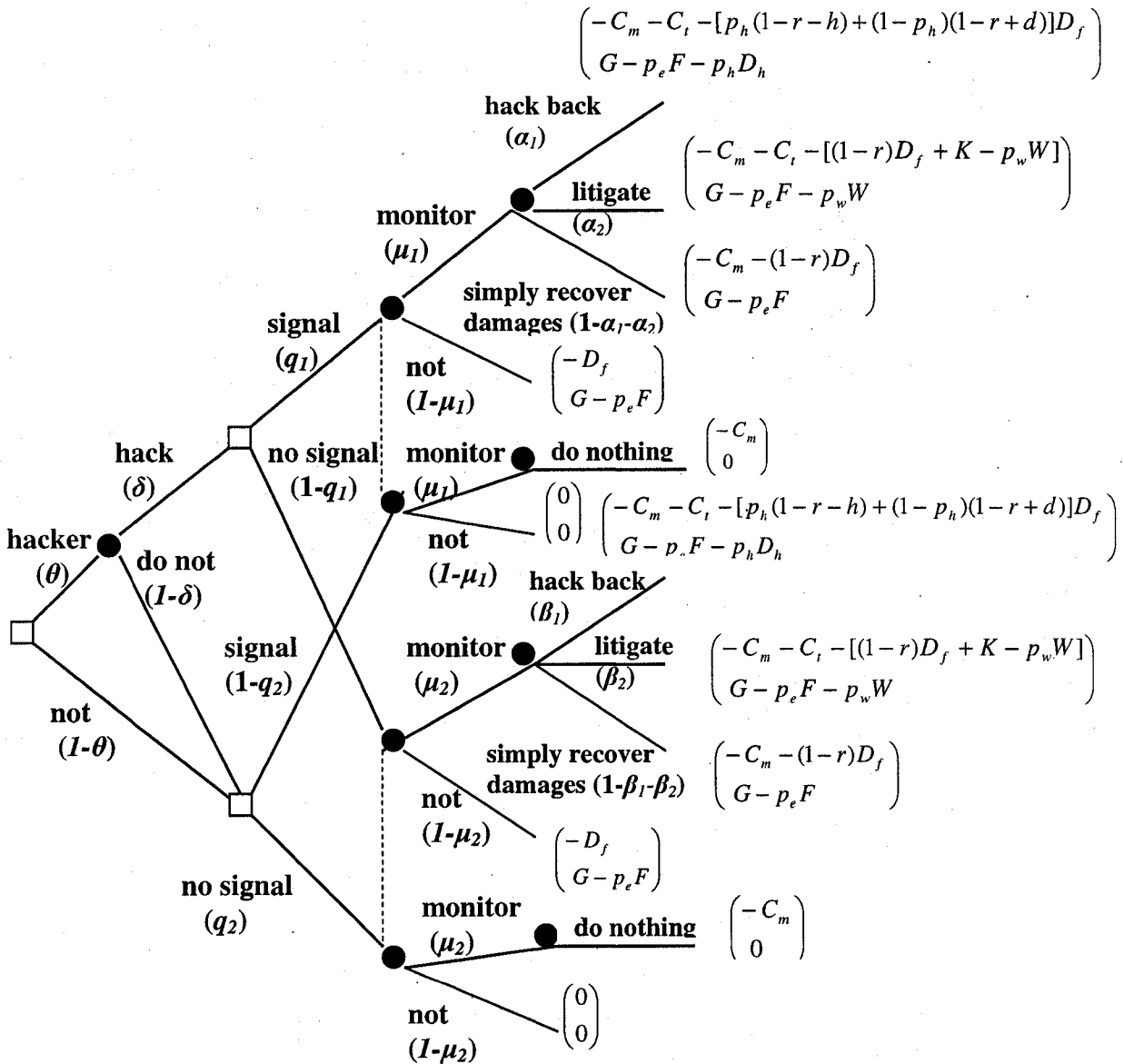


Figure 3-4. Game tree, IDS case

With the IDS, the basic model in Section 2 is modified to include Bayesian updating of the firm's information as to the probability of intrusion in its computer network. The expected pay-off for the hacker and the firm in this set up are thus:

$$H(\mu_1, \mu_2, \alpha_1, \alpha_2, \beta_1, \beta_2, \delta) \equiv \delta \left[ \begin{array}{l} G - p_e F - q_1 \mu_1 (\alpha_1 p_h D_h + \alpha_2 p_w W) \\ - (1 - q_1) \mu_2 (\beta_1 p_h D_h + \beta_2 p_w W) \end{array} \right] \quad (3-7)$$

$$F(\mu_1, \mu_2, \alpha_1, \alpha_2, \beta_1, \beta_2, \delta) \equiv [q_1 \theta \delta + (1 - q_2)(1 - \theta \delta)] F_s + [(1 - q_1) \theta \delta + q_2(1 - \theta \delta)] F_n \quad (3-8)$$

where  $F_s$ , the pay-off to the firm in the signal state, is equal to

$$F_s(\mu_1, \alpha_1, \alpha_2, \delta) \equiv -\mu_1 C_m - \eta_1 \mu_1 (\alpha_1 + \alpha_2) C_i - \eta_1 (1 - \mu_1) D_f - \eta_1 \mu_1 \left\{ \begin{array}{l} \alpha_1 [p_h (1 - r - h) D_f + (1 - p_h)(1 - r + d) D_f] \\ + \alpha_2 [(1 - r) D_f + K - p_w W] \\ + \eta_1 (1 - \alpha_1 - \alpha_2)(1 - r) D_f \end{array} \right\} \quad (3-9)$$

and  $F_n$ , the pay-off to the firm in the non-signal states, is equal to:

$$F_n(\mu_2, \beta_1, \beta_2, \delta) \equiv -\mu_2 C_m - \eta_2 \mu_2 (\beta_1 + \beta_2) C_i - \eta_2 (1 - \mu_2) D_f - \eta_2 \mu_2 \left\{ \begin{array}{l} \beta_1 [p_h (1 - r - h) D_f + (1 - p_h)(1 - r + d) D_f] \\ + \beta_2 [(1 - r) D_f + K - p_w W] \\ + (1 - \beta_1 - \beta_2)(1 - r) D_f \end{array} \right\} \quad (3-10)$$

$$\text{and where } \eta_1 = \Pr(\text{intrusion} | \text{signal}) = \frac{q_1 \theta \delta}{q_1 \theta \delta + (1 - q_2)(1 - \theta \delta)}$$

$$\text{and } \eta_2 = \Pr(\text{intrusion} | \text{no signal}) = \frac{(1 - q_1) \theta \delta}{(1 - q_1) \theta \delta + q_2 (1 - \theta \delta)}$$

Thus,

$$\frac{\partial F}{\partial \mu_1} = [q_1 \theta \delta + (1 - q_2)(1 - \theta \delta)] \left\{ -C_m + \eta_1 \begin{pmatrix} -(\alpha_1 + \alpha_2)C_t \\ + \alpha_1 [p_h h - (1 - p_h)d] D_f \\ + \alpha_2 [p_w W - K] \\ + rD_f \end{pmatrix} \right\} \quad (3-11)$$

$$\frac{\partial F}{\partial \alpha_1}(\delta) = [q_1 \theta \delta + (1 - q_2)(1 - \theta \delta)] \eta_1 \mu_1 \{-C_t + [p_h h - (1 - p_h)d] D_f\} \quad (3-12)$$

$$\frac{\partial F}{\partial \alpha_2}(\delta) = [q_1 \theta \delta + (1 - q_2)(1 - \theta \delta)] \eta_1 \mu_1 \{-C_t + [p_w W - K]\} \quad (3-13)$$

$$\frac{\partial F}{\partial \mu_2} = [(1 - q_1) \theta \delta + q_2(1 - \theta \delta)] \left\{ -C_m + \eta_2 \begin{pmatrix} -(\beta_1 + \beta_2)C_t \\ + \beta_1 [p_h h - (1 - p_h)d] D_f \\ + \beta_2 [p_w W - K] \\ + rD_f \end{pmatrix} \right\} \quad (3-14)$$

$$\frac{\partial F}{\partial \beta_1} = [(1 - q_1) \theta \delta + q_2(1 - \theta \delta)] \eta_2 \mu_2 \{-C_t + [p_h h - (1 - p_h)d] D_f\} \quad (3-15)$$

$$\frac{\partial F}{\partial \beta_2} = [(1 - q_1) \theta \delta + q_2(1 - \theta \delta)] \eta_2 \mu_2 \{-C_t + [p_w W - K]\} \quad (3-16)$$

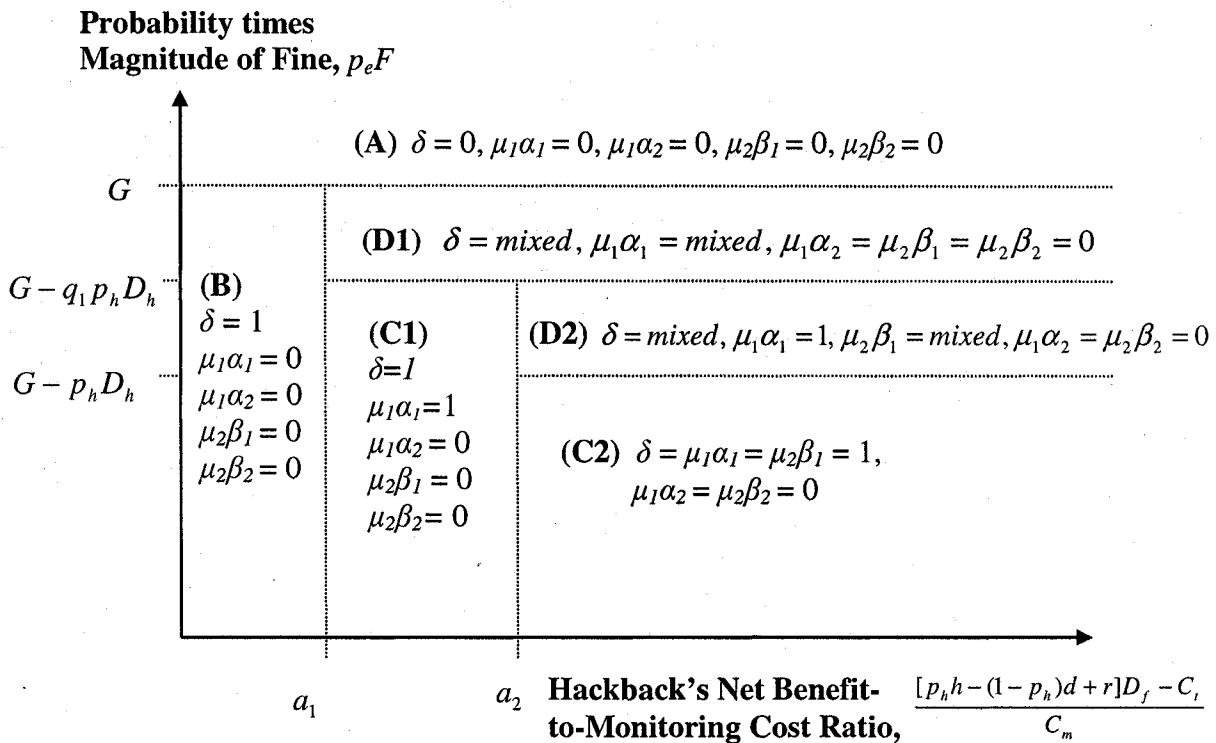
$$\frac{\partial H}{\partial \delta} = G - p_e F - q_1 \mu_1 (\alpha_1 p_h D_h + \alpha_2 p_w W) - (1 - q_1) \mu_2 (\beta_1 p_h D_h + \beta_2 p_w W). \quad (3-17)$$

Thus, with this new IDS set-up, the firm has to consider strategy for two cases: (a) when the IDS signals an intrusion; and (b) when the IDS does not signal an intrusion.<sup>172</sup> Proposition 3-3 below presents the case where litigation is not beneficial whether or not the IDS signals an intrusion, while Proposition 3-4 (which covers situations where litigation is beneficial in both the signal and non-signal states) and Proposition 3-5

<sup>172</sup> Even when the IDS does not signal an intrusion, since IDS signals are imperfect, there may be an actual intrusion taking place but the IDS does not detect it. Hence, it may still be beneficial for the firm to spend monitoring/trace costs even if the IDS does not signal an intrusion so that in the (unlikely) event that there is an intrusion, it can still react with countermeasures.

(which contemplates cases where litigation is beneficial when the IDS signals an intrusion, but not otherwise) are presented in Section 8.

**Proposition 3-3.** When  $p_w W - K < C_l$ , litigation is not beneficial irrespective of whether or not the IDS signals an intrusion, and the following Bayesian Nash equilibria obtain:



**Figure 3-5.** Nash equilibria when litigation is not beneficial (IDS available)

In general, the firm will counter-strike with a higher probability when the IDS signals an intrusion than when it does not. Thus, in region C1, the firm hacks back when the IDS sends a signal and does not hack back when the IDS does not signal an intrusion. Also, as Region D1, for example, illustrates, the probability of hacking back is greater when the IDS signals an intrusion than in the previous case when IDS was not available. So too,

the firm hacks back with less frequency when the IDS does not signal an intrusion compared to the previous no-IDS case.<sup>173</sup>

The intuition behind these results is that with the IDS, the firm's information as to the probability of intrusion is updated using Bayes' rule. The IDS thus enables the firm to have better information as to whether or not its systems are under attack.<sup>174</sup> Better information in turn enables an organization to better identify an imminent danger so as to determine if the proper self-help response is a defensive one or a more pro-active one.<sup>175</sup> The IDS thus allows the firm to fine-tune its strategy and be more efficient with its hackback/litigation response (see also Cavusoglu, Mishra, and Raghunathan 2005). The better the IDS configuration (that is, the lower the false positives and false negatives), the more efficient the firm's hackback/litigation strategy will be, and hackback's effectiveness as a cybercrime countermeasure increases.

## 4. SOCIALLY-OPTIMAL SOLUTION

### 4.1 The Social Planner's Problem

In Sections 2 and 3, we considered the (firm's) private solution to the hackback game. Since the private and socially-optimal solutions can diverge, analyzing the firm's behavior alone would not suffice to shed light on the optimality of hackback. In this

---

<sup>173</sup> That is,  $\alpha_1 > \sigma_1 > \beta_1$ .

<sup>174</sup> Thus, as Lemma 3-4 in the Appendix shows, under reasonable IDS configurations, the probability that an actual intrusion exists given that the IDS signals an intrusion,  $\eta_I$ , is greater than the (a priori) probability of an intrusion,  $\delta$ . (Equivalently, this implies that the probability of no intrusion given an IDS signal is lesser than the a priori probability of an intrusion.)

<sup>175</sup> For example, in the case of cyberterrorism or information warfare, if there is highly reliable information about a forthcoming major attack on the cyber-infrastructure where lives may be at risk, crippling the enemy's computer systems might be the best response.

section, we consider the perspective of the social planner in order to analyze whether permitting hackback would be beneficial to society or not.

In contrast to the firm, the social planner takes into account the total pay-off to all members of society (the hacker, the firm, and the third party):<sup>176</sup>

$$\begin{aligned}
 \text{Max } S = & -\mu C_m - \theta \delta \mu (\sigma_1 + \sigma_2) C_i - \theta \delta (1 - \mu) D_f \\
 & - \theta \delta \mu \left\{ \begin{aligned} & \sigma_1 [p_h (1 - r - h) D_f + (1 - p_h) (1 - r + d) D_f] \\ & + \sigma_2 [(1 - r) D_f + K - p_w W] \\ & (1 - \sigma_1 - \sigma_2) (1 - r) D_f \end{aligned} \right\} \\
 & + \delta [G - p_e F - \mu \sigma_1 p_h D_h - \mu \sigma_2 p_w W]
 \end{aligned} \tag{3-18}$$

The hacker's optimization problem is

$$\text{Max } \delta [G - p_e F - \sigma_1 \mu p_h D_h - \mu \sigma_2 p_w W]. \tag{3-19}$$

Thus,

$$\frac{\partial S}{\partial \mu} = -C_m + \theta \delta \left\{ \begin{aligned} & -(\sigma_1 + \sigma_2) C_i \\ & + \sigma_1 [p_h h - (1 - p_h) d] D_f + \\ & \sigma_2 [p_w W - K] \\ & + r D_f \end{aligned} \right\} - \delta [\sigma_1 p_h D_h + \sigma_2 p_w W] \tag{3-20}$$

$$\frac{\partial S}{\partial \sigma_1} = -\theta \delta \mu C_i + \theta \delta \mu [p_h h - (1 - p_h) d] D_f - \delta \mu p_h D_h \tag{3-21}$$

$$\frac{\partial S}{\partial \sigma_2} = -\theta \delta \mu C_i + \theta \delta \mu [p_w W - K] - \delta \mu p_w W \tag{3-22}$$

<sup>176</sup> Here, we are following the standard practice in the law and economics literature of treating the thief's utility as part of the social accounting (for example, Becker [1968] and Shavell [1991]). In this particular case, it makes much sense to include the hacker's computing resources as part of the total assets available to the society, since damages to the hacker's system are damages to the available total resources available to society. As such, since there are opportunity costs associated with the destruction of such assets, the social planner rightfully includes such assets in its social calculations, thereby resulting in the conclusion that such assets need to be protected as well, say, from wanton destruction by the counter-striker.



$$\frac{\partial H}{\partial \delta} = G - p_e F - \mu \sigma_1 p_h D_h - \mu \sigma_2 p_w W. \quad (3-23)$$

As before, the first and second term represent, respectively, the cost of tracking the hacker and the net cost to the firm of the three alternatives (that is, the hackback, litigation, and simply-recover-damages strategies). The third term is new and represents the net pay-off to the hacker. (The net pay-off of the third party is zero, since he/she is reimbursed by the firm for whatever damages he/she will suffer.<sup>177</sup>)

From equation (3-22), we know that  $\frac{\partial S}{\partial \sigma_2} < 0$ , which implies that the social planner will never litigate because from the social planner's perspective, litigation will result in court and trace costs without any corresponding net social gain (since the amount awarded by the court constitute a mere transfer from the hacker to the firm). Consequently, for the social planner, litigation is never beneficial. Hence, its Nash equilibria would be:

---

<sup>177</sup> If counter-strikers are not held liable for these damages, the total societal pay-off would be:

$$S = -\mu C_m - \theta \delta \mu (\sigma_1 + \sigma_2) C_t - \theta \delta (1 - \mu) D_f - \theta \delta \mu \left\{ \begin{array}{l} \sigma_1 [p_h (1 - r - h) D_f + (1 - p_h) (1 - r) D_f] \\ + \sigma_2 [(1 - r) D_f + K - p_w W] \\ (1 - \sigma_1 - \sigma_2) (1 - r) D_f \end{array} \right\} \\ + \delta [G - p_e F - \mu \sigma_1 p_h D_h - \mu \sigma_2 p_w W] - \theta \delta \mu (1 - p_h) d D_f,$$

which will reduce to essentially the same pay-off as the above case where firms are held liable for third-party damages. Thus, the socially-optimal Nash equilibria would be the same regardless of whether the property right is assigned to the hacker or the third party.

Probability times  
Magnitude of Fine,  $p_e F$

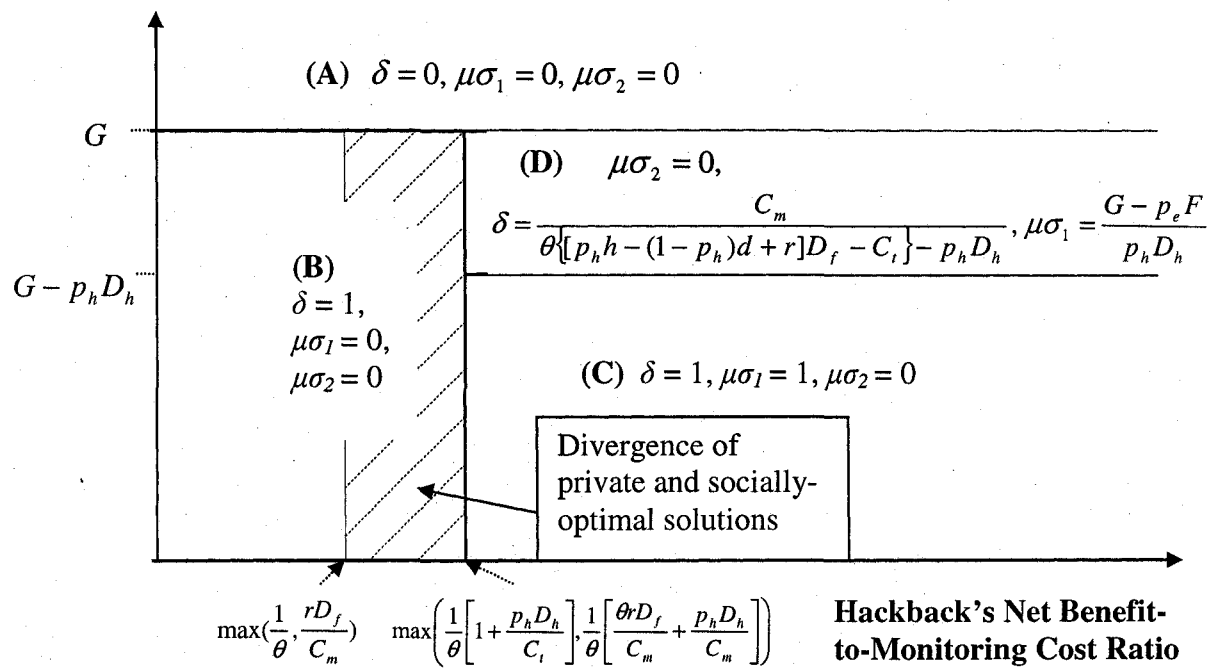


Figure 3-6. Nash equilibria of the social planner's problem

By comparing the Nash equilibria of the social planner's problem with that of the firm's solution, we can see the divergence between the private incentive to hack back and the socially-optimal level of hackback. Thus, from the shaded region above, we can see that the firm has an incentive to engage in excessive hackback. This is because the firm does not take into consideration the damage to the hacker's systems in its decision to hack back while the social planner views such damages as losses to society.

We thus think that hackback must be regulated in order to steer the firm's behavior closer towards the socially-optimal solution. The law, for one, should require that in conducting hackback, firms must exert efforts not to wantonly destroy the digital assets

of the hacker.<sup>178</sup> In Section 6, we discuss how the law on self-defense in cyberspace should be written.

#### 4.2. The Optimality of Hackback

If hackback were to be for the good of society, it must be the case that the overall social welfare is higher when hackback is allowed, compared to the case when it is not. Hence, we compare here the societal welfare under both regimes by calculating the total societal pay-off across the different regions of the Nash equilibria under both regimes.

If hackback is not available, the social planner's and the hacker's optimization problem reduces to, respectively:

$$\begin{aligned} \text{Max } S = & -\mu C_m - \theta \delta \mu \sigma_2 C_t - \theta \delta (1 - \mu) D_f \\ & - \theta \delta \mu \left\{ \begin{array}{l} \sigma_2 [(1 - r) D_f + K - p_w W] \\ (1 - \sigma_2) (1 - r) D_f \end{array} \right\} \\ & + \delta [G - p_e F - \mu \sigma_2 p_w W] \end{aligned} \quad (3-25)$$

$$\text{Max } \delta [G - p_e F - \mu \sigma_2 p_w W]. \quad (3-26)$$

Thus,

$$\frac{\partial S}{\partial \sigma_2} = -\theta \delta \mu C_t + \theta \delta \mu [p_w W - K] - \delta \mu p_w W < 0 \Rightarrow \sigma_2 = 0 \quad (3-27)$$

$$\frac{\partial S}{\partial \mu} = -C_m - \theta \delta \sigma_2 C_t + \theta \delta \sigma_2 [p_w W - K] - \delta \sigma_2 p_w W < 0 \text{ (given } \sigma_2 = 0) \quad (3-28)$$

$$\frac{\partial H}{\partial \delta} = G - p_e F - \mu \sigma_2 p_w W = G - p_e F. \quad (3-29)$$

---

<sup>178</sup> Cf. Augustine (400): war must be waged not for "love of violence, revengeful cruelty, fierce and implacable enmity, wild resistance, and the lust of power and such like"; see also, Grotius (1625) on the necessity and proportionality of the force used.

As in the case where hackback is available,  $\frac{\partial S}{\partial \sigma_2} < 0$  implies that the social planner will

never find litigation beneficial (for the same reasons aforementioned). Given that

equilibrium  $\sigma_2$  equals zero,  $\frac{\partial H}{\partial \delta} = G - p_e F$ . This implies that the Nash equilibria has

simply two regions: one is the region where  $p_e F$  is above  $G$  where  $\delta = 0$  and  $\mu \sigma_2 = 0$ ,

and the other is the region where  $p_e F$  is below  $G$  in which case,  $\delta = 1$  and  $\mu \sigma_2 = 0$ .

Substituting in for the optimal solutions, the total pay-off to society when hackback is allowed is:

$$\begin{aligned}
 S^* = & -\mu^* C_m - \theta \delta^* \mu^* \sigma_1^* C_t - \theta \delta^* (1 - \mu^*) D_f \\
 & - \theta \delta^* \mu^* \left\{ \begin{aligned} & \sigma_1^* [p_h (1 - r - h) D_f + (1 - p_h) (1 - r + d) D_f] \\ & + (1 - \sigma_1^*) (1 - r) D_f \end{aligned} \right\} \\
 & + \delta^* [G - p_e F - \mu^* \sigma_1^* p_h D_h]
 \end{aligned} \tag{3-30}$$

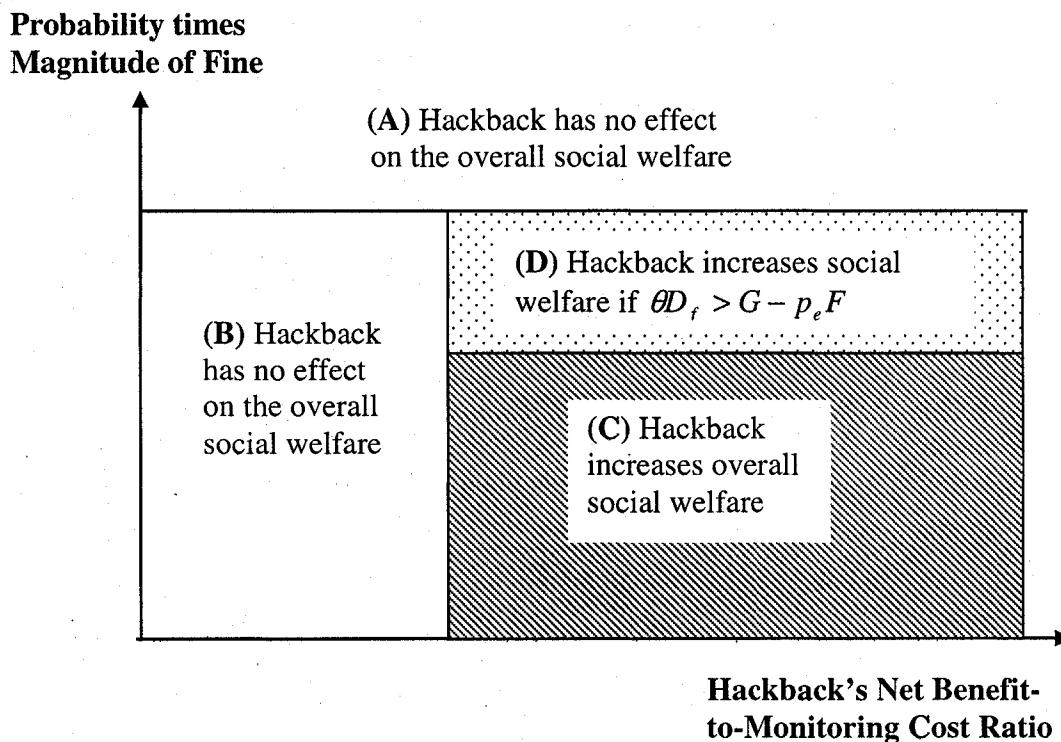
while the social pay-off under the scenario where hackback is not allowed is:

$$S^{**} = -\mu^{**} C_m - \theta \delta^{**} (1 - \mu^{**}) D_f - \theta \delta^{**} \mu^{**} [(1 - r) D_f] + \delta^{**} [G - p_e F] \tag{3-31}$$

By comparing these two pay-offs across the different regions of the Nash equilibrium solutions, we can calculate the difference in the social welfare in the case where hackback is available vis-à-vis the case where it is not, and conclude if hackback is beneficial to society or not.

Figure 3-7 below summarizes the social welfare comparisons between the two cases. In region A, since the hacker never hacks and the social planner never hacks back, the two cases – (a) hackback available and (b) hackback not available – have similar pay-offs. In region B, cases (a) and (b) again have similar pay-offs. In region C, if hackback

is available, the societal pay-off is (see Section 8 for the detailed social welfare calculations)  $-C_m - \theta C_i + \theta \{ [p_h h + (1 - p_h) d] D_f - (1 - r) D_f \} + [G - p_e F - p_h D_h]$ . If, on the other hand, hackback is not available, the societal pay-off is  $-\theta D_f + [G - p_e F]$ . Hence, the net difference between the societal pay-offs of these two cases is  $-C_m + \theta \{ [p_h h - (1 - p_h) d + r] D_f - C_i \} - p_h D_h$ , which is positive in the region. Hence, hackback is “good” for society in region C. Finally, in region D, the net difference between the payoff where hackback is available and the case where hackback is not available, after manipulations, reduces to  $(1 - \delta) \cdot \{ \theta D_f - [G - p_e F] \}$ , a positive number whenever  $\theta D_f > [G - p_e F]$ . That is, in region D, hackback is good for society whenever the expected net social waste from hacking,  $\theta D_f - (G - p_e F)$ , is positive.



**Figure 3-7.** Hackback vs. no hackback social welfare comparisons

## 5. PROPER LIABILITY RULE FOR DAMAGES TO INNOCENT THIRD PARTIES

In order to successfully trace the hacker back, the firm in many instances has to pass through several layers of other computers.<sup>179</sup> Two legal questions thus arise in these situations:

- (1) Are traceroutes (passing through third party computers) actionable trespass?
- (2) Should active defenders be held liable for damages to third party computers?

On the first question, we think that passing through third party computers constitute merely *de minimis* encroachment. It can also be argued traceroutes fall under “harmless intermeddlings with chattel” under Section 218 Comment e of the *Restatement (Second) of Torts*,<sup>180</sup> and thus, like “electromagnetic transmissions[,] are not actionable as trespasses ... unless they cause physical damage to the real property” (*Hamidi*, 71 P.3d,

---

<sup>179</sup> These third-party computers which were compromised by the hacker (“zombies”) can be used to launch attacks against other systems, as in the case of DDoS attacks (see Kesan and Majuca 2005).

<sup>180</sup> Section 218 Comment e of the *Restatement* provides:

“The interest of a chattel in its inviolability, unlike in the similar interest of a possessor of land, is not given legal protection by an action for nominal damages for harmless interferences with a chattel. In order that an actor who interferes with another’s chattel may be liable, his conduct must affect some other and more important interest of the possessor. Therefore, one who intentionally intermeddles with another’s chattel is subject to liability only if his intermeddling is harmful to the possessor’s materially valuable interest in the physical condition, quality, or value of the chattel, or if the possessor is deprived of the use of the chattel for a substantial time, or some other legally protected interest of the possessor is affected as stated in Clause (c) [relating to the deprivation of chattel’s use for a substantial time]. Sufficient legal protection ... of this chattel is afforded by his privilege to use reasonable force to protect his possession against even harmless interference.” (American Law Institute 1965, sec. 218)

Several court decisions have extended this trespass to chattel tort to Internet cases. See, for example, the case of *Hamidi*, 71 P.3d 296 where the Supreme Court of California ruled that emails by a disgruntled employee to other employees criticizing Intel’s employment practices did not constitute actionable trespass to Intel’s servers and computer systems, and that harmless interference to chattels are not actionable (but see Epstein [2005]’s disagreement with the decision). See also *CompuServe Incorporated v. Cyber Promotions, Inc.*, 962 F. Supp. 1015 [1997]; *Thrifty-tel, Inc. v. Bezenek*, 46 Cal. App. 4<sup>th</sup> 1559 [1996]). For a discussion on the debate on the appropriateness of the application of the trespass to chattel tort to computer cases, see generally McGowan (2005).

at 309). As is settled, only trespass that actually cause harm or damage to chattel are actionable (*Hamidi*, 71 P.3d, at 302).<sup>181</sup>

There is also good economic reason for not holding traceroutes as actionable trespass. Private necessity usually constitutes an exception to the general rule against trespass because emergencies give rise to transaction costs that preclude bargaining between the parties (Cooter and Ulen 1997, p. 137). For example, a boat caught in a storm could moor on someone else's private pier (*Ploof v. Putnam*, 81 Vt. 471, 71A. 188 Supreme Court of Vermont 1908). Under the same principle, it would be unreasonable to ask a firm under attack to negotiate first with the third parties. Of course, the privilege of compromised "zombies" to employ self-help measures (for example, by stopping trespass to its networks) should also be available to those in the line of traceroute, under Section 218, Comment e of the Restatement (*CompuServe*, 962 F.Supp. at 1024).

On the second question, we assumed in our model in Section 2 that counter-strikers are liable for third-party damages. If, instead, they are not, their pay-off would be:

$$F(\mu, \sigma_1, \sigma_2, \delta) \equiv -\mu C_m - \theta \delta \mu (\sigma_1 + \sigma_2) C_t - \theta \delta (1 - \mu) D_f - \theta \delta \mu \left\{ \begin{array}{l} \sigma_1 [(1-r)D_f - p_h h D_f] \\ + \sigma_2 [(1-r)D_f + K - p_w W] \\ + (1 - \sigma_1 - \sigma_2)(1-r)D_f \end{array} \right\} \quad (3-32)$$

Thus:

---

<sup>181</sup> An example of trespass that cause harm is spam, which burdens the computing system and therefore constitutes *actionable* trespass to chattel (see *CompuServe*, 962 F. Supp. 1015. See also *Thrifty-tel*, 46 Cal. App. 4<sup>th</sup> 1559 (unauthorized access by a hacker of the plaintiff's telephone service constitutes an actionable tort).

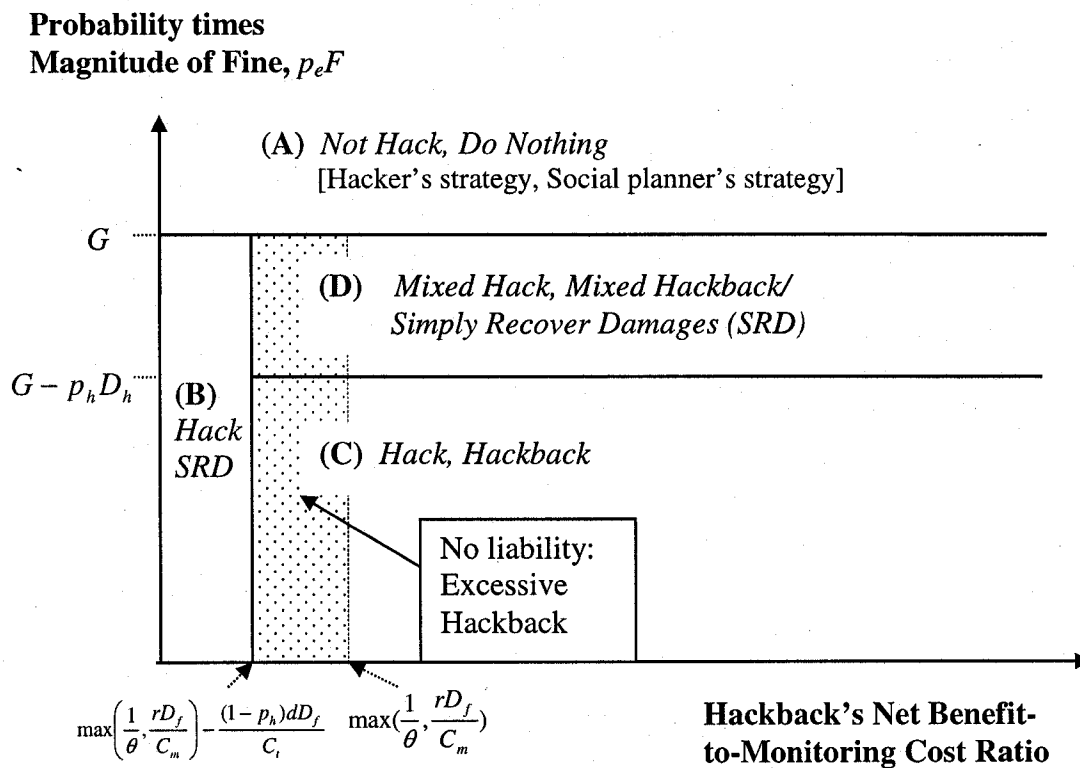
$$\frac{\partial F}{\partial \mu} = -C_m - \theta\delta(\sigma_1 + \sigma_2)C_t + \theta\delta \left\{ \begin{array}{l} \sigma_1[p_h h]D_f \\ + \sigma_2[p_w W - K] \\ + rD_f \end{array} \right\} \quad (3-33)$$

$$\frac{\partial F}{\partial \sigma_1} = -\theta\delta\mu C_t + \theta\delta\mu[p_h hD] \quad (3-34)$$

$$\frac{\partial F}{\partial \sigma_2} = -\theta\delta\mu C_t + \theta\delta\mu[p_w W - K] \quad (3-35)$$

$$\frac{\partial H}{\partial \delta} = G - p_e F - \mu[\sigma_1 p_h D_h + \sigma_2 p_w W] \quad (3-36)$$

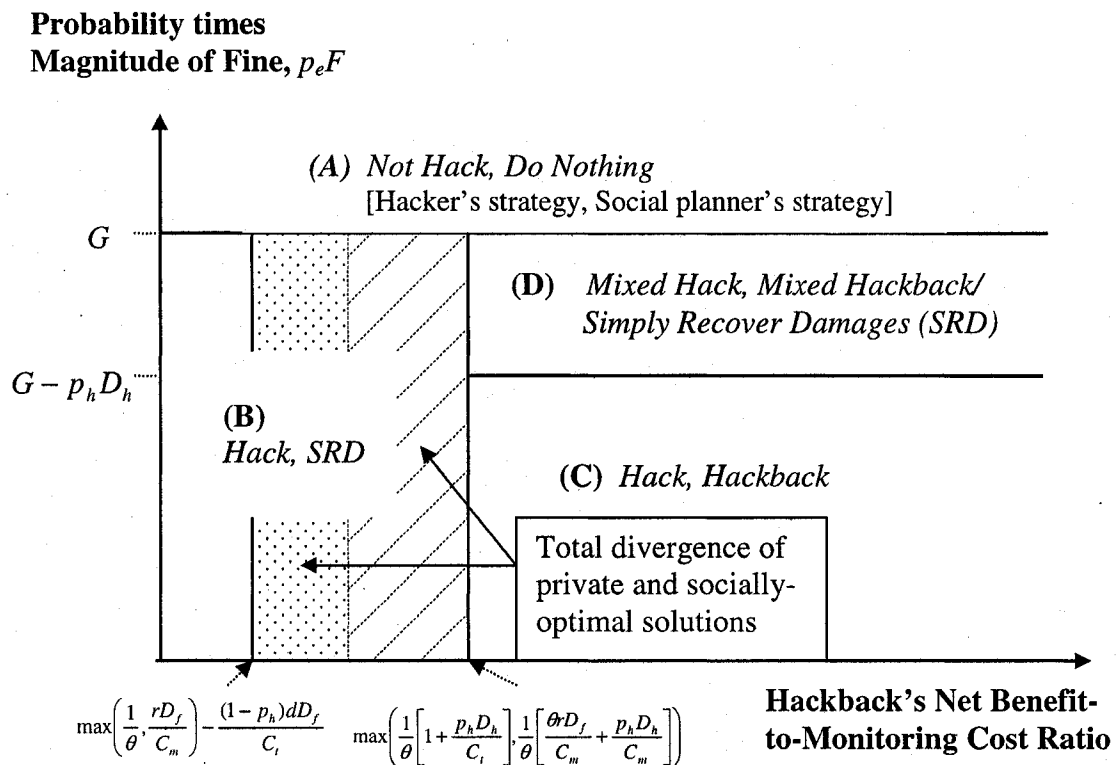
and the Nash equilibria would be:



**Figure 3-8.** Nash equilibria of the firm's problem  
(No liability rule)



Figure 3-8 shows that, *not* holding counterstrickers liable for third party damages would cause a distortion that compounds the wedge already caused by the firm not incorporating the damage to the hacker's systems into its cost-benefit calculations (Figure 3-6). With both these distortions, the overall divergence of the private and socially-optimal solutions would be larger, as depicted in Figure 3-9.



**Figure 3-9.** Divergence of private and socially-optimal equilibria

Thus, not holding firms liable for third-party damages would exacerbate the inefficiency of the *laissez-faire* hackback regime. Hence, there will now be two distortions that cause the private solution to diverge away from the socially-optimal solution: (a) the fact that the damage to the hacker's system are social losses not considered by the firm (striped lines), and (b) the fact that the damage to third parties are

social losses not internalized by active defenders (dotted lines). Thus, our model shows that liability rules for third-party damages function like an “invisible hand” guiding the private solution closer to the socially-optimal solution.

On top of liability rules, however, regulations are still needed to handle the other distortion. Besides, even if third-party liability rules are present, several “frictions” could cause a wedge between the efficient amount of hackback and the actual amount hackback (see Figure 3-10 below for the Nash equilibria when these frictions are present). For example, several of those caught in the line of crossfire are likely to not have enough computer sophistication to even detect that their systems have been hit.<sup>182</sup> (This also brings in redistributive issues, since smaller and poorer sectors are more likely not to detect they suffered collateral damages.<sup>183</sup>) Also, others may decide not to sue given the transaction costs involved with going to court.<sup>184</sup> Because of these concerns, liability rules for damage caused to third parties, in and of themselves, may not be enough to generate the optimal outcome. Consequently, on top of having liability rules, regulations establishing criteria and guidelines for valid hackback should be set in order to constrain the parties closer to the socially-optimal outcome.

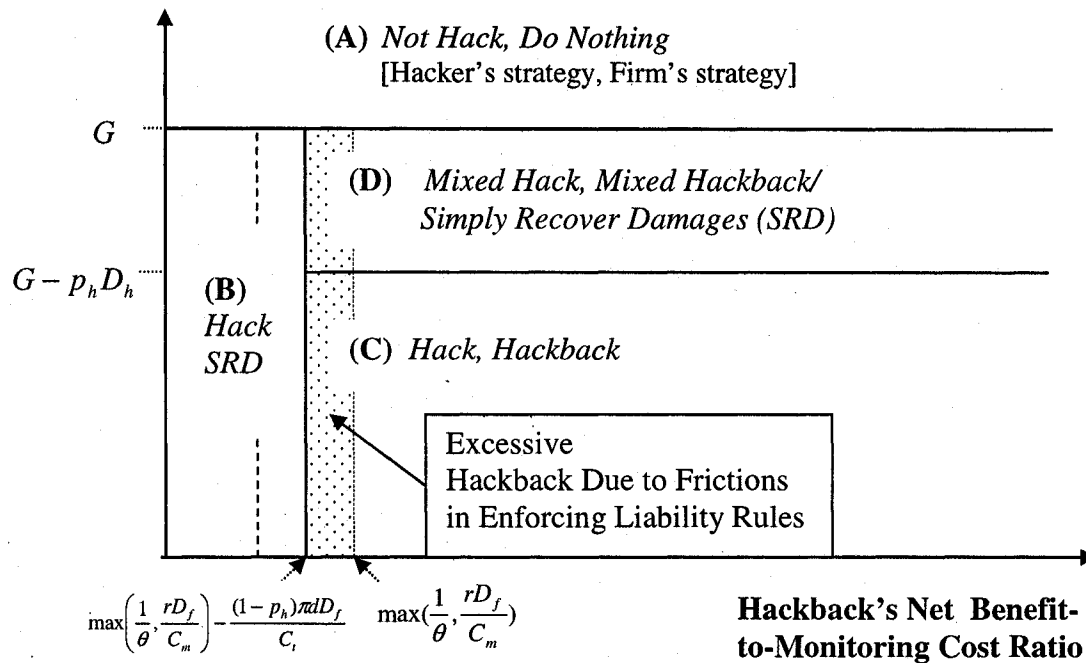
---

<sup>182</sup> We thank George Deltas for bringing up this point.

<sup>183</sup> See also Katyal (2005): “If only the more wealthy can afford the private protection strategies (for example, car alarms, The Club, and the like), then they will be able to drive while the poor will not. Criminal law exists, in part, as a subsidy to poorer elements in a community. If everyone had to fend for themselves to prevent crime, the richer ... would be able to .. [spill over] some of the crime onto their poorer neighbors. ... private precautions cost money, and to expect those with less in society to bear a greater share of crime can offend notions of distributional justice.” However, as Smith (2005) points out, “[if] wrongdoers did not know that a [hackback] system was in place, they might actually decide to reduce their law-breaking .. like the Lojack system [which are] effective and hidden security measure [that are] a form of ‘positive externality-generating unobservable self-protection’ [in the sense of Ayres and Levitt (1998)].”

<sup>184</sup> Also, the damage may be *de minimis*, in which case resort to courts may not be available (see Epstein 2005).

Probability times  
Magnitude of Fine,  $p_e F$



**Figure 3-10.** Nash equilibria of the firm's problem  
(Due to frictions in enforcing liability rules, only a fraction  $1-\pi$  goes to court)

## 6. WHAT THE LAW ON SELF-DEFENSE IN CYBERSPACE SHOULD BE

Given the results of the model, we are now ready to formulate what the law on self-defense in cyberspace ought to be.

First and foremost, we do not see any overriding reason why the law should outright deny firms the right to exercise self-defense in cyberspace (see, for example, equilibria C and D of Figure 3-7 where the availability of hackback increases the social welfare).

Although the general stance of the law has been not to allow retaliation, in many cases in the Internet, however, police enforcement is ineffective because of the speed by which attacks cause grave damage, and because hackers can hide in places outside the jurisdiction of countries with active enforcement against hacking. With the time and

expense associated with court-administered remedies, the availability of self-help could provide an equitable solution (Brandon et al. 1984, pp. 869-70). Also, as previously mentioned (see *supra* text accompanying note 147), the law in fact allows the use of self-defense in other areas such as the use of reasonable force in self-defense or in defense of property in criminal law (see American Law Institute [1985], secs. 3.04 and 3.06), to recovery of property in tort law.<sup>185</sup> Lastly, by deterring criminals, active defense can supplement law enforcement: once precedents of hackers experiencing damage from counterstrike are established, a large number of script kiddies would vanish (see discussions in Section 2.3 on the deterrent effect of hackback). In sum, we think that absent the showing of widespread misuse, active defense should not be outlawed at the outset (see also Epstein 2005).

Secondly, counterstrikes can, however, function as a wrong against innocent third parties and what passes as self-defense may in reality be another wrong. Similarly, self-help though originally justified can bring about several harmful results.<sup>186</sup> Thus, in order that the right of self-defense should not be abused, we think that reasonableness standards must be instituted and resort to legal remedies prescribed when the planned counteractions fall outside their boundaries (Epstein 2005). Hence, in our view, the law should

---

<sup>185</sup> In fact, even in the law of self-defense among nations, the general stance of international law is that nations should “refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state” (Charter of the United Nations, Art. 2[4]), but that “[n]othing in the [UN] Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a [member nation], until the Security Council has taken measures necessary to maintain international peace and security.” (Charter of the United Nations, Art. 51) (see also *Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S.)*, Jurisdiction and Admissibility, 1984 ICJ REP. 392 June 27, 1986)

<sup>186</sup> The standard litany of criticisms of hackback include misidentification problems, use of automated program by counter-strikers, shooting matches between trigger-happy defenders and intruders, self-proclaimed “white hats” releasing worm patches with good intention but with terrible results, etc. (see, for example, Katyal 2005).

in some instances allow (though not require) resort to self-help remedies, yet at the same time regulate the exercise of the privilege so as to check against its potential abuse.

This is where we differ from Himma (2004), Kerr (2005) and Katyal (2005) in that while we recognize that excesses and abuses can potentially occur, for us, this does not necessarily mean that the privilege of self-defense should be denied outright. Given the potential benefits self-help can generate when used responsibly, we think that regulating the exercise of the privilege is the best way to deal with these potential excesses.

Based on our model results, the governing regulation on self-defense in cyberspace should have the following features:

(1) Attacked firms and individuals can hack back if, and only if, the following requirements are satisfied:

(a) Hackback does not result in greater harm to innocent parties compared to the damage to the defender's systems that is sought to be mitigated. Furthermore, due care should be exercised to avoid or minimize damage to third parties and the purpose of the hackback should be limited to the prevention of damage to the firm's information technology infrastructure.

(b) Recourse to other alternatives is either ineffective or impractical. In particular, this occurs when:

(i) police enforcement is ineffective. Lemmas 3-1 and 3-3 show that effective criminal law enforcement provides wide-ranging deterrence against cybercrimes and does away with the need for counterstrikes or civil litigation.

(ii) litigation is impractical (see discussions in Sections 2.3 and 2.4).

(iii) a more defensive strategy, such as simply recovering damages or simply dropping incoming packets, would not deter the hacker.

In short, active defense is an extraordinary remedy, available only when other alternatives are ineffective or impractical.

(c) There is a serious prospect of success. There must be a relatively high chance of hitting the hacker, instead of hitting innocent persons. Thus, reasonable effort must be exerted to employ state-of-the-art traceback technology.

(d) Reasonable effort must be exerted to employ good IDS technology. This helps the firm to more carefully ascertain the existence or the imminence of the attack/danger; it also decreases the error of hitting innocent persons; and enhances the deterrent effect of hackback (see Section 3).

If a firm hacks back without these conditions being present, it oversteps the bounds for reasonable exercise of self-defense in cyberspace. The law can hold those who exercise self-help not in a legally permissible manner, liable for penalties.

(2) Even if those preconditions are present – and thus the exercise of the privilege is justified – the conduct *during* hackback must also be regulated by the law:

(a) In order to internalize the damage to third parties, active defenders should be held liable to third parties caught in the crossfire. Not holding active defenders responsible for the consequences of their action will result in externalities and excessive amount of hackback activity (see Figure 3-8).<sup>187</sup>

---

<sup>187</sup> We have also looked at the issue of notifying the third party of the hackback action and conclude that though notifying potential third party victims is a valid concern, there are probably other alternative ways of informing them other than through public registry. One concern about registration is that the attacked firm's reputation could suffer with the publication that it was hacked, which could negatively affect its revenue and stock prices. For instance, a Boeing senior info security officer we have talked to informed us that their company's hackback decision involves a team of senior officers (including marketing) and not

(b) Counter-strikers must also use only “proportionate force”, that is, they must not wantonly damage the hackers’ digital systems out of retaliation, but rather, only use force that is necessary to avoid damage to their own systems (see Figure 3-6).

In sum, the law needs to layer liability rules on top of the reasonableness conditions.

Thus, our proposed law of self-defense in cyberspace clearly prohibits retaliation<sup>188</sup> or vigilante justice. For this reason, we think that Symbiot, Inc.’s “asymmetric responses”<sup>189</sup> would most likely fall outside the scope of what we consider legitimate

---

just an information security officer decision, because of the concern that hacking back might give the impression that their IT systems are insecure. If attacked firms are required to register, such concern for the firm’s reputation could result in them not hacking back at all, and thus hackback will be “underprovided”. Thus, an alternative way could be to inform affected third parties directly, such as for example, Mullen’s (2002) proposed technology which shows a console message that gives “detailed information on what occurred and how to easily disable [the anti-worm] code, [as in fact] simply closing the console application will remove [the anti-worm] code from memory”. Ways like this may be possible ways notifying the third party.

<sup>188</sup> Under our proposed rules, a third party caught in the cross-fire cannot simply hack back the original attacked party in retaliation. The main idea of active self-defense is that it is an action meant to minimize damage to one’s self and not to inflict damage on the other, so that if the third party exercises active defense in order to reduce damage to him, then we envision that to be a valid exercise of hackback; but on the contrary, if such third party simply hacks back in retaliation, then such is prohibited. The rules then are also meant to address such possibility. Thus, valid active self-defense should generally be exercised while the attack is ongoing and not an after thought after the fact, at the time that there is no more damage to mitigate. At that stage, it is the authorities who take over and the privilege to exercise active defense ceases.

Also, instituting liability rules will also help address this possibility of hackback wars, because under these rules, the third party, if it decides to hackback the original attacked firm, becomes itself subject to the rules of active defense, which includes liability to any party (including the original attacked party) for damages. This too should reduce the possibility of the cascade effect. In short, the third party also has the right to exercise self-help, including prohibiting access/pass through to its systems, as well as more active forms of self-defense (subject to the same hackback rules).

So, we conclude that the possibility of cascade of war, if not totally checked, is at least minimized by our regulations for a valid exercise of self-defense as well as our liability rules. As an example: since our paper show that both the reasonableness regulations and the liability rules reduce the region that the firm hacks back; then, say for instance that the overall hackback \* mistake probability is  $p$ , and that this is reduced by the rules from  $p$  to say,  $p(1-r)$ , and let’s say for simplicity that A hack backs B, who hacks backs C, etc. ad infinitum, and that the damage in each case is  $D$ , then the overall sum of damages is lowered from  $Dp/[1-p]$  to  $Dp(1-r)/[1-p(1-r)]$ . Thus, at least, the effects are minimized.

In sum, we think at this possibility of cascade of war is an important consideration. Our conclusion is that our liability rules and reasonableness regulations help alleviate this problem. But it is a complex problem, and with full scale modeling with three or more parties and otherwise, will need a lot of future work, and opens up a whole new field of research. This is thus a promising future area of investigation.

<sup>189</sup> Which Symbiot defined as: “(1) escalated multilateral profiling and blacklisting of upstream providers; (2) distributed denial of service counterstrikes; (3) special operations experts applying invasive techniques; and (4) combined operations which apply financial derivatives, publicity disinformation, and other techniques of psychological operations.” (Symbiot, Inc. 2004a)

exercise of self-defense.<sup>190</sup> (Some of their less aggressive measures, however, such as defensive measures employed in pursuit of a “symmetric” response (for example, blocking a hostile act), or the use of honeypots to “divert, quarantine, and study the probable hostile acts in progress” [see Symbiot, Inc. 2004a] may be within the purview of the rules we contemplate.) In contrast, we consider more Mullen’s (2002) “neutralizing agent” technology, which either places a mutex<sup>191</sup> on the attacking box in order to prevent the Nimda and Code Red II worms processes from executing, or “injects and IPsec rule directly into process memory to block the outbound port that the worm needs to propagate” in order to stop the attack, to be more along the lines of active self-defense we are contemplating.<sup>192</sup> In short, the hackback we think of is one not intended for inflicting damages but more in a way of defense.

## 7. CONCLUSIONS

We believe that self-defense springs from the natural instinct for self-preservation. Hence, hackback should not be banned outright – it is generally accepted that one has the right to defend one’s self and one’s property and, toward this end, use reasonable force (see Aquinas c.1271, II, II, Q.64, Art. 7). The fact that the exercise of this right can be

---

<sup>190</sup> Asymmetric counterstrikes are “pre-emptive measures in response to distributed attacks orchestrated by a known source’ with ‘retaliation’ potentially ‘far in excess of the attack that the aggressor has underway.” (Smith 2005)

<sup>191</sup> See Webopedia, *Mutex*, <http://www.webopedia.com/TERM/m/mutex.html>: “Mutex” is “[s]hort for *mutual exclusion object*. In *computer programming*, a mutex is a *program object* that allows multiple program *threads* to share the same resource, such as file access, but not simultaneously. When a program is started, a mutex is created with a unique name. After this stage, any thread that needs the resource must lock the mutex from other threads while it is using the resource. The mutex is set to unlock when the data is no longer needed or the routine is finished.”

<sup>192</sup> In fact, Mullen claims: “we want to adhere not only to the concept of ‘reasonable force,’ but to utilize ‘minimal force’ where at all possible. Our goal is not to ‘fix’ everyone’s systems, and not to teach lax administrators a lesson. Our goal is to stop the propagation of global worms.” (Mullen 2002)



abused does not necessarily mean that the right should be denied at the outset; it does, however, mean that the exercise of the privilege should be regulated.

In this paper, we formulated criteria and guidelines that articulate under what circumstances self-defense is proper in cyberspace, and in what situations should we instead rely on the police or resort to the courts. Using a game-theoretic model of the interaction between the defender and the hacker, we were able to capture the interplay between legal remedies (police enforcement and court litigation), technology (IDS and traceback), and economic incentives (cost and benefits of self-help remedies), and thus develop specific rules or tests for resolving whether resort to hackback is justified vel non. Based on the results from the model, the criteria for valid resort to hackback are: (1) other alternatives, such as police enforcement and resort to courts, are either ineffective or ineffectual; (2) there is a genuine prospect of hitting the hacker instead of innocent third parties; and (3) the damage that can be mitigated to the defender's systems outweigh the potential damage to third parties. Additionally, when hackback is justified, the following rules govern conduct during hackback: (4) defenders must not use excessive force, that is, they must only use force necessary to defend their property and not needlessly destroy the hacker's digital assets; and (5) counter-strikers would be held liable for damage to other third parties. Thus, liability rules should be set in place so that firms will internalize the damage to third parties, thereby bringing the private incentive to hackback closer to the socially-optimal outcome.

In sum, we conclude that the law should permit hackback in certain situations, but it should also layer third-party liability rules on top of reasonableness conditions in order to effectively rein the potential abuses of the self-help privilege.

## 8. SUMMARY OF NOTATIONS AND PROOF OF PROPOSITIONS

### Summary of Notations

#### 1. List of Parameters

$G$  = hacker's gain from hacking

$D_f$  = firm's damage due to hacking

$D_h$  = damage to the hacker if the firm hacks back

$F$  = fine the hacker pays if caught by law enforcers

$W$  = amount awarded the firm if it wins the litigation

$K$  = cost of going to court

$r$  = percentage of damage recovered if the firm decides to "simply recover damage"

$h$  = percentage of damage mitigated by resorting to hackback

$d$  = damage incurred by third parties (as percentage of the counter-striker's damage)

$p_e$  = probability that the hacker gets caught by police enforcement

$p_h$  = probability of hitting the hacker if the firm hacks back

$p_w$  = probability of winning the case if the firm litigates

$\theta$  = proportion of hackers in the population

$\pi$  = fraction of affected third parties who forgo suit against the counterstriker

$q_1$  = probability of getting an IDS signal given that there is an intrusion

$q_2$  = probability of not getting an IDS signal given that there is no intrusion

$\eta_1$  = probability of intrusion given the IDS signals an intrusion

$\eta_2$  = probability of intrusion given the IDS does not signal an intrusion

## 2. List of Strategy Elements

$\delta$  = probability that the hacker hacks

$\mu$  = probability that the firm monitors in the no IDS case

$\sigma_1$  = probability that the firm hacks back in the no IDS case

$\sigma_2$  = probability that the firm litigates in the no IDS case

$\mu_1$  = probability that the firm monitors if the IDS signals an intrusion

$\alpha_1$  = probability that the firm hacks back if the IDS signals an intrusion

$\alpha_2$  = probability that the firm litigates if the IDS signals an intrusion

$\mu_2$  = probability that the firm monitors if the IDS does not signal an intrusion

$\beta_1$  = probability that the firm hacks back if the IDS does not signal an intrusion

$\beta_2$  = probability that the firm litigates if the IDS does not signal an intrusion

### Proof of Proposition 3-2.

*Equilibrium B1:* Since  $\frac{\partial F}{\partial \sigma_2} > \frac{\partial F}{\partial \sigma_1}$  at all points within their domain,  $\sigma_2 > \sigma_1$ . Since

$$C_t < [p_w W - K], \frac{\partial F}{\partial \sigma_2} > 0 \Rightarrow \sigma_2 = 1 \Rightarrow \sigma_1 = 0 \Rightarrow \frac{\partial F}{\partial \mu} = -C_m + \theta \delta \{p_w W - K + rD_f - C_t\}$$

$$\Rightarrow \delta = \frac{C_m}{\theta \{p_w W - K + rD_f - C_t\}}. \text{ This is true for } 0 < \delta < 1 \text{ or, equivalently,}$$

$$\frac{1}{\theta} < \frac{p_w W - K + rD_f - C_t}{C_m}. \frac{\partial H}{\partial \delta} = G - p_e F - \mu p_w W \Rightarrow \mu = \frac{G - p_e F}{p_w W}. \text{ This is true for}$$

$$0 < \mu < 1 \text{ or } 0 < G - p_e F < p_w W. \text{ Equilibrium B2: } p_e F < G - p_w W \Rightarrow$$

$$0 < G - p_e F - p_w W. p_e F < G - p_h D_h \Rightarrow 0 < G - p_e F - p_h D_h. \text{ Together, they}$$

imply  $\delta = 1$ . Given  $\delta = 1$ , and  $(\sigma_1 = 0, \sigma_2 = 1)$  as in equilibrium B1 above,

$\frac{\partial F}{\partial \mu} = -C_m + \theta\{p_w W - K + rD_f - C_t\} > 0$  in the region. Hence,  $\mu = 1$ . *Equilibrium C:*

$\frac{\partial F}{\partial \sigma_1} > \frac{\partial F}{\partial \sigma_2} \Rightarrow \sigma_1 > \sigma_2$ . Since in the region  $\frac{[p_h h - (1 - p_h) + r]D_f - C_t}{C_m} > \frac{rD_f}{C_m}$ ,

$\frac{\partial F}{\partial \sigma_1} > 0 \Rightarrow \sigma_1 = 1 \Rightarrow \sigma_2 = 0$ . Thus,  $\frac{\partial H}{\partial \delta} = G - p_e F - \mu p_h D_h > 0$  in the region

$G - p_h D_h > p_e F$ , and  $\delta = 1$ . Hence,  $\frac{\partial F}{\partial \mu} = -C_m + \theta\{[p_h h - (1 - p_h)d + r]D_f - C_t\} > 0 \Rightarrow$

$\mu = 1$ . *Equilibrium D:*  $\sigma_1 = 1$  and  $\sigma_2 = 0$  as in equilibrium C above.

Suppose  $\frac{\partial F}{\partial \mu} = 0$ . Then,  $\delta = \frac{C_m}{\theta\{[p_h h - (1 - p_h)d + r]D_f - C_t\}}$ . This is true for  $0 < \delta < 1$

or  $\frac{1}{\theta} < \frac{[p_h h - (1 - p_h)d + r]D_f - C_t}{C_m}$ . In this case,  $\frac{\partial H}{\partial \delta} = G - p_e F - \mu p_h D_h \Rightarrow$

$\mu = \frac{G - p_e F}{p_h D_h}$ . This is true for  $0 < \mu < 1$  or  $0 < G - p_e F < p_h D_h$ .

**Lemma 3-2.** (a)  $\mu_1 \alpha_2 \geq \mu_2 \beta_2$  and (b)  $\mu_1 \alpha_1 \geq \mu_2 \beta_1$ .

**Proof.** To prove (a), we only need to show that  $\frac{\partial F}{\partial \mu_1 \alpha_2} \geq \frac{\partial F}{\partial \mu_2 \beta_2}$  at all points within

their domain.  $\frac{\partial F}{\partial \mu_1 \alpha_2} = [q_1 \theta \delta + (1 - q_2)(1 - \theta \delta)] \eta_1 \{p_w W - K - C_t\}$ .

$\frac{\partial F}{\partial \mu_2 \beta_2} = [(1 - q_1) \theta \delta + q_2 (1 - \theta \delta)] \eta_2 \{p_w W - K - C_t\}$ .

$\frac{\partial F}{\partial \mu_1 \alpha_2} - \frac{\partial F}{\partial \mu_2 \beta_2} = [q_1 \theta \delta - (1 - q_1) \theta \delta] \cdot \{p_w W - K - C_t\}$ . The first term is positive. The

second term is negative only if  $[p_w W - K] < C_t$ , which means that  $\frac{\partial F}{\partial \alpha_2} < 0$  and

$\frac{\partial F}{\partial \beta_2} < 0$ , which respectively means that  $\alpha_2 = 0$  and  $\beta_2 = 0$ . The proof of (b) is

analogous.

**Lemma 3-3.**  $G < p_e F \Rightarrow \delta = 0, \mu_1 = \mu_2 = 0 \Rightarrow \mu_1 \alpha_1 = \mu_1 \alpha_2 = \mu_2 \beta_1 = \mu_2 \beta_2 = 0$ .

**Proof.**  $\frac{\partial H}{\partial \delta} < 0$  because  $G < p_e F$ , and  $\mu_1 \alpha_1 p_h D_h, \mu_1 \alpha_2 p_w W, \mu_2 \beta_1 p_h D_h,$

$\mu_2 \beta_2 p_w W, q_1$  and  $1 - q_1$  are all  $\geq 0 \Rightarrow \delta = 0$  in equilibrium. Substituting in  $\delta = 0$ ,

$\frac{\partial F}{\partial \mu_1}(\delta = 0) = (1 - q_2)[-C_m] < 0$  and  $\frac{\partial F}{\partial \mu_2}(\delta = 0) = q_2[-C_m] < 0 \Rightarrow \mu_1 = \mu_2 = 0$  in

equilibrium.

**Proof of Proposition 3-3.**

Since  $p_w W - K < C_i \Rightarrow \frac{\partial F}{\partial \alpha_2}, \frac{\partial F}{\partial \beta_2} < 0$ , all equilibria here have the common feature

that  $\alpha_2 = \beta_2 = 0$  in equilibrium.

(a) *Equilibrium B:* Since  $[(1 - q_1)\theta\delta + q_2(1 - \theta\delta)]$  and  $[q_1\theta\delta + (1 - q_2)(1 - \theta\delta)]$  are both

positive, the signs of  $\frac{\partial F}{\partial \mu_1}$  and  $\frac{\partial F}{\partial \mu_2}$  follow the signs of

$$-\frac{C_m}{\eta_1} + \alpha_1 \{ [p_h h - (1 - p_h)d]D_f - C_i \} + rD_f \text{ and}$$

$$-\frac{C_m}{\eta_2} + \beta_1 \{ [p_h h - (1 - p_h)d]D_f - C_i \} + rD_f, \text{ respectively. That is, } \frac{\partial F}{\partial \mu_1} < 0 \text{ if}$$

$$\eta_1 \{ \alpha_1 [p_h h - (1 - p_h)d]D_f - \alpha_1 C_i + rD_f \} < C_m \text{ or } \frac{\alpha_1 \{ [p_h h - (1 - p_h)d]D_f - C_i \} + rD_f}{C_m}$$

$$< a_1 \equiv \max \left[ \frac{q_1 \theta + (1 - q_2)(1 - \theta)}{q_1 \theta}, \frac{rD_f}{C_m} \right] \text{ (if } \delta = 1), \text{ which is true if}$$

$$\frac{[p_h h - (1 - p_h)d + r]D_f - C_t}{C_m} < a_1. \text{ Likewise, } \frac{\partial F}{\partial \mu_2} < 0 \text{ if}$$

$$\eta_2 \{ \beta_1 [p_h h - (1 - p_h)d]D_f - \beta_1 C_t + rD_f \} < C_m \text{ or}$$

$$\frac{\beta_1 \{ [p_h h - (1 - p_h)d]D_f - C_t \} + rD_f}{C_m} < a_2 \equiv \frac{(1 - q_1)\theta + q_2(1 - \theta)}{(1 - q_1)\theta} \text{ (if } \delta = 1), \text{ which is true}$$

$$\text{if } \frac{[p_h h - (1 - p_h)d + r]D_f - C_t}{C_m} < a_2. \text{ (For simplicity, we assume that}$$

$$\frac{(1 - q_1)\theta + q_2(1 - \theta)}{(1 - q_1)\theta} > \frac{rD_f}{C_m}.) \text{ We need to show that } \delta = 1.$$

$$\frac{\partial H}{\partial \delta} (\mu_1 = \mu_2 = 0) = G - p_e F > 0 \text{ in the region, implying that } \delta = 1.$$

$$(b) \text{ Equilibrium C1: Since } \alpha_2 = \beta_2 = 0, \mu_1 = 1 \text{ if } \frac{\partial F}{\partial \mu_1} > 0 \text{ or if}$$

$$\eta_1 \{ \alpha_1 [p_r r - (1 - p_r)d]D_f - \alpha_1 C_t + rD_f \} > C_m \text{ or } \frac{[p_h h - (1 - p_h)d + r]D_f - C_t}{C_m} > a_1 \text{ (if}$$

$$\alpha_1 = 1 \text{ and } \delta = 1). \text{ We need to check that } \alpha_1 = 1. \frac{\partial F}{\partial \alpha_1} = q_1 \theta \cdot [p_h h - (1 - p_h)d]D_f - C_t.$$

$$q_1 \theta > 0, \text{ and } [p_h h - (1 - p_h)d]D_f - C_t > 0 \text{ in the region. Thus, } \frac{\partial F}{\partial \alpha_1} > 0 \Rightarrow \alpha_1 = 1.$$

$$\text{Lastly, we need to check that } \delta = 1. \frac{\partial H}{\partial \delta} = G - p_e F - q_1 p_h D_h > 0 \text{ in the region. Hence,}$$

$$\delta = 1.$$

(c) *Equilibrium C2*:  $\frac{\partial H}{\partial \delta} > 0$  (since  $p_e F < G - p_h D_h$ )  $\Rightarrow \delta = 1$ . Since

$$\frac{[p_h h - (1 - p_h)d + r]D_f - C_t}{C_m} > a_2 > a_1 \geq \frac{rD_f}{C_m}, \text{ then } [p_h h - (1 - p_h)]D_f > C_t, \text{ implying}$$

that  $\alpha_1 = \beta_1 = 1$ .  $\frac{\partial F}{\partial \mu_1}(\alpha_1 = \beta_1 = \delta = 1) =$

$$[q_1 \theta + (1 - q_2)(1 - \theta)] \cdot \left( -C_m + \frac{q_1 \theta}{q_1 \theta + (1 - q_2)(1 - \theta)} \{ [p_h h - (1 - p_h)d + r]D_f - C_t \} \right) \text{ which is}$$

positive in the range  $\frac{[p_h h - (1 - p_h)d + r]D_f - C_t}{C_m} > a_2 > a_1$ . Likewise,

$$\frac{\partial F}{\partial \mu_2}(\alpha_1 = \beta_1 = \delta = 1) = [(1 - q_1)\theta + q_2(1 - \theta)] \cdot \left( -C_m + \frac{(1 - q_1)\theta}{(1 - q_1)\theta + q_2(1 - \theta)} \{ [p_h h - (1 - p_h)d + r]D_f - C_t \} \right)$$

is positive in the range  $\frac{[p_h h - (1 - p_h)d + r]D_f - C_t}{C_m} > a_2$ .

(d) *Equilibrium D1*: In the region  $\frac{[p_h h - (1 - p_h)d + r]D_f - C_t}{C_m} > a_1 \geq \frac{rD_f}{C_m}$ ,

$[p_h h - (1 - p_h)d]D_f > C_t$ . Thus,  $\frac{\partial F}{\partial \alpha_1} > 0$  and  $\frac{\partial F}{\partial \beta_1} > 0$  implying that  $\alpha_1 = \beta_1 = 1$ .

Given  $\alpha_1 = 1$ ,  $\mu_2 \beta_1 = \mu_2 \beta_2 = \mu_1 \alpha_2 = 0$ ,  $\frac{\partial H}{\partial \delta} = G - p_e F - q_1 \mu_1 p_h D_h$ . Suppose  $\frac{\partial H}{\partial \delta} = 0$ .

Then,  $\mu_1 = \frac{G - p_e F}{q_1 p_h D_h}$  where  $\mu_1 \in (0, 1)$  or  $0 < G - p_e F < q_1 p_h D_h$ . Given that  $\mu_1 = \text{mixed}$

(that is,  $\frac{\partial F}{\partial \mu_1} = 0$ ), then  $\delta = \frac{(1 - q_2)C_m}{q_1 \theta \{ [p_h h - (1 - p_h)d + r]D_f - C_t \} - \theta(q_1 + q_2 - 1)C_m}$ .

$\delta \in (0, 1)$  implies  $C_m < \frac{\theta q_1}{(1 - \theta)(1 - q_2) + \theta q_1} \{ [p_h h - (1 - p_h)d + r]D_f - C_t \}$  or

$\frac{[p_h h - (1 - p_h)d + r]D_f - C_t}{C_m} > a_2$ . We need to show that  $\mu_2 = 0$ .  $\frac{\partial F}{\partial \mu_2} < 0$  if

$[(1 - q_1)\theta\delta + q_2(1 - \theta\delta)] \cdot C_m > (1 - q_1)\theta\delta \cdot \{[p_h h - (1 - p_h)d + r]D_f - C_t\}$ , or if

$\left[1 + \frac{q_2}{(1 - q_1)\theta\delta} - \frac{q_2}{(1 - q_1)}\right] > \frac{\{[p_h h - (1 - p_h)d + r]D_f - C_t\}}{C_m}$ , or, given that

$\delta = \frac{(1 - q_2)C_m}{q_1\theta\{[p_h h - (1 - p_h)d + r]D_f - C_t\} - \theta(q_1 + q_2 - 1)C_m}$ , if

$\frac{q_2}{(1 - q_1)} \cdot \left[ \frac{q_1\{[p_h h - (1 - p_h)d + r]D_f - C_t - C_m\} + (1 - q_2)C_m}{(1 - q_2)C_m} \right] > \frac{\{[p_h h - (1 - p_h)d + r]D_f - C_t\}}{C_m} - 1$ , or if

$\frac{q_2}{(1 - q_1)} \cdot \frac{q_1}{(1 - q_2)} \left[ \frac{\{[p_h h - (1 - p_h)d + r]D_f - C_t - C_m\}}{C_m} \right] > \frac{\{[p_h h - (1 - p_h)d + r]D_f - C_t\}}{C_m} - 1$ , which is

true since  $q_1$  and  $q_2$  are both greater than 0.5 by assumption. Therefore,  $\mu_2 = 0$ . Hence,

for  $G - q_1 p_h D_h < p_e F < G$  and  $\frac{[p_h h - (1 - p_h)d + r]D_f - C_t}{C_m} > a_2$ ,

$\delta = \frac{(1 - q_2)C_m}{q_1\theta\{[p_h h - (1 - p_h)d + r]D_f - C_t\} - \theta(q_1 + q_2 - 1)C_m}$ ,  $\mu_1 \alpha_1 = \frac{G - p_e F}{q_1 p_h D_h}$  and

$\mu_1 \alpha_2 = \mu_2 \beta_1 = \mu_2 \beta_2 = 0$  are equilibrium strategies.

(e) *Equilibrium D2*:  $\frac{[p_h h - (1 - p_h)d + r]D_f - C_t}{C_m} > a_2 > a_1 \geq \frac{rD_f}{C_m} \Rightarrow$

$[p_h h - (1 - p_h)d]D_f > C_t \Rightarrow \alpha_1 = \beta_1 = 1$  in the range. Suppose  $\frac{\partial H}{\partial \delta} = \frac{\partial F}{\partial \mu_2} = 0$ .

$\frac{\partial H}{\partial \delta} = 0 \Rightarrow \mu_2 = \frac{G - p_e F - q_1 p_h D_h}{(1 - q_1) p_h D_h}$  if  $\mu_1 = 1$ . This is true for  $\mu_2 \in (0, 1)$  or

$G - p_h D_h < p_e F < G - q_1 p_h D_h \cdot \frac{\partial F}{\partial \mu_2} = 0 \Rightarrow$



$$\delta = \frac{q_2 C_m}{\theta(q_1 + q_2 - 1)C_m + (1 - q_1)\theta\{[p_h h - (1 - p_h)d + r]D_f - C_t\}}. \text{ This is true for } \delta \in (0, 1) \text{ or}$$

$$C_m < \{[p_h h - (1 - p_h)d + r]D_f - C_t\} \frac{(1 - q_1)\theta}{(1 - \theta)q_2 + \theta(1 - q_1)} \text{ or}$$

$$\frac{[p_h h - (1 - p_h)d + r]D_f - C_t}{C_m} > a_2. \text{ Verify that } \mu_l = 1 \text{ or } \frac{\partial F}{\partial \mu_l} > 0. \text{ This is true if}$$

$$[q_1 \theta \delta + (1 - q_2)(1 - \theta \delta)] \cdot C_m < q_1 \theta \delta \cdot \{[p_h h - (1 - p_h)d + r]D_f - C_t\} \text{ or if}$$

$$\left[1 + \frac{(1 - q_2)(1 - \theta \delta)}{q_1 \theta \delta}\right] < \frac{\{[p_h h - (1 - p_h)d + r]D_f - C_t\}}{C_m} \text{ or, given that}$$

$$\delta = \frac{q_2 C_m}{\theta(q_1 + q_2 - 1)C_m + (1 - q_1)\theta\{[p_h h - (1 - p_h)d + r]D_f - C_t\}}, \text{ is equivalent to}$$

$$\left[1 + \frac{(1 - q_2)}{q_1} \cdot \frac{(q_1 + q_2 - 1)C_m + (1 - q_1)\{[p_h h - (1 - p_h)d + r]D_f - C_t\}}{q_2 C_m} - \frac{(1 - q_2)}{q_1}\right] < \frac{\{[p_h h - (1 - p_h)d + r]D_f - C_t\}}{C_m},$$

$$\text{or } 1 + \frac{(1 - q_2)}{q_1} \cdot \left[\frac{(1 - q_1)\{[p_h h - (1 - p_h)d + r]D_f - C_t - C_m\}}{q_2 C_m}\right] < \frac{\{[p_h h - (1 - p_h)d + r]D_f - C_t\}}{C_m}, \text{ or}$$

$$\frac{(1 - q_2)}{q_1} \cdot \frac{(1 - q_1)}{q_2} \left[\frac{\{[p_h h - (1 - p_h)d + r]D_f - C_t - C_m\}}{C_m}\right] < \frac{\{[p_h h - (1 - p_h)d + r]D_f - C_t\}}{C_m} - 1, \text{ which is}$$

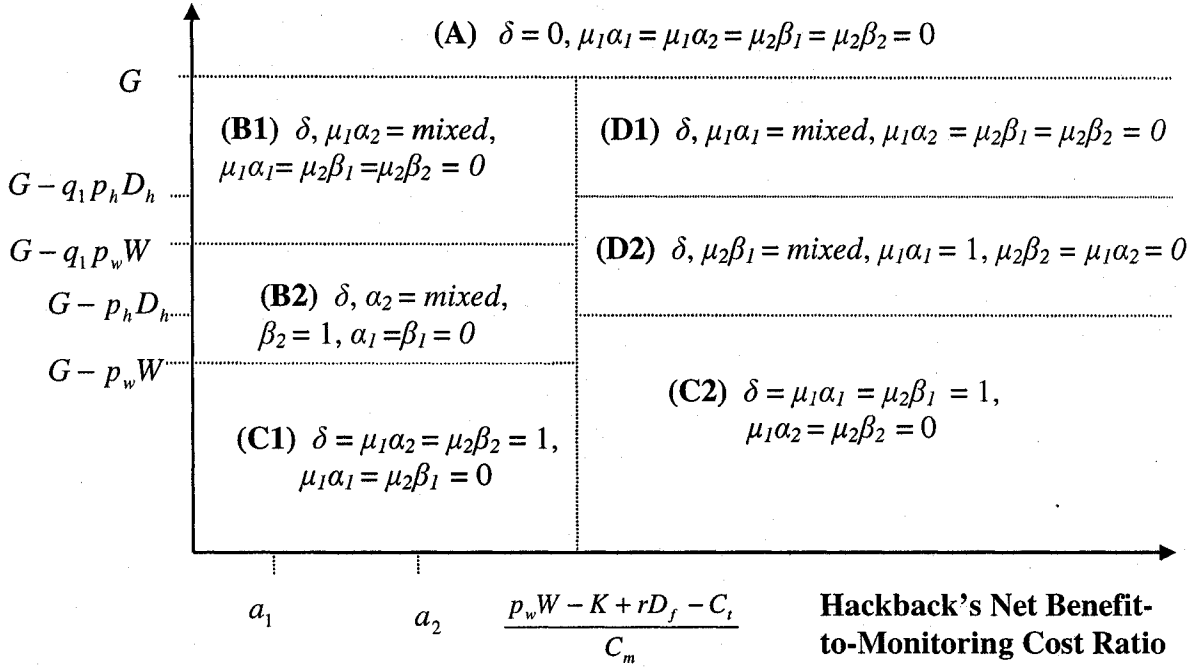
true since  $q_1$  and  $q_2$  are both greater than 0.5 by assumption. Hence,  $\mu_l = 1$ .

$$\textbf{Proposition 3-4.} \text{ When } a_1 < a_2 \equiv \frac{(1 - q_1)\theta + q_2(1 - \theta)}{(1 - q_1)\theta} < \frac{p_w W - K + rD_f - C_t}{C_m},$$

litigation is beneficial regardless of whether or not the IDS signals an intrusion. In this

case, the following Bayesian Nash equilibria obtain:

Probability times  
Magnitude of Fine,  $p_e F$



**Figure 3-A1.** Nash equilibria when litigation is beneficial (IDS available)

**Proof.** Proof analogous to Proposition 3-3 with  $\frac{p_w W - K + r D_f - C_t}{C_m}$  substituting for

$\frac{[p_h h - (1 - p_h) d + r] D_f - C_t}{C_m}$ ,  $G - q_1 p_w W$  substituting for  $G - q_1 p_h D_h$ , etc.

**Lemma 3-4.**  $\eta_1 > \delta$  (given  $q_1, q_2 > 0.5$ ).

**Proof** (by contradiction). Assume that  $\eta_1 \leq \delta$ . Then, by algebraic manipulation,  $q_1 \leq q_1 \delta + (1 - q_2)(1 - \delta) \Rightarrow q_1 \leq 1 - q_2$ . This is a contradiction since  $q_1$  and  $q_2$  are both greater than 0.5 by assumption. Hence,  $\eta_1 > \delta$ .

**Proposition 3-5.** When  $a_1 < \frac{p_w W - K + r D_f - C_t}{C_m} < a_2$ , litigation is beneficial when the IDS signals an intrusion, but not otherwise. In this case, the following Bayesian Nash

equilibria obtain:

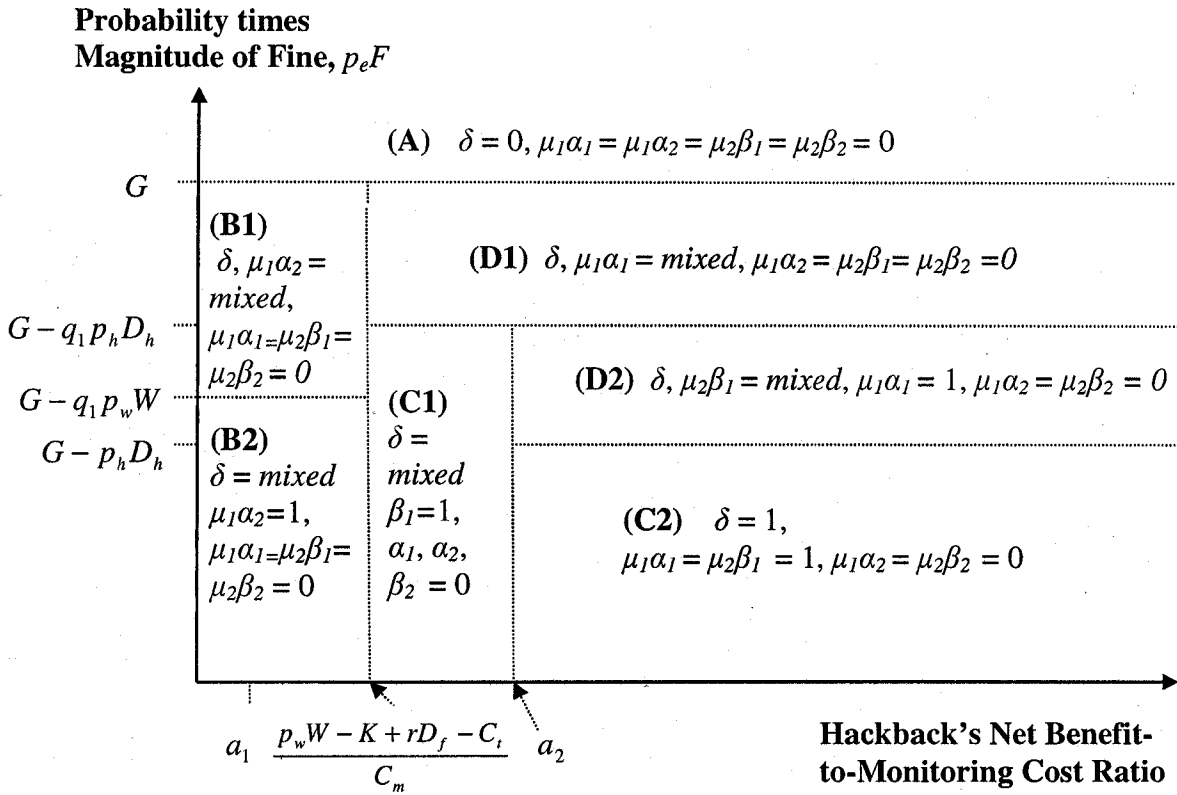


Figure 3-A2. Nash equilibria when litigation is beneficial when the IDS signals an intrusion, but not otherwise

**Proof.** Proof analogous to Proposition 3-3 with  $\frac{p_w W - K + r D_f - C_t}{C_m}$  substituting for  $\frac{[p_h h - (1 - p_h) d + r] D_f - C_t}{C_m}$ , etc.

### Socially-Optimal Solution

**Proof of Nash Equilibria for the Social Planner's Problem.** The proof is

analogous to previous Nash equilibria calculations taking note of the following:  $\frac{\partial S}{\partial \sigma_1} > 0$

if  $\theta\delta\mu\{[p_h h - (1 - p_h)d]D_f - C_i > \delta\mu p_h D_h\}$ , or if

$$\frac{[p_h h - (1 - p_h)d + r]D_f - C_i}{C_m} > \frac{1}{\theta} \cdot \left[ \frac{\theta r D_f}{C_m} + \frac{p_h D_h}{C_m} \right]. \text{ In this case, } \sigma_1 = 1 \text{ and}$$

$$\frac{\partial S}{\partial \mu} = -C_m + \theta\delta\{[p_h h - (1 - p_h)d + r]D_f - C_i\} - \delta p_h D_h = 0 \Rightarrow$$

$$\delta = \frac{C_m}{\theta\{[p_h h - (1 - p_h)d + r]D_f - C_i\} - p_h D_h} \text{ for}$$

$$C_m < \theta\{[p_h h - (1 - p_h)d + r]D_f - C_i\} - p_h D_h, \text{ or}$$

$$\frac{1}{\theta} \left[ 1 + \frac{p_h D_h}{C_m} \right] < \frac{[p_h h - (1 - p_h)d + r]D_f - C_i}{C_m}. \text{ Also, given } \sigma_1 = 1,$$

$$\frac{\partial H}{\partial \delta} = G - p_e F - \mu p_h D_h = 0 \Rightarrow \mu = \frac{G - p_e F}{p_h D_h} \text{ for } 0 < G - p_e F < p_h D_h.$$

### Social Welfare Calculations

Region A: Case (a) hackback available:  $\delta^* = 0$  and  $\mu^* = 0 \Rightarrow S^* = 0$ . Case (b).

hackback not available:  $\delta^{**} = 0$  and  $\mu^{**} = 0 \Rightarrow S^{**} = 0$

Region B: Case (a):  $\delta^* = 1$  and  $\mu^* = 0$   $\sigma_1^* = 0 \Rightarrow S^* = -\theta D_f + [G - p_e F]$ . Case (b):

$$\delta^{**} = 1 \text{ and } \mu^{**} = 0 \Rightarrow S^{**} = -\theta D_f + [G - p_e F].$$

Region C: (a):  $\delta^* = 1$  and  $\sigma_1^* = 1 \Rightarrow$

$$S^* = -C_m - \theta C_i + \theta\{[p_h h + (1 - p_h)d]D_f - (1 - r)D_f\} + [G - p_e F - p_h D_h].$$

(b):  $\delta^{**} = 1 \Rightarrow S^{**} = -\theta D_f + [G - p_e F]$ . The net difference between the two pay-offs is

$-C_m + \theta \{ [p_h h - (1 - p_h)d + r] D_f - C_t \} - p_h D_h$  which is positive under the region

$$\frac{[p_h h - (1 - p_h)d + r] D_f - C_t}{C_m} > \frac{1}{\theta} \left[ 1 + \frac{p_h D_h}{C_m} \right].$$

Region D: (a)  $\delta^* = \frac{C_m}{\theta \{ [p_h h - (1 - p_h)d + r] D_f - C_t \} - p_h D_h}$  and  $\mu^* = \frac{G - p_e F}{p_h D_h}$ . (b)

$\delta^{**} = 1$  and  $S^{**} = -\theta D_f + [G - p_e F]$ . Hence, the difference between the two pay-offs is

$-\mu^* C_m + \theta \delta^* \mu^* \{ [p_h h - (1 - p_h)d + r] D_f - C_t \} + \theta D_f (1 - \delta^*) - [G - p_e F] (1 - \delta^*)$ . Since

$\delta^* = \frac{C_m}{\theta \{ [p_h h - (1 - p_h)d + r] D_f - C_t \} - p_h D_h}$ , then the first two terms equals

$$-\mu^* C_m + \theta \left[ \frac{C_m}{\theta \{ [p_h h - (1 - p_h)d + r] D_f - C_t \} - p_h D_h} \right] \mu^* \{ [p_h h - (1 - p_h)d + r] D_f - C_t \} = 0.$$

The last two terms equals  $(1 - \delta) \cdot \{ \theta D_f - [G - p_e F] \}$  which is positive

whenever  $\theta D_f > [G - p_e F]$ .

## CHAPTER 4:

### OPTIMAL MIX OF INDIVIDUAL PRECAUTIONS AND POLICE ENFORCEMENT WHEN RISKS ARE INTERRELATED: THE CASE OF CYBERCRIMES

#### 1. INTRODUCTION

Is Internet security a public good? How should society handle the spill-over effects arising from the interrelatedness of Internet risks? What role, if any, does police enforcement play? What optimal combination of each of these security measures – police enforcement, and individual investments in both private and non-rivalrous security goods – should be used to effectively combat cybercrimes?

In this paper, we argue that some, but not all, investments in security have the nature of public goods. A textbook definition is that a “public good is a commodity for which use of a unit of the good by one agent does not preclude its use by other agents.”

(MasColell, Whinston, and Green 1995, p. 359). Put differently, public goods are goods which are nonrival or nondepletable: consumption by one person does not diminish or reduce the supply available to others.<sup>193</sup> Classic examples are national defense, police protection, lighthouses, public parks, information and knowledge, clean air, etc. In contrast, private goods are goods “whose consumption only affects a single economic agent” (Varian 1992, p. 414). Classic examples of private goods are bread, shoes, etc.

---

<sup>193</sup> A distinction is also sometimes made in the literature according to the excludability of an individual from the enjoyment of a public good. “Every private good is automatically excludable, but public goods may or may not be.” (MasColell, Whinston, and Green 1995, p. 360) For simplicity, we will abstract from the issue of excludability.

On the basis of the above definition, we think that Internet security has both public and private goods aspects. Insofar as everyone shares common available risks (has a common pool of hackers and vulnerabilities that can be exploited), and will thus all benefit from the reduction in such common pool of risks (“public bads”), then Internet security has public goods aspects, in the same manner that police and fire protection are traditionally regarded as public goods. On the other hand, insofar as there are residual risks not entirely eliminated by police enforcement, individuals can protect themselves against the residual risks by investing in individual-level precautions. These individual precautions in turn can take one of two forms: (a) investments in private security goods (such as the purchase of firewalls, intrusion detection systems [IDS], anti-virus, security authentication codes, etc.); or (b) investments in non-rivalrous security goods (such as compiling information on software vulnerabilities, security holes, security incidents, hacking patterns, state of the art, etc.) which have the aspects of public goods. In sum, Internet security has both public and private goods dimensions; the public goods aspects of Internet security in turn can be provided either privately or publicly by the government (see Table 4-1 below).

**Table 4-1. Private and Public Goods Aspects of Internet Security**

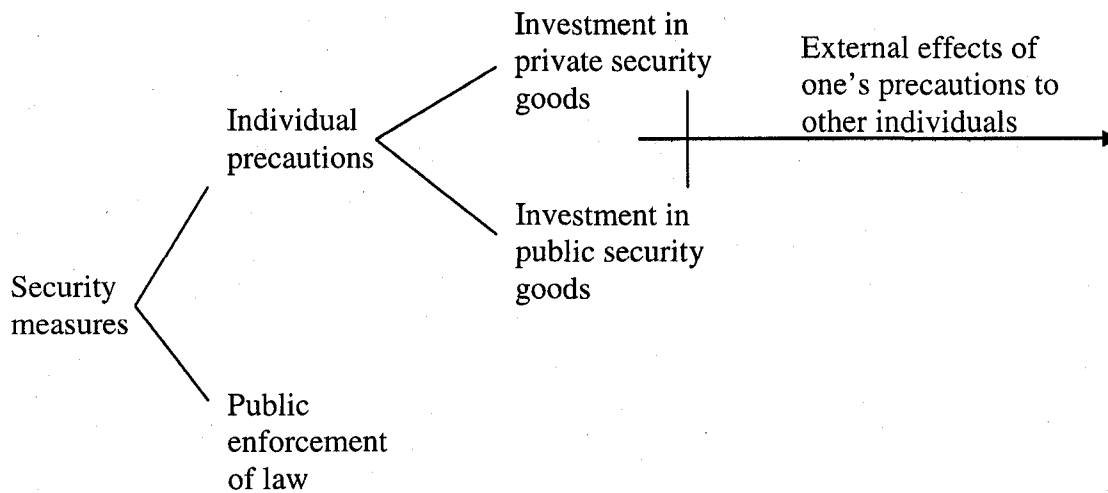
Nature of the good/service	How Provided	
	Privately (by individuals/firms)	Publicly (by the government)
Private goods	IDS, firewalls, etc.	
Public	information on attacks, vulnerabilities, solutions	police enforcement/protection

Another important consideration is that, in the Internet, there is significant interrelatedness of risks giving rise to externalities among individual websites. For example, if an individual does not use an anti-virus to clean his/her system, the computer

virus can affect not only his/her computer systems, but others' as well. Hence, a computer system can be breached, not only directly but also indirectly through the negligence of other individuals in interconnected networks. In other words, privately provided private security goods do not have private benefits alone – due to externalities, these private investments have spill-over effects to other Internet users (the public).

Thus, in this paper, we study a model that combines all of these elements (see Figure 4-1):

- private investments in security;
- investments in security that have the nature of public goods;
- externalities; and
- public enforcement of law.



**Figure 4-1.** Elements of the model

That is, we model the situation where firms invest in both private and public security goods, when there is public enforcement of law against hackers. The previous studies that have analyzed private security expenditures as a way to protect against crimes have



modeled private precautions but leave out public enforcement of law in their models (Shavell 1991, Kobayashi 2005). In reality, crimes can be solved by a combination of private precautions and public enforcement of the law. Expenditures on police enforcement reduce the number of crime incidents, while investments in individual precautions reduce the effectiveness of criminals in causing harm to the victims. In this paper, we study a model where crimes are addressed through a combination of private and public measures. By so doing, we hope to capture the substitutability between the private and public responses, and determine what is the optimal combination of these approaches.

Although past studies have looked at some of the aspects mentioned in Figure 4-1 individually and in isolation – for example, Heal and Kunreather (2003) has looked at interrelatedness of risks, for example, in the context of terrorism and computer security; Shavell (1991) has looked at investments in rivalrous private precautions in general; and Kobayashi (2005) has considered investments in both private and public cybersecurity goods *individually* (that is, he considered separate investments in *either* of these goods, but not both of them together) – none of these studies have looked at all the elements mentioned above together. Looking at these elements together, we think, presents a more holistic view of the various ways society can protect itself against cyberattacks, and enables one to see the interplay, substitutability and optimal combination of these means to effectively combat cyber-attacks. Also, by modeling the collective solution, we aim to examine what role, if any, cooperation plays in Internet security.

We find that just because Internet security has public goods aspect does not necessary mean that the government, rather than the individual, should provide it. Rather, the

solution is a combination of public and private alternatives. The problem with ceding entirely to the government the function of providing Internet security is that such a solution is susceptible to the well-known problem of “government failure”.<sup>194</sup> On the other hand, the problem with adopting an entirely private solution is that such is susceptible to the problem of “market failure”: the externalities and public goods aspect of Internet security results in the divergence between the private solution and the socially-optimal solution. The solution therefore, we think, is a careful balance between private and public measures. Which brings us to the next result.

How then should society achieve an optimal allocation of security investments across the various public and private alternatives? We find that the socially-optimal level of security is achieved by combining private security investment, non-rivalrous security investment, and law enforcement measures in such a way that their marginal-social-benefit-to-marginal-social-cost ratios are equalized. These marginal *social* benefits of the

---

<sup>194</sup> “Government failure” refers to the situation where government intervention, say geared at correcting a market failure, not only fails to generate societal efficiency, but actually makes the situation worse (see, for example, Colander 2004). The reasons for this are myriad. One is that government actions reflect politics, and may not necessarily reflect good economics or the constituent’s will. For example, politicians’ actions may be influenced by special interests, since politicians themselves abide by the laws of supply and demand. Second, even if assuming that the government is well-intentioned in solving the problem, its lack of information relative to the market may mean that it is not the best actor for the job. Third, intervention in markets is complex and can lead to unintended consequences, and so, even if the intervention solves one problem area, there could be some distortion effects in other areas of the economy. Lastly, because of the bureaucratic nature of the intervention process, government action adjusts slowly to allow for fine-tuning with the changing nature of market conditions (see Colander 2004).

In Internet security, government failure can manifest itself in the inability of the government to know what the optimal social level of cybersecurity should be, considering that it does not possess the error correction mechanism of the market’s profit and loss system (Coyne and Lesson, forthcoming; Powell 2005). And because the public goods aspects of Internet security imply that these goods are not traded openly in the market, it is difficult for the government to estimate the socially-optimal level of cybersecurity and then measure it up against what was provided by the market (Powell 2005). Furthermore, since the government does not have the same market pressures, it does not have the same incentive as the market participants to employ the hardware and software configuration that will reduce the damage from specific attacks, at the least cost (Coyne and Lesson, forthcoming). In fact, there may be public relations pressures on the bureaucrats to make them pressure firms to overspend instead (Powell 2005). Another problem is that, once the regulation is passed, and the cybersecurity situation changes, it is often difficult for bureaucracy-tied policy-makers to assess, evaluate, and change the original policy. This is a particularly important consideration in the case of information security because of the ever dynamic nature of the technology environment (Coyne and Lesson, forthcoming).

private and public security good investments are greater than the marginal *private* benefits because individuals don't take into account the spill-over effects their own security investments have on other computer systems, resulting in an underinvestment of both non-rivalrous and rivalrous security goods. Additionally, we find that in certain situations it would be optimal for the government to deliberately lower the level of police enforcement in order to induce firms to invest more in individual precautions.

Lastly, we find that under certain conditions, a cooperative undertaking results in the close approximation of the socially-optimal level of private and public security good investments and police enforcement expenditures. This thus lends support to the recent government initiative to encourage the formation of information sharing and assessment centers (ISACs). The Shapley (1953) value can be used as a criterion for allocating the costs and benefits among the members of an ISAC. Alternatively, tradeable externality permits may be considered as another mechanism for apportionment among group members. Some sort of political equilibrium mechanism wherein members vote so that their preferences may be incorporated into the group's decision-making process may be considered as well.

This result further buttresses our conclusion that even if there is a market failure arising from public goods and externalities aspects of Internet security, it does not necessarily mean that government role is automatically prescribed to the exclusion of the private sector. Since under certain conditions the collective will approximate the socially-optimal solution, then some form decentralized group solution can be utilized in certain cases to help address the problem of Internet security. The situation we envision is some form of a group formation of the Buchanan (1965, 1999) type where members of

the group choose the size of the group membership, the amount of the public good, and the incentives (that is, Pigouvian penalties and subsidies) (see, for example, Fabella 2005, which shows how contractarian governance can, under certain conditions, restore Pareto optimality in situations that would otherwise have resulted in an invisible hand failure). A cooperative game theoretic formulation of this club theory is available (see, for example, Pauly 1967, 1970) and its specific application to Internet security along the lines contemplated here may be explored further.

We illustrate our results with specific functional forms and simulations.

Section 2 presents the model. Section 3 discusses the socially-optimal solution to the problem. Section 4 considers the individual's private solution, while Section 5 delves into the cooperative solution of the model. Section 6 presents specific examples, illustrations of specific functional forms, as well as some simulations. Section 7 presents the conclusions and summary of the paper.

## 2. THE MODEL

In this section, we study a model of 2 symmetric risk-neutral firms and  $h$  identical risk-neutral hackers, and in Section 8 generalize the model to  $n$  firms. Hacking requires an effort level  $e$  to each hacker, while firm 1 and firm 2 spend, respectively,  $x_1$  and  $x_2$  on private security goods, and  $y_1$  and  $y_2$  on public security goods. The government decides on the level of police enforcement expenditures,  $z$ . The hacking effort costs  $c(e)$ , while the cost of individual investments in private security goods, and the cost (per firm) of maintaining the police force, are respectively  $f(x)$  and  $g(z)$ , where  $f'(x) > 0$ ,  $f''(x) \geq 0$ ,

$g'(z) > 0$ , and  $g''(z) \geq 0$  by assumption. The cost per unit of non-rivalrous security goods are normalized to 1 for simplicity.

The hacker's optimization problem is

$$\text{Max}_e G(e, x_1, x_2, y_T(y_1, y_2), z) = e \cdot g(x_1, x_2, y_T(y_1, y_2), z) - c(e), \quad (4-1)$$

where  $g(\cdot)$  is the hacker's gain from hacking,  $c(e)$  is the cost of the effort to the hacker, and  $y_T$ , the total amount of non-rivalrous security goods available to both firms, equals  $y_1 + y_2$ . It is reasonable to suppose that the gain of the hacker decreases (at a decreasing rate) with an increase in any of the security measures  $x_1, x_2, y_T$ , and  $z$ , that is,  $\frac{\partial g}{\partial x_1} < 0$ ,

$$\frac{\partial g}{\partial x_2} < 0, \frac{\partial g}{\partial y_T} < 0, \frac{\partial g}{\partial z} < 0, \frac{\partial^2 g}{\partial x_1^2} > 0, \frac{\partial^2 g}{\partial x_2^2} > 0, \frac{\partial^2 g}{\partial y_T^2} > 0, \text{ and } \frac{\partial^2 g}{\partial z^2} > 0. \text{ We further}$$

assume that  $c'(e) > 0$  and  $c''(e) > 0$ .

The hacker's first-order condition is  $g(x_1, x_2, y_T(y_1, y_2), z) = c'(e)$ , which defines  $e = e(x_1, x_2, y_T(y_1, y_2), z)$  implicitly. Hence,

$$g(x_1, x_2, y_T(y_1, y_2), z) = c'(e(x_1, x_2, y_T(y_1, y_2), z)), \text{ and } \frac{\partial g}{\partial x_1} = c'' \cdot \frac{\partial e}{\partial x_1} \Rightarrow \frac{\partial e}{\partial x_1} = \frac{\frac{\partial g}{\partial x_1}}{c''} < 0;$$

$$\frac{\partial g}{\partial x_2} = c'' \cdot \frac{\partial e}{\partial x_2} \Rightarrow \frac{\partial e}{\partial x_2} = \frac{\frac{\partial g}{\partial x_2}}{c''} < 0; \text{ and } \frac{\partial g}{\partial z} = c'' \cdot \frac{\partial e}{\partial z} \Rightarrow \frac{\partial e}{\partial z} = \frac{\frac{\partial g}{\partial z}}{c''} < 0. \text{ That is, the effort}$$

level of the hacker decreases, *ceteris paribus*, with an increase in any of the security measures.

Define  $p(x_1, x_2, y_T(y_1, y_2), z)$  to be the probability of the loss,  $L(x_1, x_2, y_T(y_1, y_2), z)$  to be the magnitude of loss, and  $s(x_1, x_2, y_T(y_1, y_2), z) = L - g$  to be the deadweight social welfare loss from hacking.

Police enforcement and private precautions lower the probability of one's sites being attacked, thus:

$$p_z(x_1, x_2, y_T(y_1, y_2), z) < 0 \quad (4-2)$$

$$p_{x_i}(x_1, x_2, y_T(y_1, y_2), z) < 0. \quad (4-3)$$

Private security expenditures not only lower the probability of breach, but also lower the amount of the loss. For example, file recovery efforts like regular back-ups, and disaster planning strategies are designed to mitigate the amount of a loss arising from a computer incident. We also assume that public enforcement also lowers the magnitude of the loss, thus

$$L_{x_i}(x_1, x_2, y_T(y_1, y_2), z) < 0 \quad (4-4)$$

$$L_z(x_1, x_2, y_T(y_1, y_2), z) < 0. \quad (4-5)$$

Also, as mentioned in Chapters 1 and 2, in the Internet, security is interdependent. The lack of security in a network can cause damage not only to that network, but also to other networks linked to it. If a computer virus or worm, for instance, penetrates an unprotected machine, there is a chance that it can breach other computers as well, as in fact a lot of viruses reproduce themselves (Heal and Kunreuther 2003). Neglect by an individual therefore contributes to the probability of computer breach to other's systems. The probability of computer intrusion in one firm depends not only on its own

precautions, but also on the precautions of others. Likewise, one's private precautions lower the probability of breach not only of one's own computer systems but other systems as well. For example, if a computer administrator regularly uses anti-virus software, then it not only reduces its own probability of intrusion, but also lowers the probability that a virus or a worm can infect other computers through its machine. A very common example is the proliferation of emails with virus attachments. A person who does not anti-virus does not affect his/her machine only, since many viruses are programmed to be sent to others in the email group. Had the person used an anti-virus software and not been infected, the others would not have been infected also. Thus,

$$p_{x_2}(x_1, x_2, y_T(y_1, y_2), z) < 0. \quad (4-6)$$

We also assume that one's private security expenditures also reduce the amount of others' loss. Since compromised computers can be used to launch attacks against other computers, if one's computers are not secure, hackers can possibly stage the attack against other websites through one's systems. In the case of denial-of-service attacks (DoS) and distribute denial-of-service attacks (DDoS) against other sites, the amount of damage to the attacked site depends, among others, on the length of time of the attack and number of computers from where the attacks are staged. In essence, this implies that

$$L_{x_2}(x_1, x_2, y_T(y_1, y_2), z) < 0. \quad (4-7)$$

Finally, we assume that the following hold with respect the second and cross-partial derivatives:

$$p_{x_1 x_2}(x_1, x_2, y_T(y_1, y_2), z) > 0 \quad (4-8)$$

$$p_{x_1z}(x_1, x_2, y_T(y_1, y_2), z) > 0 \quad (4-9)$$

$$L_{x_1x_2}(x_1, x_2, y_T(y_1, y_2), z) > 0 \quad (4-10)$$

$$L_{zz}(x_1, x_2, y_T(y_1, y_2), z) > 0 \quad (4-11)$$

$$L_{x_1z}(x_1, x_2, y_T(y_1, y_2), z) > 0 \quad (4-12)$$

$$p_{zz}(x_1, x_2, y_T(y_1, y_2), z) > 0 \quad (4-13)$$

$$p_{x_1x_1}(x_1, x_2, y_T(y_1, y_2), z) > 0. \quad (4-14)$$

### 3. THE SOCIALLY-OPTIMAL SOLUTION

**Proposition 4-1.** The socially-optimum level of security is achieved by equalizing the marginal benefit to marginal cost ratios of each of the three alternatives -- private security investment, non-rivalrous security investment, and law enforcement measures.

**Proof.** The social planner's problem is

$$\begin{aligned} \text{Min} \quad & 2[f(x) + g(z)] + y_T + h \cdot \left\{ \begin{aligned} & c[e(x_1, x_2, y_T(y_1, y_2), z)] \\ & + e(x_1, x_2, y_T(y_1, y_2), z) \cdot s(x_1, x_2, y_T(y_1, y_2), z) \end{aligned} \right\} \\ & \{x, y_T, z\} \end{aligned} \quad (4-15)$$

The first-order conditions are:

$$\{x\} \quad 2f'(x) + h \cdot \{c' \cdot (e_{x_1} + e_{x_2}) + e \cdot (s_{x_1} + s_{x_2}) + s \cdot (e_{x_1} + e_{x_2})\} = 0 \quad (4-16)$$

$$\{y_T\} \quad 1 + h \cdot \{c' \cdot e_{y_T} + e \cdot s_{y_T} + s \cdot e_{y_T}\} = 0 \quad (4-17)$$

$$\{z\} \quad 2g'(z) + h \cdot \{c' \cdot e_z + e \cdot s_z + s \cdot e_z\} = 0. \quad (4-18)$$



From the hacker's first-order conditions, we know that  $c' = g$  and by definition we have

$s = L - g$  and  $p = \frac{h}{2}e$ . Substituting these into (4-16), (4-17) and (4-18), we know that,

respectively,

$$-(p_{x_1} + p_{x_2})L - p(s_{x_1} + s_{x_2}) = f'(x) \quad (4-19)$$

$$-2(p_{y_T}L + ps_{y_T}) = 1 \quad (4-20)$$

$$-p_z \cdot L - p \cdot s_z = g'(z) \quad (4-21)$$

The first term in equation (4-19),  $-(p_{x_1} + p_{x_2})L$  represents the total marginal *diversion effect*. That is, because of the observable precaution, the probability of intrusion of a website is reduced as hackers are diverted to other sites that don't have the observable precautions. Hence, the overall expected amount of loss caused by the hacker decreases as a result of installing observable precautions. In contrast to the standard results where the marginal diversion effect equals  $-p_{x_1}L$  (see Shavell 1991, p. 129), here, because of the interrelated of the security, the overall diversion effect has to account for the reduction in the probability of intrusion of a website as a result of the investments of security by the other website,  $-p_{x_2}L$ .

The second term in equation (4-19),  $-p(s_{x_1} + s_{x_2}) = 1$ , represents the marginal *social waste reduction effect* – it captures the expected reduction in the amount of deadweight social welfare loss as a result of the security investment. By definition, this term can be decomposed into the expected amount stolen from the firm,  $-p(L_{x_1} + L_{x_2})$ , that is, the marginal *theft reduction effect* in Shavell (1991)'s terminology, *minus* the expected

reduction of the gain to the hacker,  $-p(g_{x_1} + g_{x_2})$ . As evident from the first part of this decomposition, a website benefits from the security investment of another website which reduces the amount stolen from the first website. For example, in many cases, where compromised computers can be used to intrude into the target website, a stronger security infrastructure would decrease the amount of time the hacker would have to steal the target website's computer systems.

Thus, in contrast to previous results, equation (4-19) shows that with the externalities, the *social* marginal benefit of investing in security now includes not only the reduction of the probability or amount stolen from one's digital assets, but also the reduction of the probability of intrusion and amount stolen from the other website.

Dividing equations (4-19) and (4-21) by  $f'(x)$  and  $g'(z)$ , respectively, proves the proposition. Hence, under the socially-optimal solution, the marginal benefit to marginal cost ratios of the private security good, the public security good, and law enforcement measures are equalized:

$$\frac{-(p_{x_1} + p_{x_2})L - p(s_{x_1} + s_{x_2})}{f'(x)} = \frac{-2(p_{y_r}L + ps_{y_r})}{1} = \frac{-p_z \cdot L - p \cdot s_z}{g'(z)} \quad (4-22)$$

**Corollary 4-1.** The more responsive the probability and the magnitude of the loss is to a particular security measure, the more of that security measure should be used, holding constant the cost of providing such measure.

**Proof.** Note that equation (4-22) can be rewritten in elasticity form. Thus, defining

$\varepsilon_{p_1} = \frac{\partial p}{\partial x} \cdot \frac{x}{p}$ , and defining  $\varepsilon_{p_2}$ ,  $\varepsilon_{s_1}$ ,  $\varepsilon_{s_2}$ ,  $\varepsilon_{p_1}$ ,  $\varepsilon_{s_{y_1}}$ ,  $\varepsilon_{s_{y_2}}$ ,  $\varepsilon_{p_{y_1}}$ ,  $\varepsilon_{p_{y_2}}$ ,  $\varepsilon_{f_y}$ ,  $\varepsilon_{p_z}$ ,  $\varepsilon_{s_z}$ , and

$\varepsilon_{g_z}$  analogously, equation (4-22) becomes:

$$\frac{\left\{ \begin{array}{l} -\frac{pL}{x} \cdot (\varepsilon_{p_1} + \varepsilon_{p_2}) \\ -\frac{pS}{x} \cdot (\varepsilon_{s_1} + \varepsilon_{s_2}) \end{array} \right\}}{\frac{f}{x} \cdot \varepsilon_{f_x}} = \frac{\left\{ -2 \left[ \frac{pL}{x} \cdot \varepsilon_{p_{yT}} + \frac{pS}{y_T} \cdot \varepsilon_{s_{yT}} \right] \right\}}{1} = \frac{\left\{ -\frac{pL}{z} \cdot \varepsilon_{p_z} - \frac{pS}{z} \cdot \varepsilon_{s_z} \right\}}{\frac{g}{z} \cdot \varepsilon_{g_z}}. \quad (4-23)$$

Hence, the social planner adjusts the level of private rivalrous and non-rivalrous security investments, and law enforcement expenditures, in accordance with the responsiveness to them of the probability of loss, the amount of social loss, and the cost of providing the security measures. In general, the more responsive is the probability of loss and the social loss to private rivalrous investment, the higher is the optimal level of private rivalrous investment. The same thing applies to private non-rivalrous security investments, and the public expenditures on law enforcement. This is akin to price discrimination by a monopolist who sells in different markets, and charges price according to the price elasticity of demand in these markets. Of course, in the present security case, the social planner also needs to take into account the responsiveness of the costs to these changes in the level of the different security measures.

#### 4. THE INDIVIDUAL SOLUTION

**Proposition 4-2.** The interrelatedness of the risks causes individual firms to underinvest in private security.

**Proof.** Given the level of police enforcement and the firm 2's level of private and public security investments, firm 1 chooses  $x$  and  $y$  to:

$$\begin{aligned} \text{Min } & p(x_1, x_2, y_T(y_1, y_2), z) \cdot L(x_1, x_2, y_T(y_1, y_2), z) + f(x_1) + y_1 + g(z) \\ & \{x_1, y_1 \mid x_2, y_2, z\} \end{aligned} \quad (4-24)$$

where  $y_T = y_1 + y_2$ .

The first-order (optimality) conditions are:

$$\begin{aligned} \{x_1\} \quad & -p_{x_1}(x_1, x_2, y_T(y_1, y_2), z) \cdot L(x_1, x_2, y_T(y_1, y_2), z) \\ & - p(x_1, x_2, y_T(y_1, y_2), z) \cdot L_{x_1}(x_1, x_2, y_T(y_1, y_2), z) = f'(x) \end{aligned} \quad (4-25)$$

$$\begin{aligned} \{y_1\} \quad & -p_{y_T}(x_1, x_2, y_T(y_1, y_2), z) \cdot L(x_1, x_2, y_T(y_1, y_2), z) \\ & - p(x_1, x_2, y_T(y_1, y_2), z) \cdot L_{y_T}(x_1, x_2, y_T(y_1, y_2), z) = 1 \end{aligned} \quad (4-26)$$

Comparing equation (4-19) with (4-25) proves the proposition.

For the firm, the motivation behind investing in precaution (marginal benefit) is the reduction in the expected cost of the harm to it. Equation (4-26) states that, for individual precaution to be at the optimal level, the cost to the firm of a little more precaution, normalized to 1 unit, should equal the decrease in the expected cost of the loss from hacking, both in terms of reduction in the intrusion rate and the reduction in the loss from intrusions.

Equation (4-26) implies that

$$1 = -\frac{pL}{x}(\varepsilon_p + \varepsilon_l) \quad (4-27)$$

where  $\varepsilon_p = \frac{\partial p}{\partial x} \cdot \frac{x}{p}$ , etc.

Equation (4-27) says that the individual will equate the marginal cost to the reduction in the expected cost per unit of precaution multiplied by the sum of the responsiveness of both the probability and the magnitude of the loss to the change in one's own private security investment. The higher the expected loss and the more responsive the probability of the loss and the magnitude of the loss are to the amount of precaution, the higher is the marginal benefit of the precaution, and thus the higher is the optimal level of private precaution.

**Proposition 4-3.** The level of public security goods is also underprovided, the public good nature of the security investment causes the divergence of the level of public security expenditures from the socially-optimal amount. However, the externality effect drops out; that is, in the case of public security goods, the positive "externality" of the one's public security good investment to others is "internalized" by the firm in calculating its optimal level of public security goods.

**Proof.** Comparing (4-20) with (4-26) proves the proposition.

At first blush, it may seem that in the case of public security goods, there will both be the free-riding from the public good and the externality effect compounding together to worsen the underinvestment to a large extent. But upon perusal, we see that the "externality effect" drops out of the picture. The reason for this is that the individual already takes into account the positive effect upon him/her of the other person's use of his/her privately provided public security good. It is as if he/she is making the other person as his/her agent (in the legal sense of the word) in that he/she knows that if he/she invests in the public security good, that same good will be available to the other party,

which use of such good will reduce such party's intrusion, which will then also indirectly benefit the original spender as well.

This is thus one less problem associated with the market solution and one argument in favor of it compared to the government-provided-security alternative.

**Proposition 4-4.** The amount of underinvestment in both the private security and public security goods investment worsens as the number of firms increases.

**Proof.** See Section 8.

The question that we address next is how a website's choice of  $x^*$  and  $y^*$  changes with a change in the level of law enforcement expenditures,  $z$ .

**Proposition 4-5.** Under regular conditions, an increase in the government law enforcement expenditures lowers both private rivalrous and non-rivalrous expenditures, except if the cross elasticities of substitution between rivalrous and non-rivalrous security expenditures are so high they dominate the effect of the reduction in one type of private security expenditure caused by the increase in government expenditures.

**Proof.** The second website will face a similar optimization problem as the first website. We assume that the two firms are symmetrical so that  $x_1 = x_2$  and  $y_1 = y_2$  in equilibrium. Totally differentiating the first-order conditions given in equations (4-25) and (4-26), and, imposing symmetry, we arrive at a system of two equations, thus:

$$\begin{aligned} & \left[ (p_{x_1x_1} + p_{x_1x_2}) \cdot L + p_{x_1} \cdot (L_{x_1} + L_{x_2}) + (p_{x_1} + p_{x_2}) \cdot L_{x_1} + p \cdot (L_{x_1x_1} + L_{x_1x_2}) + f''(x) \right] \cdot dx \\ & + 2 \cdot \left[ p_{x_1y_1} \cdot L + p_{x_1} \cdot L_{y_1} + p_{y_1} \cdot L_{x_1} + p \cdot L_{x_1y_1} \right] \cdot dy \\ & + \left[ p_{x_1z} \cdot L + p_{x_1} \cdot L_z + p_z \cdot L_{x_1} + p \cdot L_{x_1z} \right] \cdot dz = 0 \end{aligned}$$

$$\begin{aligned} & \left[ (p_{y_T x_1} + p_{y_T x_2}) \cdot L + p_{y_T} \cdot (L_{x_1} + L_{x_2}) + (p_{x_1} + p_{x_2}) \cdot L_{y_T} + p \cdot (L_{y_T x_1} + L_{y_T x_2}) \right] \cdot dx \\ & + 2 \cdot \left[ p_{y_T y_T} \cdot L + p_{y_T} \cdot L_{y_T} + p_{y_T} \cdot L_{y_T} + p \cdot L_{y_T y_T} \right] \cdot dy \\ & + \left[ p_{y_T z} L + p_{y_T} L_z + p_z L_{y_T} + p \cdot L_{y_T z} \right] \cdot dz = 0 \end{aligned}$$

This is a system of implicit functions. Assuming that the determinant of the coefficient matrix at  $\{x^*, x^*, y^*, y^*, z\}$  is non-zero, by the implicit function theorem, we can solve for:

$$dx = -dz \cdot \frac{\begin{aligned} & \left[ p_{x_1 z} L + p_{x_1} L_z + p_z L_{x_1} + p \cdot L_{x_1 z} \right] \cdot \left[ 2 \cdot \begin{pmatrix} p_{y_T y_T} \cdot L + p_{y_T} \cdot L_{y_T} \\ + p_{y_T} \cdot L_{y_T} + p \cdot L_{y_T y_T} \end{pmatrix} \right] \\ & - \left[ p_{y_T z} L + p_{y_T} L_z + p_z L_{y_T} + p \cdot L_{y_T z} \right] \cdot \left[ 2 \cdot \begin{pmatrix} p_{x_1 y_T} \cdot L + p_{x_1} \cdot L_{y_T} \\ + p_{y_T} \cdot L_{x_1} + p \cdot L_{x_1 y_T} \end{pmatrix} \right] \end{aligned}}{D}$$

and

$$dy = -dz \cdot \frac{\begin{aligned} & \left[ p_{y_T z} L + p_{y_T} L_z + p_z L_{y_T} + p \cdot L_{y_T z} \right] \cdot \begin{pmatrix} (p_{x_1 x_1} + p_{x_1 x_2}) \cdot L + p_{x_1} \cdot (L_{x_1} + L_{x_2}) \\ + (p_{x_1} + p_{x_2}) \cdot L_{x_1} + p \cdot (L_{x_1 x_1} + L_{x_1 x_2}) + f''(x) \end{pmatrix} \\ & - \left[ p_{x_1 z} L + p_{x_1} L_z + p_z L_{x_1} + p \cdot L_{x_1 z} \right] \cdot \begin{pmatrix} (p_{y_T x_1} + p_{y_T x_2}) \cdot L + p_{y_T} \cdot (L_{x_1} + L_{x_2}) \\ + (p_{x_1} + p_{x_2}) \cdot L_{y_T} + p \cdot (L_{y_T x_1} + L_{y_T x_2}) \end{pmatrix} \end{aligned}}{D}$$

where

$$D = \begin{pmatrix} \left[ (p_{x_1 x_1} + p_{x_1 x_2}) \cdot L + p_{x_1} \cdot (L_{x_1} + L_{x_2}) + (p_{x_1} + p_{x_2}) \cdot L_{x_1} + p \cdot (L_{x_1 x_1} + L_{x_1 x_2}) + f''(x) \right] \cdot \left[ 2 \cdot \left[ p_{y_T y_T} \cdot L + p_{y_T} \cdot L_{y_T} + p_{y_T} \cdot L_{y_T} + p \cdot L_{y_T y_T} \right] \right] \\ - \left[ 2 \cdot \left[ p_{x_1 y_T} \cdot L + p_{x_1} \cdot L_{y_T} + p_{y_T} \cdot L_{x_1} + p \cdot L_{x_1 y_T} \right] \cdot \left[ (p_{y_T x_1} + p_{y_T x_2}) \cdot L + p_{y_T} \cdot (L_{x_1} + L_{x_2}) + (p_{x_1} + p_{x_2}) \cdot L_{y_T} + p \cdot (L_{y_T x_1} + L_{y_T x_2}) \right] \right] \end{pmatrix}$$

From the equations above, it is clear that  $\frac{dx}{dz} < 0$   $\left( \frac{dy}{dz} < 0 \right)$ , so long as it is not the case that both (a) the cross effects between  $x$  and  $y$  are so great and (b) the elasticity of substitution between  $z$  and  $y$  ( $z$  and  $x$ ) is much greater than that between  $z$  and  $x$  ( $z$  and  $y$ ), as to overwhelm the effect of reduction  $x$  ( $y$ ) as a result of increase in  $z$ . Thus, in general, public expenditures on law enforcement has a moral hazard effect: it reduces the propensity of firms to invest in private and public security goods for its own protection.

**Proposition 4-6.** (a) The government decidedly lowers the level of police enforcement in order to induce private firms to invest more in individual precautions. (b) As the number of firms,  $n$ , increases, and the amount of the underinvestment in private and public security goods investment correspondingly increase, the government also tailor-fits its adjustment according to the size of the underinvestment.

**Proof.** (a) Imposing symmetry, we have  $x_1^* = x_2^* = x^*$  and  $y_1 = y_2 = y^*$ , which are both functions implicitly of  $z$ .

The government thus chooses  $z$  in order to

$$\begin{aligned} \text{Min } & 2 \cdot [f(x^*(z)) + y^*(z) + g(z)] \\ & + h \cdot \left\{ c[e(x^*(z), x^*(z), y_T^*(y^*(z), y^*(z)), z)] + \right. \\ & \left. e(x^*(z), x^*(z), y_T^*(y^*(z), y^*(z)), z) \cdot s(x^*(z), x^*(z), y_T^*(y^*(z), y^*(z)), z) \right\} \end{aligned} \quad (4-28)$$

where  $y_T^* = y_1^*(z) + y_2^*(z)$ .

The first-order (optimality) condition is:



$$\begin{aligned}
& 2 \left[ f' \cdot \frac{\partial x^*}{\partial z} + \frac{\partial y^*}{\partial z} + g'(z) \right] + h \cdot \left[ c'(e) \cdot \left( e_{x_1} \frac{\partial x^*}{\partial z} + e_{x_2} \frac{\partial x^*}{\partial z} + 2e_{y_r} \frac{\partial y^*}{\partial z} + e_z \right) \right] \\
& + h \cdot e \cdot \left( s_{x_1} \frac{\partial x^*}{\partial z} + s_{x_2} \frac{\partial x^*}{\partial z} + 2s_{y_r} \frac{\partial y^*}{\partial z} + s_z \right) + h \cdot s \cdot \left( e_{x_1} \frac{\partial x^*}{\partial z} + e_{x_2} \frac{\partial x^*}{\partial z} + 2e_{y_r} \frac{\partial y^*}{\partial z} + e_z \right) = 0.
\end{aligned} \tag{4-29}$$

Solving for  $g'(z)$ , we have

$$-p_z L - p s_z - \frac{\partial x^*}{\partial z} [f'(x) + (p_{x_1} + p_{x_2})L + p(s_{x_1} + s_{x_2})] - \frac{\partial y^*}{\partial z} [1 + 2p_{y_r} L + 2ps_{y_r}] = g'(z). \tag{4-30}$$

Substituting in for the firm's first order conditions, equation (4-30) becomes:

$$-p_z L - p s_z - \frac{\partial x^*}{\partial z} [p_{x_2} L + pL_{x_2} - p \cdot (g_{x_1} + g_{x_2})] - \frac{\partial y^*}{\partial z} [p_{y_r} L + ps_{y_r} - pg_{y_r}] = g'(z) \tag{4-31}$$

Thus, by comparing (4-31) with (4-21), we know that the government will deliberately underprovide on public law enforcement expenditures by the sum of the amount of the individual's underinvestment in private and public security goods (that is, the difference between the social planner's and the private firm's first order conditions: equations (4-19) minus (4-25) and (4-20) minus (4-26)), weighted by the responsiveness of these security investments to law enforcement expenditures.

The proof of part (b) of the proposition ( $n$ -firm case) is in Section 8.

## 5. THE COOPERATIVE SOLUTION

**Proposition 4-7.** Under the social loss case (that is, if  $L = s$ ), a cooperative results in socially-optimal levels of expenditures in police enforcement and private and public security goods investments.

**Proof.** The cooperative's problem is to

$$\begin{aligned} \text{Min } & 2 \cdot p(x_1, x_2, y_T(y_1, y_2), z) \cdot L(x_1, x_2, y_T(y_1, y_2), z) + 2 \cdot f(x) + y_T + 2 \cdot g(z) \\ & x, y_T \end{aligned} \quad (4-32)$$

The first-order conditions are:

$$\{x\} \quad -[(p_{x_1} + p_{x_2})L + p(L_{x_1} + L_{x_2})] = f'(x) \quad (4-33)$$

$$\{y_T\} \quad -2[p_{y_T}L + pL_{y_T}] = 1 \quad (4-34)$$

which implies that

$$\frac{-[(p_{x_1} + p_{x_2})L + p(L_{x_1} + L_{x_2})]}{f'(x)} = -2[p_{y_T}L + pL_{y_T}] \quad (4-35)$$

### Government

$$\begin{aligned} \text{Min } & 2[f(x^{**}(z)) + g(z)] + y_T^{**}(z) \\ & + h \cdot \left\{ c[e(x^{**}(z), x^{**}(z), y_T^{**}(y^{**}(z), y^{**}(z)), z)] + \right. \\ & \left. e(x^{**}(z), x^{**}(z), y_T^{**}(y^{**}(z), y^{**}(z)), z) \cdot s(x^{**}(z), x^{**}(z), y_T^{**}(y^{**}(z), y^{**}(z)), z)] \right\} \end{aligned} \quad (4-36)$$

The first-order condition is equal to

$$-p_z L - ps_z - \frac{\partial x^{**}}{\partial z} [f'(x) + L(p_{x_1} + p_{x_2}) + p(s_{x_1} + s_{x_2})] - \frac{\partial y_T^{**}}{\partial z} [1 + 2p_{y_T}L + 2ps_{y_T}] = g'(z) \quad (4-37)$$

Substituting in the collective's first-order condition (and if  $L = s$ ), this reduces to

$$-p_z L - ps_z = g'(z). \quad (4-38)$$

As can be seen from the results of this section, a cooperative solution promises to approximate well the socially-optimal solution. This finding is consistent with the

present move of the U.S. government to encourage the formation of ISACs. The question that now arises however is how ISAC group members among themselves can allocate the costs associated with generating the (public) security goods. Other than the ISAC member bargaining among themselves, one mechanism that could be explored is the creation of tradeable externality permits among the members of ISACs themselves, with the overall group “quota” on the externality determined by the coalition on the basis of optimization by the collective. Thus, under this scenario, the overall level of externalities that will be allowed will be determined on the basis on optimization by the collective, and then, the distribution of allowable externalities among the members will be priced out the members – that is, those desirous to “use” the externality will purchase the externality permit by bidding for it.

If such “market-based” allocation of the externality would prove to be unwieldy in practice, then another solution that can be considered is the allocating among the members on the basis of his or her Shapley value:

$$\psi_i = \sum_C \frac{(n-k)!(k-1)!}{n!} [v(C) - v(C - \{i\})] \quad (4-39)$$

where  $k$  is the size of the coalition  $C$ ,  $n$  is the total players,  $v(C)$  is the value of the coalition,  $v(C - \{i\})$  is the value of the coalition without player  $i$ , and where the sum is taken over all the coalition  $C$  that includes  $i$  as a member. Since  $[v(C) - v(C - \{i\})]$  is the marginal contribution of  $i$  to the coalition  $C$ , the Shapley value of  $i$  simply reflects the expected marginal contribution of  $i$ . Hence, the Shapley value would be an appropriate measure in this case, since it approximates what an actual market mechanism would reward to the member for his/her contribution, and the Shapley value is a way of tying

the pay-offs to the member's marginal productivity, when an actual market cannot be arranged. This approach of applying the principles of cooperative game theory has been adopted in various cost-allocation games such as municipal cost-sharing (see, for example, Suzuki and Nakayama 1976; Young, Okada, and Hashimoto 1982), building airport runways (see, for example, Littlechild 1974, Littlechild and Owen 1973), and minimum cost spanning tree games (see, for example, Granot and Huberman 1981, Granot and Huberman 1984, Megiddo 1978).

Another form of decentralized group solution that can be utilized is one of the Buchanan (1965; 1999) type where the members of the group choose the size of the group membership, the amount of the public good, and the incentives (that is, Pigouvian penalties and subsidies) (see, for example, Fabella 2005). A cooperative game-theoretic formulation of this club theory is available (see, for example, Pauly 1967, 1970) and its specific application to Internet security along the lines contemplated here may be explored further.

In sum, some form of decentralized group formation can be used to help address the problem of Internet security. Thus, it does not necessarily mean that just because there is a market failure arising from the public goods and externalities aspects of Internet security, government role is automatically prescribed to the exclusion of the private sector. Instead, both public and private sector initiatives can be utilized together.

In Table 4-2 below, we summarize the amounts of privately-provided private and public security goods, and the level of government-provided law enforcement expenditures, under different scenarios.

**Table 4-2.** Summary of First-Order Conditions and Level of Security Investments  
(By Type of Agent and Security Investment)

	<b>First Order Condition (x)</b>	<b>Level of Private Security Good</b>
Individual	$-p_{x_1} \cdot L - p \cdot L_{x_1} = f'(x)$	$x^*$
Collective	$-(p_{x_1} + p_{x_2})L - p(L_{x_1} + L_{x_2}) = f'(x)$	$x^{**}$
Socially Optimal	$-(p_{x_1} + p_{x_2})L - p(s_{x_1} + s_{x_2}) = f'(x)$	$x^o$
	<b>First Order Condition (y)</b>	<b>Level of Public Security Good</b>
Individual	$-p_{y_T} L - pL_{y_T} = 1$	$y^*$
Collective	$-2[p_{y_T} L + pL_{y_T}] = 1$	$y^{**}$
Socially Optimal	$-2[p_{y_T} L + ps_{y_T}] = 1$	$y^o$
	<b>First Order Condition (z)</b>	<b>Public Enforcement of Law</b>
Individual	$-p_z L - ps_z - \frac{\partial x^*}{\partial z} [p_{x_2} L + pL_{x_2} - p \cdot (g_{x_1} + g_{x_2})]$ $- \frac{\partial y^*}{\partial z} [p_{y_T} L + ps_{y_T} - pg_{y_T}] = g'(z)$	$z^*$
Collective	$-p_z L - ps_z = g'(z)$	$z^{**}$
Socially Optimal	$-p_z L - ps_z = g'(z)$	$z^o$

## 6. EXAMPLES AND SIMULATIONS

We can illustrate the abovementioned results and make the discussions more concrete by specifying functional forms. We adopt the following functional specifications for the probability and loss functions:

$$p(x_1, x_2, y_T, z) = (1-q)e^{-(\alpha x_1 y_T + \theta z)} + qe^{-(\alpha x_1 y_T + \beta x_2 y_T + \theta z)} \quad (4-40)$$

$$L(x_1, x_2, y_T, z) = A[(1-q) \cdot (x_1 y_T)^a z^c + q \cdot (x_1 y_T)^a (x_2 y_T)^b z^c] \quad (4-41)$$

$$g(x_1, x_2, y_T, z) = \lambda(x_1, x_2, y_T, z) \cdot A[(1-q) \cdot (x_1 y_T)^a z^c + q \cdot (x_1 y_T)^a (x_2 y_T)^b z^c] \quad (4-42)$$

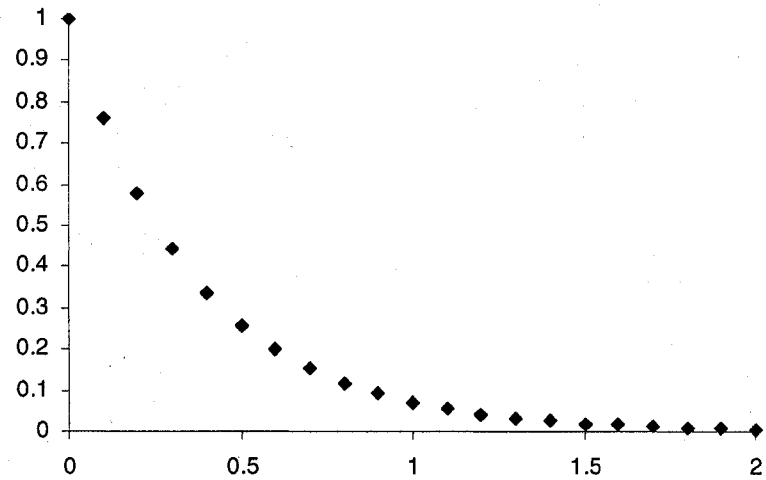
where  $\lambda \in [0, 1]$ . Thus,

$$s(x_1, x_2, y_T, z) = [1 - \lambda] \cdot A \left[ (1 - q) \cdot (x_1 y_T)^a z^c + q \cdot (x_1 y_T)^a (x_2 y_T)^b z^c \right] \quad (4-43)$$

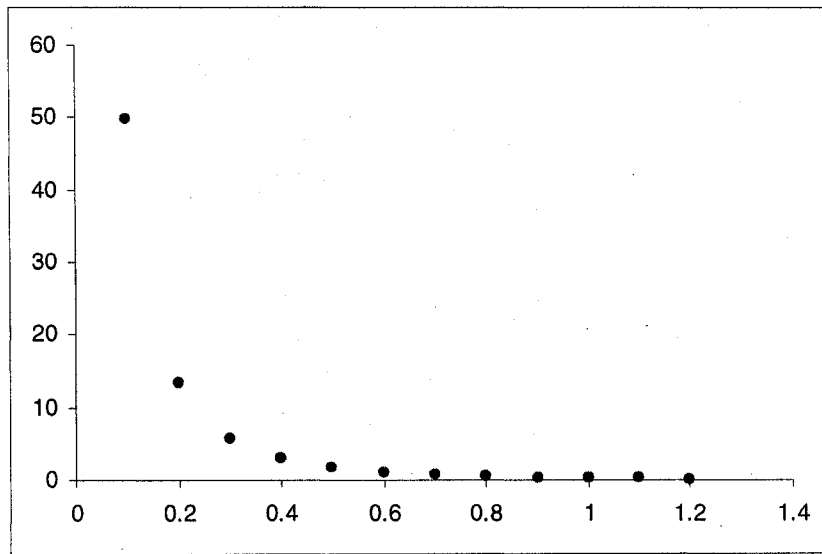
We assume  $0 < \alpha, \beta, \theta \leq 1$ .

We thus decompose the attack into direct attacks and attacks staged indirectly through other compromised computers. Thus, equation (4-40) tells us that total probability of attack to firm 1 is the combination of the direct attack probability,  $e^{-(\alpha_1 y_T + \theta z)}$ , and the probability that firm 1 will be attacked indirectly through firm 2,  $e^{-(\alpha_1 y_T + \beta x_2 y_T + \theta z)}$ .  $(1 - q)$  provides a relative measure of the number of the *direct* computer attacks, while  $q$  provides a relative measure of attacks staged *indirectly* through other compromised computers. Thus,  $q$  measures the strength of the interdependence of the security of the two firms. That is, if  $q = 0$ , the indirect effect,  $q \cdot e^{-(\alpha_1 y_T + \beta x_2 y_T + \theta z)}$ , drops out and the probability of attack is simply the probability of direct attack to firm 1. On the other hand, a relatively large  $q$  signifies that firm 1 must guard not only against direct attacks to its systems, but also attacks and viruses coming from computer computers. Normally, we expect  $q$  to be greater than 0, reflecting the interdependent nature of computer security, and at the same time  $q$  is expected to be less than 1/2, signifying that direct attacks always account for the greater portion of attacks than indirect attacks.

We note that the probability of attack ranges from 0 to 1 – as it ought to be – under these functional forms. Also, the probability of attack decreases with an increase in the level of the private security investment, the public security investment, or the law enforcement expenditures (see Figure 4-2 below). The same thing holds true for the magnitude of the loss. Thus, the probability times the magnitude of the loss goes down with  $x$ ,  $y_T$ , and  $z$  (see, for example, Figure 4-3 below).



**Figure 4-2.**  $p(x_1, x_2, y_T, z)$  when  $x_1 = x_2 = z, y_T = 1$



**Figure 4-3.**  $p(x_1, x_2, y_T, z) \cdot L(x_1, x_2, y_T, z)$  when  $x_1 = x_2 = z, y_T = 1$

We also note that an increase in the security investment of firm 2, decreases the indirect attack probability (that is,  $\frac{\partial e^{-(\alpha x_1 y_T + \beta x_2 y_T + \theta z)}}{\partial x_2} < 0$ ), but doesn't affect the direct

attack probability, as  $\frac{\partial e^{-(\alpha x_1 y_T + \theta z)}}{\partial x_2} = 0$ . In contrast, firm 1 can decrease the probability

that its systems will be breached either directly or indirectly by increasing its own

precaution,  $x_1$ , since both  $\frac{\partial e^{-(\alpha x_1 y_T + \theta z)}}{\partial x_1}$  and  $\frac{\partial e^{-(\alpha x_1 y_T + \beta x_2 y_T + \theta z)}}{\partial x_1}$  are negative.

The parameters  $\alpha$ ,  $\beta$ , and  $\theta$  measure the relative effectiveness of one's own precautions, other's precautions, and police protection, respectively, in reducing computer intrusions in one's systems, while  $a$ ,  $b$ , and  $c$  measure the same with respect to the reduction in the magnitude of the loss. We calculate next the first, second, and cross-partial derivatives, thus:

$$L_{x_1} = A \left[ (1-q) \alpha x_1^{a-1} y_T^a z^c + q \alpha x_1^{a-1} y_T^a (x_2 y_T)^b z^c \right] \quad (4-44)$$

$$L_{x_2} = A q (x_1 y_T)^a b x_2^{b-1} y_T^b z^c \quad (4-45)$$

$$L_{y_T} = A \left[ (1-q) x_1^a a y_T^{a-1} z^c + q x_1^a x_2^b (a+b) y_T^{a+b-1} z^c \right] \quad (4-46)$$

$$L_z = A \left[ (1-q) (x_1 y_T)^a c z^{c-1} + q (x_1 y_T)^a (x_2 y_T)^b c z^{c-1} \right] \quad (4-47)$$

$$p_{x_1} = -\alpha y_T \cdot \left[ (1-q) \cdot e^{-(\alpha x_1 y_T + \theta z)} + q \cdot e^{-(\alpha x_1 y_T + \beta x_2 y_T + \theta z)} \right] \quad (4-48)$$

$$p_{x_2} = -\beta y_T \cdot \left[ q \cdot e^{-(\alpha x_1 y_T + \beta x_2 y_T + \theta z)} \right] \quad (4-49)$$

$$p_{y_T} = -\alpha x_1 (1-q) e^{-(\alpha x_1 y_T + \theta z)} - (\alpha x_1 + \beta x_2) q e^{-(\alpha x_1 y_T + \beta x_2 y_T + \theta z)} \quad (4-50)$$

$$p_z = -\theta \left[ (1-q) \cdot e^{-(\alpha x_1 y_T + \theta z)} + q \cdot e^{-(\alpha x_1 y_T + \beta x_2 y_T + \theta z)} \right] \quad (4-51)$$

$$L_{x_1 x_1} = A \left[ (a-1)(1-q) \alpha x_1^{a-2} y_T^a z^c + q a (a-1) x_1^{a-2} y_T^a (x_2 y_T)^b z^c \right] \quad (4-52)$$

$$L_{x_1 x_2} = A q \alpha x_1^{a-1} y_T^a b x_2^{b-1} y_T^b z^c \quad (4-53)$$

$$L_{x_1 y_T} = A \left[ (1-q) \alpha x_1^{a-1} a y_T^{a-1} z^c + q \alpha x_1^{a-1} x_2^b (a+b) y_T^{a+b-1} z^c \right] \quad (4-54)$$



$$L_{x_1z} = A[(1-q)ax_1^{a-1}y_T^a cz^{c-1} + qax_1^{a-1}y_T^a(x_2y_T)^b cz^{c-1}] \quad (4-55)$$

$$p_{x_1x_1} = (\alpha y_T)^2 [(1-q)e^{-(\alpha_1 y_T + \theta z)} + qe^{-(\alpha_1 y_T + \beta x_2 y_T + \theta z)}] = (\alpha y_T)^2 \cdot p \quad (4-56)$$

$$p_{x_1x_2} = (\alpha y_T)(\beta y_T) [qe^{-(\alpha_1 y_T + \beta x_2 y_T + \theta z)}] \quad (4-57)$$

$$\begin{aligned} p_{x_1y_T} &= -\alpha [(1-q)e^{-(\alpha_1 y_T + \theta z)} + qe^{-(\alpha_1 y_T + \beta x_2 y_T + \theta z)}] \\ &\quad - (\alpha y_T) [(1-q)e^{-(\alpha_1 y_T + \theta z)} (-\alpha x_1) + qe^{-(\alpha_1 y_T + \beta x_2 y_T + \theta z)} (-\alpha x_1 - \beta x_2)] \\ &= -\alpha \cdot p - (\alpha y_T) \cdot p_{y_T} \end{aligned} \quad (4-58)$$

$$p_{x_1z} = -(\alpha y_T) [(1-q)e^{-(\alpha_1 y_T + \theta z)} (-\theta) + qe^{-(\alpha_1 y_T + \beta x_2 y_T + \theta z)} (-\theta)] = -(\alpha y_T) \cdot p_z \quad (4-59)$$

We now illustrate the important points of our simulations with the use of graphs.

Figure 4-4 shows that the optimal level of Internet security should be determined by balancing the trade-off between the reduction in the probability times the magnitude of the loss and the cost associated with providing the security. Figure 4-5, on the other hand, depicts the marginal benefit of the precaution to the individual firm vis-à-vis the marginal benefit to the cooperative. The optimal level of precaution is determined by equalizing the marginal benefit to the marginal cost.

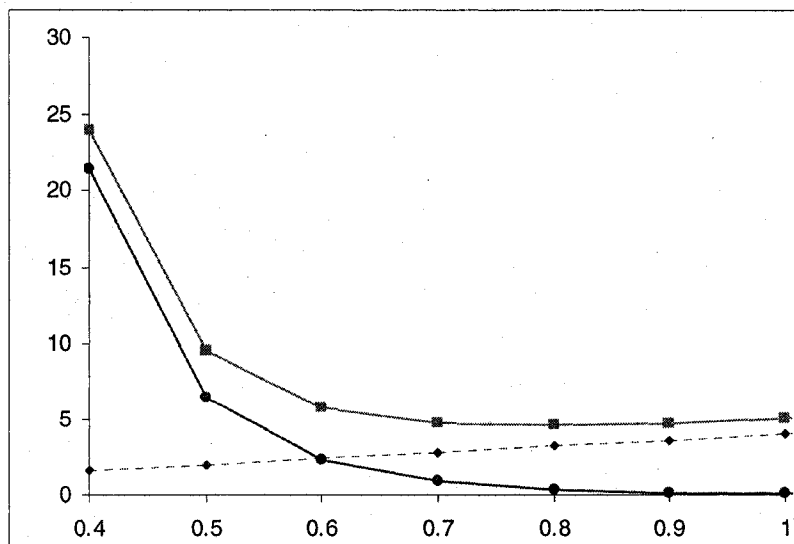


Figure 4-4.  $p \cdot L + f(x_1) + y_T + g(z)$  when  $x_1 = x_2 = z$ ,  $y_T = 1$ ,  $f(x_1) = 4x_1$

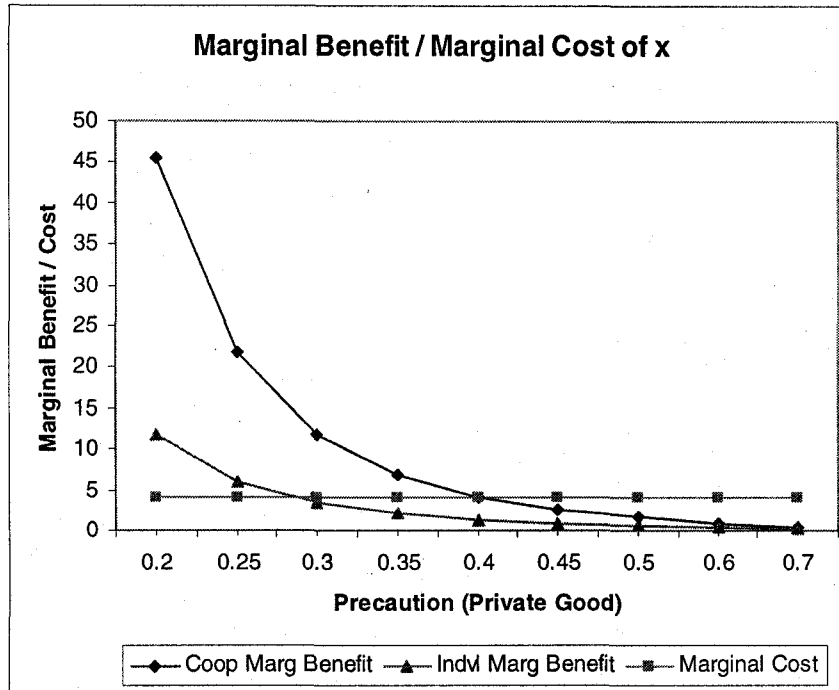
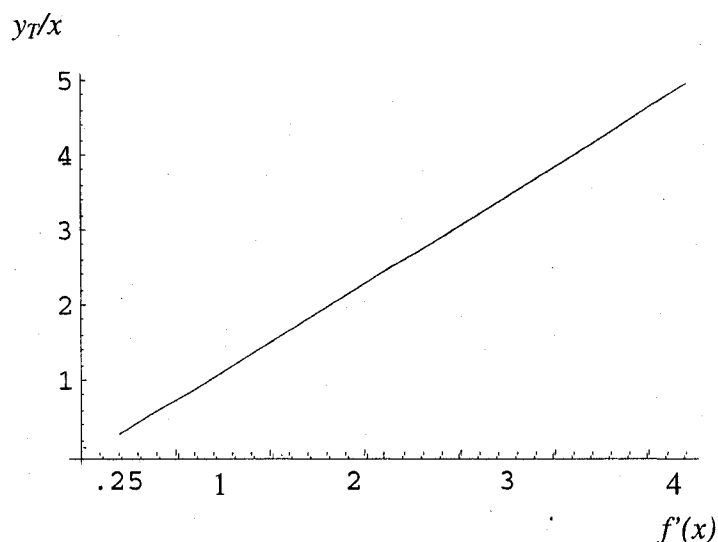


Figure 4-5. Optimal private precaution: cooperative vs. individual solution

Also, as Proposition 1 implies, the marginal cost of a particular type of security measure is an important consideration in determining the optimal-level of investment in that security measure relative to the others. Our simulations confirm this point. Thus, under the abovementioned functional specifications, we find that as the marginal cost of the private security good increases, *ceteris paribus*, the investment in private security measures decreases relative to the level of investment in public security goods. More specifically, for the collective and social planner,  $\frac{y_T}{x} = 2f'(x)$  for any parameter specification. (Mathematically, the reason for this is that, looking at the marginal benefit of  $x$  and  $y_T$  for the collective and the social planner, we see that  $p_{y_T}$  is basically equal to  $p_{x_1} + p_{x_2}$  -- and  $L_{y_T}(s_{y_T})$  is basically equal to  $L_{x_1} + L_{x_2}(s_{x_1} + s_{x_2})$  -- with the  $x$  and  $y_T$  interchanged. Thus, from the first-order conditions, we know that that the marginal

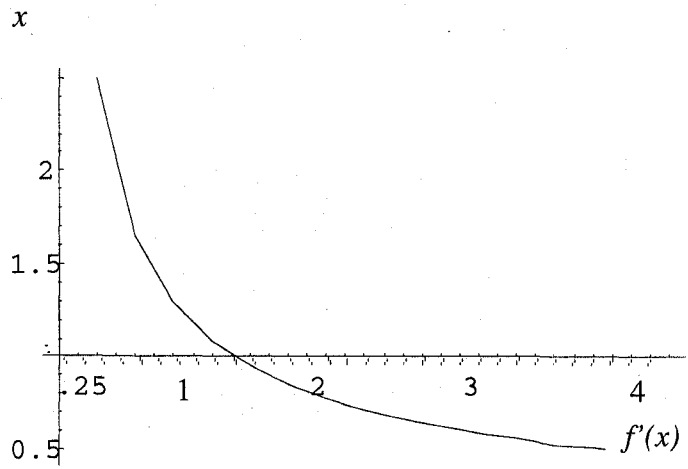
conditions for  $x$  and  $y_T$  are simply differentiated by 2, the number of firms, and  $f'(x)$ , the marginal cost of  $x$  (since the marginal cost of  $y_T$  is normalized to 1).)

As for the individual solution, although the relationship between  $y_T$  and  $x$  is not as neatly summarized by a formula,<sup>195</sup> our simulations show however that  $\frac{y_T}{x}$  nonetheless monotonically increases with the marginal cost of  $x$ , *ceteris paribus*. We find this to be true for different values of  $\alpha$ ,  $\beta$ ,  $\theta$ ,  $\lambda$ ,  $q$ ,  $a$ ,  $b$ , and  $c$ . Thus, for example, if  $q = 0.5$ ,  $\alpha = 1.5$ ,  $\beta = 1$ ,  $\theta = 0.5$ ,  $a = -1.5$ ,  $b = -1$ ,  $c = -0.5$ ,  $\lambda = 0.5$ , and  $g'(z) = 4$ , we have:

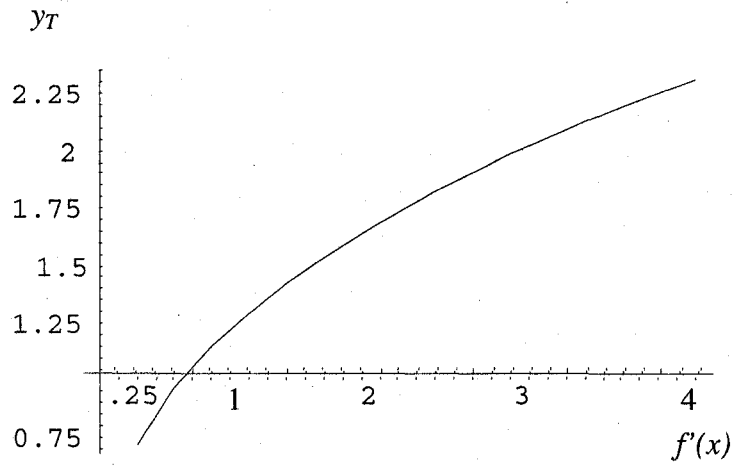


**Figure 4-6.** Individual firm's  $y_T/x$  as a function of  $f'(x)$

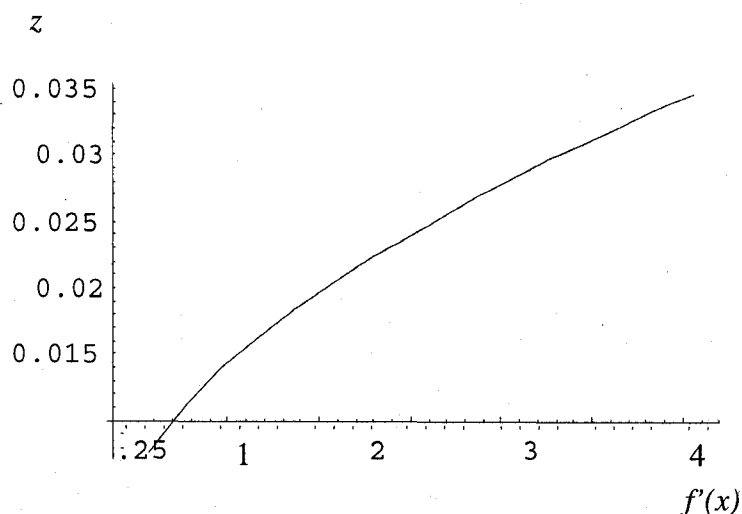
<sup>195</sup> The reason for the difference between the individual and the collective/socially-optimal cases will be discussed in the next result.



**Figure 4-7.** Individual firm's  $x$  as a function of  $f'(x)$



**Figure 4-8.** Individual firm's  $y_T$  as a function of  $f'(x)$



**Figure 4-9.** Individual firm's  $z$  as a function of  $f'(x)$

Thus, as the above simulations illustrate, if the (marginal) costs of a security measure are high, the firms will tend to provide less of that security measure and substitute it with the others.

Another important finding we gather from the simulations is that, as  $q$ , the measure of interdependence, increases, the individual firm will increase investment in public security goods,  $y_T$ , relative to its investment in private security goods,  $x$ .<sup>196</sup> The reason for this is that, looking at the first-order conditions for  $y_T$  and  $x$ , we see that the marginal benefit of the public and private security goods are differentiated by the terms  $\beta x_2 \cdot qe^{-(\alpha x_1 y_T + \beta x_2 y_T + \theta z)}$  and  $b \cdot q x_1^a x_2^b y_T^{a+b-1} z$ , representing the *additional* reduction in both the probability and magnitude of the loss that the individual firm achieves because its public security goods

<sup>196</sup> Thus, for  $\alpha = 1.5$ ,  $\beta = 1$ ,  $\theta = 0.5$ ,  $\lambda = 0.5$ ,  $a = -1.5$ ,  $b = -1$ ,  $c = -0.5$ ,  $f'(x) = 4$ , and  $g'(z) = 0.5$ , we have  $x = 0.1923, 0.2141$ , and  $0.2355$  for  $q = 0.2, 0.5$ , and  $0.8$  respectively, while  $y_T = 1.0232, 1.2626$ , and  $1.49$ , for the same values of  $q$ . Again, we have rigorously tried the simulations for different values of the parameters (for example, high  $f'(x)$  case, low  $f'(x)$  case, high  $g'(z)$ , low  $g'(z)$ , high/low  $\alpha$ , high/low  $\theta$ , high  $\lambda$ /low  $\lambda$ , high/low  $|a|$ , etc.) and the result remains the same.

investment is being used by other firm, which use in turn benefits firm 1. Hence, although firm 2 is technically free-riding on firm 1's investment in public security good, such free-riding is actually benefiting firm 1, because the more secure firm 2 is, the less firm 1 is affected by intrusions coming its way through firm 2. Hence, the more interrelated cybersecurity is, the higher an individual firm's public security investment relative to private security investment tends to be.

In contrast, the ratio of public-to-private security goods investment of both the social planner and the collective is constant at  $\frac{y_T}{x} = 2 \cdot f'(x)$  and doesn't vary with the level of security interdependence,  $q$ . This formula states that the collective and social-planner will choose more public security investment relative to private security investment as its weapon of attack against cybercrimes, the higher the marginal cost of private security goods is, and the higher the number of firms (2 in this case). However, both the collective and the social planner will not vary their public-to-private security goods ratio according to the level of interdependence. On the other hand, although the individual firm also takes into account the marginal cost and the number of firms in its determination of its public-to-private security goods ratio, it also, on top of the above considerations, includes the level of interdependence in its calculation. The higher the level of interdependence, the bigger the bang per buck of its public security investment will be, since the more interdependent firms' security are, the more will the "free-riding" by the other firms in its public goods investment benefit it.<sup>197</sup> This phenomenon, however, does not apply in the case of the socially-optimal and the collective solution

---

<sup>197</sup> In other words, the greater the interdependence, the more will a firm want other firms to "free-ride" on its non-rivalrous security investment.

because the social planner and the cooperative already takes into account the external effects of both the public goods *and* the private goods investment on other firms' security, and so, the ratio  $\frac{y_T}{x}$  is constant for different levels of  $q$  in those cases. In contrast, in the case of the individual firm, while the public goods investments are available for use by the other firms (and which use by other firms benefits the security of the provider of the public security good), the private goods investments (by definition) are not. Hence, for the individual firm, the ratio  $\frac{y_T}{x}$  is higher the greater  $q$  is; for the collective and the social planner, such ratio is constant with  $q$  and follows the

$$\frac{y_T}{x} = 2 \cdot f'(x) \text{ formula.}$$

## 7. CONCLUSIONS

In reality, crimes are solved by a combination of private precautions and public enforcement of the law. Thus, in this paper, we studied a model where crimes are addressed through a combination of private and public measures. By so doing, we were able to capture the substitutability between the private and public responses as well as determine the optimal combination of those approaches.

In addition, our model captured two other important aspects of cybercrime protection. First, in the Internet, individual precautions can take one of two forms: (a) investments in private security goods (such as the purchase of firewalls); or (b) investments in non-rivalrous security goods (such as compiling information on software vulnerabilities, security holes, security incidents, and hacking patterns) which therefore have aspects of public goods. Second, in the Internet, there are significant interrelatedness of risks,

which give rise to externalities among individual websites. That is, we studied a model that combines all of these elements: private investments in security; investments in security that has the nature of public goods; externalities; and public enforcement of law.

We found that the socially-optimal level of security is achieved by equalizing the marginal-benefit-to-marginal-cost ratios of each of the three alternatives – private security investment, non-rivalrous security investment, and law enforcement measures. Furthermore, the interrelatedness of Internet risks causes individual firms to underinvest in private and public security goods. The government thus decidedly lowers the level of police enforcement expenditures in order to induce firms to invest more in individual precautions. We also found that, under certain conditions, cooperation results in socially-optimal levels of expenditures in private and public security goods expenditures. Our simulations illustrated the results of the model under several scenarios.

## 8. GENERAL CASE: $n$ FIRMS

### Social Planner

$$\begin{array}{l} \text{Min} \\ \{x, y_T, z\} \end{array} \quad \begin{array}{l} n[f(x) + g(z)] + y_T \\ + h \cdot \left\{ \begin{array}{l} c[e(x_1, x_2, \dots, x_n, y_T(y_1, y_2, \dots, y_n), z)] \\ + e(x_1, x_2, \dots, x_n, y_T(y_1, y_2, \dots, y_n), z) \cdot s(x_1, x_2, \dots, x_n, y_T(y_1, y_2, \dots, y_n), z) \end{array} \right\} \end{array} \quad (4-A1)$$

where:

$$y_T = y_1 + y_2 + \dots + y_n$$

First Order Conditions:



$$\{x\} \quad nf'(x) + h \cdot \{c' \cdot (e_{x_1} + e_{x_2} + \dots + e_{x_n}) + e \cdot (s_{x_1} + s_{x_2} + \dots + s_{x_n}) + s \cdot (e_{x_1} + e_{x_2} + \dots + e_{x_n})\} = 0 \quad (4-A2)$$

$$\{y_T\} \quad 1 + h \cdot \{c' \cdot e_{y_T} + e \cdot s_{y_T} + s \cdot e_{y_T}\} = 0 \quad (4-A3)$$

$$\{z\} \quad ng'(z) + h \cdot \{c' \cdot e_z + e \cdot s_z + s \cdot e_z\} = 0. \quad (4-A4)$$

Applying

$$c' = g; s = L - g; p = \frac{h}{n}e \Rightarrow e = \frac{np}{h}, e_{x_1} = \frac{n}{h}p_{x_1}, \text{ etc.},$$

we have:

$$-\left(\sum_{i=1}^n p_{x_i}\right) \cdot L - p \cdot \left(\sum_{i=1}^n s_{x_i}\right) = f'(x) \quad (4-A5)$$

$$-n(p_{y_T}L + ps_{y_T}) = 1 \quad (4-A6)$$

$$-p_z \cdot L - p \cdot s_z = g'(z) \quad (4-A7)$$

### The Individual Solution

$$\begin{aligned} \text{Min} \quad & p(x_1, x_2, \dots, x_n, y_T(y_1, y_2, \dots, y_n), z) \cdot L(x_1, x_2, \dots, x_n, y_T(y_1, y_2, \dots, y_n), z) \\ & + f(x_1) + y_1 + g(z) \end{aligned} \quad (4-A8)$$

$$\left\{ \begin{array}{l} x_1, y_1 \\ x_2, y_2, \dots, x_n, y_n, z \end{array} \right\}$$

$$\{x_1\} \quad -p_{x_1} \cdot L - p \cdot L_{x_1} = f'(x) \quad (4-A9)$$

$$\{y_1\} \quad -p_{y_T} \cdot L - p \cdot L_{y_T} = 1 \quad (4-A10)$$

Notes: As  $n$  increases, underinvestment worsens!

Also, the “public good effect” worsens.

Totally differentiating the FOCs and imposing symmetry, we have:

$$\begin{aligned}
& \left[ \left( \sum_{i=1}^n p_{x_i x_i} \right) \cdot L + p_{x_1} \cdot \left( \sum_{i=1}^n L_{x_i} \right) + \left( \sum_{i=1}^n p_{x_i} \right) \cdot L_{x_1} + p \cdot \left( \sum_{i=1}^n L_{x_i x_i} \right) + f''(x) \right] \cdot dx \\
& + n \cdot \left[ p_{x_1 y_T} \cdot L + p_{x_1} \cdot L_{y_T} + p_{y_T} \cdot L_{x_1} + p \cdot L_{x_1 y_T} \right] \cdot dy \\
& + \left[ p_{x_1 z} L + p_{x_1} L_z + p_z L_{x_1} + p \cdot L_{x_1 z} \right] \cdot dz = 0
\end{aligned} \tag{4-A11}$$

$$\begin{aligned}
& \left[ \left( \sum_{i=1}^n p_{y_T x_i} \right) \cdot L + p_{y_T} \cdot \left( \sum_{i=1}^n L_{x_i} \right) + \left( \sum_{i=1}^n p_{x_i} \right) \cdot L_{y_T} + p \cdot \left( \sum_{i=1}^n L_{y_T x_i} \right) \right] \cdot dx \\
& + n \cdot \left[ p_{y_T y_T} \cdot L + p_{y_T} \cdot L_{y_T} + p_{y_T} \cdot L_{y_T} + p \cdot L_{y_T y_T} \right] \cdot dy \\
& + \left[ p_{y_T z} L + p_{y_T} L_z + p_z L_{y_T} + p \cdot L_{y_T z} \right] \cdot dz
\end{aligned} \tag{4-A12}$$

Again, assuming that the determinant of the coefficient matrix at  $\{x^*, \dots, x^*, y^*, \dots, y^*, z\}$

is non-zero, by the implicit function theorem, we have:

$$dx = -dz \cdot \frac{\left\{ \begin{aligned} & \left[ p_{x_1 z} L + p_{x_1} L_z + p_z L_{x_1} + p \cdot L_{x_1 z} \right] \cdot \left[ n \cdot \left( \begin{aligned} & p_{y_T y_T} \cdot L + p_{y_T} \cdot L_{y_T} \\ & + p_{y_T} \cdot L_{y_T} + p \cdot L_{y_T y_T} \end{aligned} \right) \right] \\ & - \left[ p_{y_T z} L + p_{y_T} L_z + p_z L_{y_T} + p \cdot L_{y_T z} \right] \cdot \left[ n \cdot \left( \begin{aligned} & p_{x_1 y_T} \cdot L + p_{x_1} \cdot L_{y_T} \\ & + p_{y_T} \cdot L_{x_1} + p \cdot L_{x_1 y_T} \end{aligned} \right) \right] \end{aligned} \right\}}{D} \tag{4-A13}$$

and

$$dy = -dz \cdot \frac{\left\{ \begin{aligned} & \left[ p_{y_T z} L + p_{y_T} L_z + p_z L_{y_T} + p \cdot L_{y_T z} \right] \cdot \left( \begin{aligned} & \left( \sum_{i=1}^n p_{x_i x_i} \right) \cdot L + p_{x_1} \cdot \left( \sum_{i=1}^n L_{x_i} \right) \\ & + \left( \sum_{i=1}^n p_{x_i} \right) \cdot L_{x_1} + p \cdot \left( \sum_{i=1}^n L_{x_i x_i} \right) + f''(x) \end{aligned} \right) \\ & - \left[ p_{x_1 z} L + p_{x_1} L_z + p_z L_{x_1} + p \cdot L_{x_1 z} \right] \cdot \left( \begin{aligned} & \left( \sum_{i=1}^n p_{y_T x_i} \right) \cdot L + p_{y_T} \cdot \left( \sum_{i=1}^n L_{x_i} \right) \\ & + \left( \sum_{i=1}^n p_{x_i} \right) \cdot L_{y_T} + p \cdot \left( \sum_{i=1}^n L_{y_T x_i} \right) \end{aligned} \right) \end{aligned} \right\}}{D} \tag{4-A14}$$

where

$$D \equiv \left\{ \begin{array}{l} \left( \left( \sum_{i=1}^n p_{x_i x_i} \right) \cdot L + p_{x_i} \cdot \left( \sum_{i=1}^n L_{x_i} \right) + \left( \sum_{i=1}^n p_{x_i} \right) \cdot L_{x_i} + p \cdot \left( \sum_{i=1}^n L_{x_i x_i} \right) + f''(x) \cdot \right. \\ \left. n \cdot \left[ p_{y_T y_T} \cdot L + p_{y_T} \cdot L_{y_T} + p_{y_T} \cdot L_{y_T} + p \cdot L_{y_T y_T} \right] \right) \\ \left( n \cdot \left[ p_{x_i y_T} \cdot L + p_{x_i} \cdot L_{y_T} + p_{y_T} \cdot L_{x_i} + p \cdot L_{x_i y_T} \right] \cdot \right. \\ \left. - \left( \left( \sum_{i=1}^n p_{y_T x_i} \right) \cdot L + p_{y_T} \cdot \left( \sum_{i=1}^n L_{x_i} \right) + \left( \sum_{i=1}^n p_{x_i} \right) \cdot L_{y_T} + p \cdot \left( \sum_{i=1}^n L_{y_T x_i} \right) \right) \right\} \quad (4-A15)$$

The government chooses  $z$  in order to

$$\begin{aligned} \text{Min } n \cdot [f(x^*(z)) + y^*(z) + g(z)] \\ + h \cdot \left\{ c[e(x^*(z), \dots, x^*(z), y_T^*(z), \dots, y^*(z)), z] + \right. \\ \left. e(x^*(z), \dots, x^*(z), y_T^*(z), \dots, y^*(z), z) \cdot s(x^*(z), \dots, x^*(z), y_T^*(z), \dots, y^*(z), z) \right\} \end{aligned} \quad (4-A16)$$

where  $y_T^* = y_1^*(z) + y_2^*(z) + \dots + y_n^*(z)$ .

The first-order condition is:

$$\begin{aligned} n \cdot \left[ f' \cdot \frac{\partial x^*}{\partial z} + \frac{\partial y^*}{\partial z} + g'(z) \right] + h \cdot \left[ c'(e) \cdot \left( \left( \sum_{i=1}^n e_{x_i} \right) \cdot \frac{\partial x^*}{\partial z} + n \cdot e_{y_T} \cdot \frac{\partial y^*}{\partial z} + e_z \right) \right] \\ + h \cdot e \cdot \left( \left( \sum_{i=1}^n s_{x_i} \right) \cdot \frac{\partial x^*}{\partial z} + n \cdot s_{y_T} \cdot \frac{\partial y^*}{\partial z} + s_z \right) + h \cdot s \cdot \left( \left( \sum_{i=1}^n e_{x_i} \right) \cdot \frac{\partial x^*}{\partial z} + n \cdot e_{y_T} \cdot \frac{\partial y^*}{\partial z} + e_z \right) = 0. \end{aligned} \quad (4-A17)$$

Solving for  $g'(z)$ , we have:

$$-p_z L - p_{s_z} - \frac{\partial x^*}{\partial z} \left[ f'(x) + \left( \sum_{i=1}^n p_{x_i} \right) \cdot L + p \cdot \left( \sum_{i=1}^n s_{x_i} \right) \right] - \frac{\partial y^*}{\partial z} [1 + n \cdot p_{y_T} L + n \cdot p_{s_{y_T}}] = g'(z). \quad (4-A18)$$

Substituting in for the firm's first order conditions, we have:

$$-p_z L - p s_z - \frac{\partial x^*}{\partial z} \left[ \left( \sum_{i=2}^n p_{x_i} \right) \cdot L + p \cdot \left( \sum_{i=2}^n L_{x_i} \right) - p \cdot \left( \sum_{i=1}^n g_{x_i} \right) \right] - \frac{\partial y^*}{\partial z} \left[ (n-1) \cdot p_{y_T} L + (n-1) \cdot p L_{y_T} - n \cdot p g_{y_T} \right] = g'(z) \quad (4-A19)$$

Conclusion: The government also adjusts the adjustment by the size of the underinvestment.

### The Cooperative Solution

$$\begin{aligned} \text{Min } & n \cdot p(x_1, \dots, x_n, y_T(y_1, \dots, y_n), z) \cdot L(x_1, \dots, x_n, y_T(y_1, \dots, y_n), z) + n \cdot f(x) + y_T + n \cdot g(z) \\ & x, y_T \end{aligned} \quad (4-A20)$$

First Order Conditions:

$$\{x\} - \left[ \left( \sum_{i=1}^n p_{x_i} \right) \cdot L + p \cdot \left( \sum_{i=1}^n L_{x_i} \right) \right] = f'(x) \quad (4-A21)$$

$$\{y_T\} - n \cdot [p_{y_T} L + p L_{y_T}] = 1 \quad (4-A22)$$

**Id; Government**

$$\begin{aligned} \text{Min } & n \cdot [f(x^{**}(z)) + g(z)] + y_T^{**}(z) \\ & + h \cdot \left\{ \begin{aligned} & c[e(x^{**}(z), \dots, x^{**}(z), y_T^{**}(z), \dots, y_T^{**}(z)), z)] + \\ & e(x^{**}(z), \dots, x^{**}(z), y_T^{**}(z), \dots, y_T^{**}(z), z) \cdot s(x^{**}(z), \dots, x^{**}(z), y_T^{**}(z), \dots, y_T^{**}(z), z) \end{aligned} \right\} \end{aligned} \quad (4-A23)$$

First Order Condition:

$$-p_z L - p s_z - \frac{\partial x^{**}}{\partial z} \left[ f'(x) + L \cdot \left( \sum_{i=1}^n p_{x_i} \right) + p \cdot \left( \sum_{i=1}^n s_{x_i} \right) \right] - \frac{\partial y^{**}}{\partial z} [1 + n \cdot p_{y_T} L + n \cdot p s_{y_T}] = g'(z) \quad (4-A24)$$

Substituting in the collective's first-order condition (and if  $L = s$ ), this reduces to

$$-p_z L - p s_z = g'(z). \quad (4-A25)$$

**CHAPTER 5:**  
**SUMMARY OF CONCLUSIONS AND  
POSSIBLE AVENUES FOR FUTURE RESEARCH**

**1. SUMMARY**

This dissertation employed law and economics analysis to study Internet security. Chapter 1 provided the introduction to the problem of cybercrime and cyber-attacks, and reviewed the different technological, economic, and law-based solutions hitherto proposed to combat the problem. We concluded that a combination of technological, economic, and law-based solutions are necessary to effectively combat cybercrime, since each of these methods alone is insufficient to address the problem. The succeeding three chapters presented the main essays of the dissertation.

In Chapter 2, we proposed that cyberinsurance can be a powerful market-based tool to align market incentives toward improving Internet security. We presented three economic arguments to support the case for cyberinsurance as a market solution to managing information technology (IT) security risks. We also conducted time and case studies to trace the evolution of the cyberinsurance industry and concluded that, in practice, although there were issues that needed to be worked out to fully implement this market-based solution, nonetheless, cyberinsurers were able to find ways to address these frictions to the market solution. We thus concluded that there is significant theoretical foundation, in addition to market-based evidence, to support the assertion that cyberinsurance results in: (1) better IT safety infrastructure; (2) standards based on the

optimal amount of care; and (3) the correction of a market failure, which results in increased overall social welfare.

In Chapter 3, we examined whether firms or individuals whose computer systems are under attack should be permitted to hack back, and how the law of self-defense in cyberspace should be designed. We employed a formal, game-theoretic analysis of the strategic interaction between the hacker and the attacked firm/individual, including Bayesian updating to study the effect of intrusion detection system (IDS) technology, as well as the consideration of the social planner's perspective and different liability regimes. We concluded that neither total prohibition nor unrestrained permission of hackback is optimal. Instead, hackback should be permitted when: (1) other alternatives, such as police enforcement and resort to courts, are either ineffective or ineffectual; (2) there is a serious prospect of hitting the hacker instead of innocent third parties; and (3) the damages to the attacked firm's (that is, the entity that is hacking back) systems that can be potentially mitigated outweigh the potential damages to third parties.

Also, even if hackback is permissible under the abovementioned rules, the conduct during hackback must also be regulated. Specifically, counter-strikers must use only "proportionate force"; that is, they must not wantonly damage the hackers' digital systems out of retaliation, but rather, only use force that is necessary to avoid damage to their own systems. Also, active defenders should be held liable to third parties caught in the crossfire, so that damages to third parties may be internalized. Lastly, better IDS and traceback technologies improve the effectiveness of hackback as deterrence to the hacker, highlighting the role of technology in analyzing the appropriateness of hackback.

In sum, hackback should be resorted to only as a means of defense, and not for the purpose of inflicting damages.

In Chapter 4, we examined whether Internet security is a public good, and how society should handle the spill-over effects arising from the interrelatedness of Internet risks. Additionally, we analyzed what role, if any, does police enforcement play, and what optimal combination of each of the security measures – police enforcement, and individual investments in both private and non-rivalrous security goods – should be used to effectively combat cybercrime. We concluded that some, but not all, investments in security have the nature of public goods. Thus, we modeled the situation where firms invest in both private and public security goods, where public enforcement of law is present. That is, our model contained these elements: private investments in security; investments in security that have the nature of public goods; externalities; and public enforcement of law. By so doing, we gained insights on the substitutability between the private and public measures, and on how to combine these approaches optimally.

We concluded that the socially-optimal level of security is achieved by equalizing the marginal-benefit-to-marginal-cost ratios of each of the three alternatives – private security investment, non-rivalrous security investment, and law enforcement measures. Furthermore, the interrelatedness of Internet risks causes individual firms to underinvest in private and public security goods. The government thus decidedly lowers the level of police enforcement expenditures in order to induce firms to invest more in individual precautions. We also found that, under certain conditions, cooperation results in socially-optimal levels of expenditures in private and public security goods expenditures. The Shapley (1953) value can be used as a criterion for allocating the costs and benefits

among the members of a security cooperative. Several simulations illustrated the results of the model under several scenarios.

## **2. POSSIBLE AVENUES FOR FUTURE RESEARCH**

This dissertation may be complete in its present condition, but in the course of our research, we have come across future topics that may be interesting pursuit of independent research.

One possible area of future research is concerning the possibility of hackers purchasing information or source code on the black market and reverse-engineering it. This is so considering that the person who has the software code or vulnerability information could potentially use it several times (for example, for copyright violation purposes, hacking, etc.). That is, the software code or vulnerability information is “non-rival”, which means that the vulnerability finder can use such information for both legitimate and illicit purposes. For example, an individual can pore through the millions of line of code and work for (or sell the bug information to) the software producer since these software codes are being subjected to testing and in fact bug finders are hired/paid to search for bugs, including security vulnerabilities. So, the vulnerability finder can simply search for bugs and be paid by the software manufacturer. Another legitimate business purpose is for the vulnerability finder to sell the information to firms like iDefense (a Verisign Company) and Tipping Point (a division of 3M) who purchase these vulnerability information in the open market to protect their subscription-based customers (see, for example, Sutton and Nagle 2006). As for illegitimate purposes, an individual who acquires a source code could use it for copyright violation purposes. Thus, an individual could acquire and reverse-engineer a software code to make another software



product in violation of the copyright of the software developer. Another alternative income opportunity to the vulnerability finder is to either to sell the vulnerability information to a hacker in the black market or to be a hacker himself. For example, we have found (relatively new) cases where some vulnerability finder had sold the vulnerability information in the informal market, such as the case of this vulnerability finder posting IE7 and Windows Vista bugs/exploit for sale to the highest bidder, in a website well-known to security practitioners (<http://lists.grok.org.uk/pipermail/full-disclosure/2006-May/045763.html>), and apparently quiet successful at it (<http://lists.grok.org.uk/pipermail/full-disclosure/2006-May/046325.html>) (see also Finjan Malicious Code Research Center 2006). There are also reports of a Russian hacker posting an IE vulnerability and exploit for sale in the black market for \$300 (*BusinessWeek* 2005).

Thus, we have found that when Microsoft Window's source code leaked, although it seemed that Microsoft was primarily concerned about the possible violation of its copyright (*CNN.com* 2004b; Lemos 2004; Gonsalves 2004), Microsoft was also concerned that the leak of such code could result in people finding more vulnerabilities in its product, and it is conceivable that such leak could have been responsible for subsequent discoveries of vulnerabilities in Windows (Thurrott 2004). Hence, it is conceivable that hackers could purchase security information on the black market -- say from those who wrote the original code (although I have not found a single report of this happening so far) -- and reverse-engineer it. This issue might be an interesting topic to pursue later on considering that modeling the business decision of an individual who has

the software code and has to make several cost vs. income-opportunity calculations, could be complex.

Another possible area of future research is regarding the other potential areas of market failure in Internet security such as asymmetric information. The Common Criteria standard may help alleviate this problem, but we have to bear in mind that the information security environment is very dynamic and it may be extremely difficult or costly if not impossible to guard against future vulnerabilities. The research questions may be whether a Lemons Law equivalent for software should be enacted, or whether contract law (for example, extending the Magnuson-Moss Act [against anti-warranty] to software – in effect addressing the shrink-wrap disclaimers to the warranty of merchantability) and/or tort law should be used (if so what is the liability regime, strict, negligence-rule, etc.). The pros and cons must be balanced (that is, being overly strict to software developers might curtail innovation) and a more in-depth study -- such as empirically studying the various costs and benefits, as well as modeling where the right balance should be struck considering the pros and cons -- may be a future area of research. The law and economics of software-related litigation is complex and will require a lot of future work; it opens up as well a whole new field of research and is a promising future area of investigation.

## REFERENCES

- 45 C.F.R. Parts 160, 162, and 164, *available at*  
<http://www.cms.gov/regulations/hipaa/cms0003-5/0049f-econ-ofr-2-12-03.pdf>.
- Agora Workshop. 2003. Active Defenses to Cyber Attacks.  
<http://staff.washington.edu/dittrich/ad/AD-workshop-091203.ppt>.
- Alpcan, Tansu, and Tamer Basar. 2004. A Game Theoretic Approach to Decision and Analysis in Network Intrusion Detection. In *Proceedings of the 43rd IEEE Conference on Decision and Control*.
- American International Group (AIG), Inc. 2005. The AIG NetAdvantage Suite – Coverage Highlights,  
<http://www.aignetadvantage.com/content/netad/coveragelandscape.pdf>.
- American International Group (AIG), Inc. 2003. Information Security Self Assessment,  
[http://www.aignetadvantage.com/content/netad/netadvantage\\_assessment.doc](http://www.aignetadvantage.com/content/netad/netadvantage_assessment.doc).
- American Law Institute. 1965. *Restatement (Second) of Torts*. Philadelphia: American Law Institute.
- American Law Institute. 1985. *Model Penal Code and Commentaries (Official Draft and Revised Comments)*. Philadelphia: American Law Institute.
- Aquinas, Thomas. c.1271. *Summa Theologica*. <http://www.newadvent.org/summa/>.
- Ardis, Patrick M. et al. 1985. Fidelity and Computer Related Risk Insurance. *Magazine of Bank Administration*.
- Arora, Ashish, Jonathan P. Caulkins, and Rahul Telang. 2003. Sell First, Fix Later: Impact of Patching on Software Quality, *available at*  
<http://www.heinz.cmu.edu/wpapers/retrievePDF?id=2003-16>.
- Arora, Ashish et al. 2004. Impact of Vulnerability Disclosure and Patch Availability—An Empirical Analysis. *Conference Papers in Proceedings of the Third Annual Workshop on Economics of Information Security*, *available at*  
<http://www.dtc.umn.edu/weis2004/telang.pdf> (April 2004).
- Arora, Ashish, Rahul Telang, and Hao Xu. 2004. Optimal Policy for Software Vulnerability Disclosure, *Conference Papers in Proceedings of the Third Annual Workshop on Economics of Information Security*, *available at*  
<http://www.dtc.umn.edu/weis2004/xu.pdf>.

- Arrow, Kenneth. 1963. Uncertainty and the Welfare Economics of Medical Care. *American Economic Review* 53:941.
- Augustinus, Aurelius. 400. *Contra Faustum Manichaeum*.  
<http://www.newadvent.org/fathers/1406.htm>.
- Augustinus, Aurelius. c.423. *De Civitate Dei*.  
<http://www.newadvent.org/fathers/120119.htm>.
- Ayres, Ian, and Steven Levitt. 1998. Measuring Positive Externalities from Unobservable Victim Precaution: An Empirical Analysis of Lojack. *Quarterly Journal of Economics* 113:43-77.
- Back, Adam. Hash Cash: Partial Hash Collision Based Postage Scheme, *available at* <http://www.cypherspace.org/adam/hashcash> (last visited May 26, 2004).
- Back, Adam. 2002. Hash Cash—A Denial of Service Counter-Measure, *available at* <http://www.cypherspace.org/adam/hashcash/hashcash.pdf>.
- Baer, W. 2003. Rewarding IT Security in the Marketplace, *31<sup>st</sup> Research Conference on Communication, Information, and Internet Policy (TPRC)*.
- Baker & McKenzie. Security Law Resources: Legislation, Regulations and Policy—By U.S. State, *at* <http://www.bakernet.com/ecommerce/legis-s.htm>.
- Banham, R. 2002. Hacking It (Cyberinsurance)(Statistical Data Included), *CFO-Magazine for Senior Financial Executives*, August, *available at* [http://www.findarticles.com/p/articles/mi\\_m3870/is\\_9\\_16/ai\\_63916347](http://www.findarticles.com/p/articles/mi_m3870/is_9_16/ai_63916347) (last visited March 13, 2006).
- Barron, Cheryll Aimee. 2000. High Tech's Missionaries of Sloppiness, *at* [http://www.salon.com/tech/feature/2001/12/06/bad\\_companies/print.html](http://www.salon.com/tech/feature/2001/12/06/bad_companies/print.html).
- Beh, Hazel Glenn. 2002. Physical Losses in Cyberspace. *Connecticut Insurance Journal* 8:55-68.
- Bernhofen, Daniel M., and John C. Brown. 2005. An Empirical Assessment of the Comparative Advantage Gains from Trade: Evidence from Japan. *American Economic Review* 95(1):208-225.
- Böhme, R. Cyberinsurance Revisited, *Workshop on the Economics of Information Security (WEIS)*, Harvard University, 2005.
- Brandon, Douglas Ivor, Melinda Lee Cooper, Jeremy H. Greshin, Alvin Louis Harris, James M. Head Jr., Keith R. Jacques, and Lea Wiggins. 1984. Special Project, Self-

- help: Extrajudicial Rights, Privileges and Remedies in Contemporary American Society. *Vanderbilt Law Review* 37:845-1040.
- Brenner, Susan W. 2005. Should Criminal Liability Be Used to Secure Data Privacy? In *Securing Privacy In The Internet Age*, Stanford University Press.
- Brown, Brian D. 2001. Emerging Insurance Products in the Electronic Age. *Fall Brief* 31:28.
- Brush, Colleen. 2001. Surcharge for Insecurity. *Information Security Magazine*, available at [http://www.esmartcorp.com/Hacker%20Articles/ar\\_surcharge\\_for\\_insecurity.htm](http://www.esmartcorp.com/Hacker%20Articles/ar_surcharge_for_insecurity.htm) (last visited April 23, 2004).
- Bryce, Robert. 2001. Hack Insurer Adds Microsoft Surcharge. *Interactive Week*, August 20.
- Buchanan, James. 1999. Three Research Programs in Constitutional Political Economy: Discussion of Political Science and Economics. In Alt, J., M. Levi, and E. Ostrom (Eds.), *Competition and Cooperation: Conversations with Nobelists About Economics and Political Science*. New York: Russel Sage Foundation.
- Buchanan, James. 1965. An Economic Theory of Clubs. *Economica* 32:1-14.
- BusinessWeek*. 2005. From Black Market to Free Market. News: Analysis and Commentary August 22, 2005, at [http://www.businessweek.com/magazine/content/05\\_34/b3948022\\_mz011.htm?chan=tc](http://www.businessweek.com/magazine/content/05_34/b3948022_mz011.htm?chan=tc) (last visited August 3, 2006).
- Business Wire*. 2001. Recourse Technologies Partners with Safeonline to Bring Even Greater Levels of Control to IT Systems Protection, available at [http://www.findarticles.com/p/articles/mi\\_m0EIN/is\\_2001\\_Jan\\_30/ai\\_69704293](http://www.findarticles.com/p/articles/mi_m0EIN/is_2001_Jan_30/ai_69704293) (last visited August 2, 2006).
- Camp, L. Jean, and Catherine Wolfram. 2000. Pricing Security. *Proceedings of the CERT Information Survivability Workshop*, Boston, MA Oct. 24-26, 2000, available at <http://www.cert.org/research/isw/isw2000/papers/54.pdf>.
- Carver, Doris L. 1988. Acceptable Legal Standards for Software. *IEEE Software* 5(3):87-93.
- Cavusoglu, Huseyin, Birenda Mishra, and Srinivasan Raghunathan. 2005. The Value of Intrusion Detection Systems (IDSs) in Information Technology (IT) Security. *Information Systems Research* 16(1):28-46.

- Cavusoglu, Huseyin, Birendra Mishra, and Srinivasan Raghunathan. 2004. The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. *International Journal of Electronic Commerce* 9:69-104, available at <http://info.freeman.tulane.edu/huseyin/paper/market.pdf>.
- Cavusoglu, Huseyin, Birenda Mishra, and Srinivasan Raghunathan. 2002. A Model for Evaluating IT Security Investments. Working paper.
- CERT Coordination Center. 2003. *CERT/CC Statistics, 1988-2003*, available at [http://www.cert.org/stats/cert\\_stats.html](http://www.cert.org/stats/cert_stats.html).
- CERT Coordination Center. 2006. *CERT/CC Statistics, 1998-2005*, <http://www.cert.org/stats/>.
- Chandler, Jennifer. 2005. Tort Liability for Cyber Insecurity: The Case of Distributed Denial of Service Attacks. In *Securing Privacy In The Internet Age*, Stanford University Press.
- Cheswick, William R., Steven M. Bellovin, and Aviel D. Rubin. 2003. *Firewalls and Internet Security*. 2nd Ed. Boston, MA: Addison-Wesley.
- Christiansen, John. 2003. Active Defense Scenario. <http://staff.washington.edu/dittrich/ad/Active%20Defense%20Scenario.doc>.
- Christie, Les. 2004a. Six Steps to Protect Your Computer: What You Can Do to Fend Off Hacker Attacks. *CNN Money*. August 4, available at [http://money.cnn.com/2004/08/03/pf/security\\_sixsteps/index.htm](http://money.cnn.com/2004/08/03/pf/security_sixsteps/index.htm).
- Christie, Les. 2004b. Going Phishing: Cybercrime is on the Upswing, Here's How to Protect Yourself. *CNN Money*. August 3, at [http://money.cnn.com/2004/08/03/pf/security\\_phishing/index.htm](http://money.cnn.com/2004/08/03/pf/security_phishing/index.htm).
- CIO Magazine*. 2001. CIOs Say Law Enforcement Can't Hack It When It Comes to Hackers, <http://www.cio.com/knowpulse/aug2001/index.html>.
- Clark, D. 1998. Cigna Set to Offer Coverage Linked to Cisco, NetSolve. *Wall Street Journal*, B-6, Oct. 5, 1998.
- Clark, Matthew. 2002. B2B E-Commerce Sales to Skyrocket, May 8, 2002, at <http://www.enn.ie/news.html?code=7426802> (last visited April 24, 2004).
- CNN.com*. 2004a. Microsoft Releases Free Windows Upgrade. August 6. <http://www.cnn.com/2004/TECH/08/06/microsoft.update.ap/index.html>.

- CNN.com*. 2004b. Microsoft Grapples With Leak of Source Code Online. February 13. <http://www.cnn.com/2004/TECH/internet/02/13/microsoft.code.ap/> (last visited August 3, 2006).
- Coase, Ronald. 1960. The Problem of Social Cost. *J. L. & Econ.* 1.
- Cochrane, John H. 1997. Where is the Market Going? Uncertain Facts and Novel Theories. *Economic Perspectives* 21:3.
- Colander, David C. 2004. *Microeconomics*, 5<sup>th</sup> Ed. McGraw-Hill/Irwin.
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components. July 2005. Draft v3.0, Rev 2, at [http://niap.bahialab.com/cc-scheme/cc\\_docs/ccmb-2005-07-003.pdf](http://niap.bahialab.com/cc-scheme/cc_docs/ccmb-2005-07-003.pdf).
- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model. June 2005, Draft v3.0, Rev 2, Figure 2, at p. 27, at [http://niap.bahialab.com/cc-scheme/cc\\_docs/ccmb-2005-07-001.pdf](http://niap.bahialab.com/cc-scheme/cc_docs/ccmb-2005-07-001.pdf).
- Common Criteria: An Introduction, ["Common Criteria Introduction"], at <http://www.commoncriteriaportal.org/public/files/ccintroduction.pdf>.
- Cooter, Robert, and Thomas Ulen. 2004. *Law and Economics*, 4th Ed. Boston, MA: Pearson Addison Wesley.
- Coyne, Christopher J., and Peter T. Leeson. Forthcoming. Who's to Protect Cyberspace? *Journal of Law, Economics and Policy*.
- Crane, Matthew. 2001. International Liability in Cyberspace. *Duke L. & Tech. Rev.* 23:1.
- Davis, B. 1998. Cigna Offers Anti-Hacker Insurance, <http://www.techweb.com/wire/story/TWB19981005S0010>.
- DeForrest, Mark Edward. 1997. Just War Theory and the Recent U.S. Air Strikes Against Iraq. Gonzaga University, School of Law. <http://law.gonzaga.edu/borders/documents/deforres.htm>
- Dolinar, Lou. 2004. Fake Spyware Removal Programs Disabling PCs. *Newsday.com*, August 8, available at <http://www.newsday.com/business/nyc-biz-spy0809,0,5985461.story?coll=ny-business-headlines>.
- Dornseif, Maximillian, and Sascha A. May. 2004. Modelling the Costs and Benefits of Honeynets. *Conference Papers in Proceedings of the Third Annual Workshop on Economics of Information Security*, May 3, available at <http://www.dtc.umn.edu/weis2004/dornseif.pdf>.

- Duffy, Daintry. 2002. Safety at a Premium. *CSO Magazine*, December, available at <http://www.csoonline.com/read/120902/safety.html> (last visited April 23, 2004).
- Duffy, Daintry. 2000. Prepare for the Worst, *Darwin Mag.*, December, available at <http://www.darwinmag.com/read/120100/worst.html> (last visited April 24, 2004).
- Durney, Edward G. 1983. Comment, The Warranty of Merchantability and Computer Software Contracts: A Square Peg Won't Fit in a Round Hole, *Washington Law Review* 59:511.
- Duvall, M. 1998. Big Blue to Offer Hacker Insurance Services. *ZDNet*.
- Edwards, Lilian. 2005. The Problem with Privacy: A Modest Proposal. In *Securing Privacy In The Internet Age*, Stanford University Press.
- Ehrlich, Isaac, and Gary Becker. 1972. Market Insurance, Self-Insurance, and Self-Protection. *Journal of Political Economy* 80(4):623-648.
- Epstein, Richard A. 2005. Self-help: From Stone Age to the Internet Age. *Journal of Law, Economics, and Policy* 1:1-32.
- Escamilla, T. 1998. *Intrusion Detection: Network Security Beyond the Firewall*.
- Ettredge, Michael, and Vernon Richardson. 2002. Assessing the Risk in E-Commerce. *Proceedings of the Thirty-Fifth Hawaii International Conference on System Sciences*, [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=268737](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=268737).
- Fabella, Raul, V. 2005. A Nozick-Buchanan Contractarian Governance as Solution to Some Invisible Hand Failures. *Quarterly Review of Economics and Finance* 45:284-295.
- Fama, Eugene F., Lawrence Fisher, Michael Jensen, and Richard Roll. 1969. The Adjustment of Stock Prices to New Information. *International Economic Review* 10:1-21.
- Feenstra, Robert C. 2003. *Advanced International Trade: Theory and Evidence*. Princeton University Press.
- Ferguson, P., and D. Senie. 2000. Network Ingress Filtering: Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing. *RFC 2827, Internet Engineering Task Force*, available at <http://www.rfc-editor.org/rfc/rfc2827.txt>.
- Finjan Malicious Code Research Center. 2006. Web Security Trends Report. Q2 2006, available at <http://www.finjan.com/Content.aspx?id=827> (last visited August 3, 2006).



- Fisher, Susan E. 2001. Seeking Full Protection for Net Asset. *InfoWorld*, October 5, available at <http://webbytes.com/portfolio/text/iw100501.html> (last visited April 23, 2004).
- Garg, Ashish, Jeffrey Curtis, and Hilary Halper. 2003. The Financial Impact of IT Security Breaches: What Do Investors Think. *Info Systems Security*, [http://www.auerbach-publications.com/dynamic\\_data/2466\\_1358\\_cost.pdf](http://www.auerbach-publications.com/dynamic_data/2466_1358_cost.pdf).
- Gemignani, Michael C. 1981. Product Liability and Software. *Rutgers Computers and Technology Law Journal* 8:173.
- Gohring, Nancy. 2002. Cyberinsurance May Cover Damage of Computer Woes. *Seattle Times*, July 29, available at <http://www.landfield.com/isn/mail-archive/2002/Jul/0133.html> (last visited April 23, 2004).
- Gold, Joshua. 2002. Insurance Coverage for Internet and Computer Related Claims. *Computer & Internet Law* 19(4):8.
- Gomulkiewicz, Robert W. 1997. The Implied Warranty of Merchantability in Software Contracts: A Warranty No One Dares to Give and How to Change That. *John Marshall Journal of Computer & Information Law* 16:393.
- Gonsalves, Antone. 2004. Microsoft Threatens to Sue Downloaders of Leaked Source Code. *InformationWeek*, February 18, at <http://www.informationweek.com/story/showArticle.jhtml?articleID=17701340> (last visited August 3, 2006).
- Gralla, Preston. 2001. Electronic Safety Net: Cyberinsurance Policies Can Offer Protection When Technology Fails, *CIO Mag.*, December 1, available at [http://www.cio.com/archive/120101/et\\_article.html](http://www.cio.com/archive/120101/et_article.html) (last visited Apr. 22, 2004).
- Granot, D., and G. Huberman. 1984. On the Core and Nucleolus of Minimum Cost Spanning Tree Games. *Mathematical Programming* 29:323-347.
- Granot, D., and G. Huberman. 1981. Minimum Cost Spanning Tree Games. *Mathematical Programming* 21:1-18.
- Greenberg, P. 2000. AIG Unveils E-Commerce Insurance Plans. *E-Commerce Times*, January 18.
- Greenemeier, L. 1998. IBM Invests in Hacker Insurance Program. *Midrange Systems*.
- Grinols, Earl L. 1984. A Thorn in the Lion's Paw: Has Britain Paid Too Much for Common Market Membership? *Journal of International Economics* 16:271-294.

- Grinols, Earl L., and Kar-Yiu Wong. 1991. An Exact Measure of Welfare Change. *Canadian Journal of Economics* 24(2):428-449.
- Grotius, Hugo. 1625. *Jure Belli ac Pacis* ("On the Law of War and Peace"). <http://www.geocities.com/Athens/Thebes/8098/>.
- Hahn, Robert H., and Anne Layne-Farrar. 2006. The Law and Economics of Software Security. Working Paper No. 06-08. *AEI-Brookings Joint Center for Regulatory Studies*, available at <http://aei-brookings.org/publications/abstract.php?pid=1064>.
- Harrison, A. 2000. Counterpane Offers Internet Security Insurance. *Computerworld*.
- Heal, Geoffrey, and Howard Kunreuther. 2003. You Only Die Once: Managing Discrete Interdependent Risks, available at [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=419240](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=419240).
- Hensing, Robert. 2004a. Patch Warfare and Security Incident Response, *Presentation at Information Security Day*, Northwestern University, July 30.
- Hensing, Robert. 2004b. Securing Windows Networks: Security from the Frontline, *Presentation at Information Security Day*, Northwestern University, July 30.
- Himma, Kenneth Einar. 2004. Targeting the Innocent: Active Defense and the Moral Immunity of Innocent Persons from Aggression. *Journal of Information, Communication, and Ethics in Society* 2, no. 1.
- Hoffman, Lance J. 2005. An Architecture to Allow Metadata-Driven Legal and Economic Controls in Privacy Sensitive Systems. In *Securing Privacy In The Internet Age*, Stanford University Press.
- Information Security*. 2001. Industry Briefs. April. [http://infosecuritymag.techtarget.com/articles/april01/departments\\_news.shtml](http://infosecuritymag.techtarget.com/articles/april01/departments_news.shtml) (last visited April 23, 2004).
- Insecure.org*. Nmap Network Security Scanner Man Page, at [http://insecure.org/nmap/data/nmap\\_manpage.html](http://insecure.org/nmap/data/nmap_manpage.html).
- Insurance Information Institute. 2003. Computer Security-Related Insurance Issues, September, available at <http://www.iii.org/media/hottopics/insurance/computer/> (last visited April 14, 2004).
- InsureTrust.com. 2003. Webnet Protection Policy (Draft), [http://www.insuretrust.com/Policies/WebNet\\_Policy.pdf](http://www.insuretrust.com/Policies/WebNet_Policy.pdf).
- InsureTrust.com. Network Security Services Baseline Risk Assessment, <http://www.insuretrust.com/pdfs/Base%20Line%20Risk%20Assessment%20Summary.doc>.

- Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness, 12 C.F.R. Part 30 [Office of Comptroller of the Currency], 12 C.F.R. Parts 208, 211, 225 & 263 [Federal Reserve System], 12 C.F.R. Parts 308 & 364 [Federal Deposit Insurance Corporation], and 12 C.F.R. Parts 568 & 570 [Office of Thrift Supervision], *available at* <http://federalreserve.gov/boarddocs/press/boardacts/2001/20010117/attachment.pdf>.
- Irwin, Douglas A. 2005. The Welfare Costs of Autarky: Evidence from the Jeffersonian Trade Embargo, 1807-1809. *Review of International Economics* 13(4):631-645.
- James, Fleming Jr. 1948. Accident Liability Reconsidered: The Impact of Liability Insurance. *Yale Law Journal* 57(4):549-570.
- Jayawal, Vikas, William Yurcik, and David Doss. 2002. Internet Hack Back: Counter Attacks as Self-Defense or Vigilantism? In *Proceedings of the IEEE International Symposium on Technology and Society (ISTAS)*.
- Juniper Networks. 2004. Firewalls, *Presentation at Information Security Day*, Northwestern University, July 30.
- Kannan, Karthik, Rahul Telang, and Hao Xu. 2003. Market for Software Vulnerabilities? Think Again, *available at* [http://papers.ssrn.com/sol3/Delivery.cfm/Delivery.cfm/SSRN\\_ID473321\\_code264190.pdf?abstractid=473321&mirid=1](http://papers.ssrn.com/sol3/Delivery.cfm/Delivery.cfm/SSRN_ID473321_code264190.pdf?abstractid=473321&mirid=1).
- Katyal, Neal. 2005. Community Self-help. *Journal of Law, Economics, and Policy* 1:33-68.
- Kaufman, Charlie, Radia Perlman, and Mike Speciner. 2002. *Network Security: Private Communication in a Public World*, 2nd Ed.
- Kehne, Jeffrey. 1986. Note, Encouraging Safety Through Insurance-Based Incentives: Financial Responsibility for Hazardous Waste. *Yale Law Journal* 96:403-427.
- Kenneally, Erin. 2000. The Byte Stops Here: Duty and Liability for Negligent Internet Security. *Computer Security Journal* 16(2), *available at* <http://www.gocsi.com/pdfs/byte.pdf>.
- Kerr, Orin S. 2005. Virtual Crime, Virtual Deterrence: A Skeptical View of Self-help, Architecture, and Civil Liability. *Journal of Law, Economics, and Policy* 1:197-214.
- Kesan, Jay P., and Ruperto P. Majuca. 2005. Cybercrimes and Cyber-Attacks: Technological, Economic, and Law-Based Solutions. In vol. 4 of *Cybercrime & Security*, edited by Pauline C. Reich. Dobbs Ferry, N.Y.: Oceania Publications.

- Kesan, Jay P., Ruperto P. Majuca, and William Yurcik. 2005a. CyberInsurance as a Market-Based Solution to the Problem of CyberSecurity – A Case Study, 4<sup>th</sup> *Workshop on the Economics of Information Security (WEIS)*, Harvard University.
- Kesan, Jay P., Ruperto P. Majuca, and William Yurcik. 2005b. The Economic Case for Cyberinsurance. In *Securing Privacy in the Internet Age*, Stanford University Press.
- Kiefer, Kimberly, and Randy V. Sabett. 2002. Openness of Internet Creates Potential for Corporate Information Security Liability. *BNA Privacy & Security Law Report* 1:788.
- Kit, E. 1995. *Software Testing in the Real World: Improving the Process*.
- Kneuper, Robert and Bruce Yandle. 1994. Auto Insurers and the Air Bag. *Journal of Risk and Insurance* 61:107, available at 1994 WL 13386236.
- Knight, Will. 2000. Hacking Will Cost World \$1.6 Trillion This Year, July 11, 2000, available at <http://news.zdnet.co.uk/internet/security/0,39020375,2080075,00.htm> (last visited April 24, 2004).
- Kobayashi, Bruce H. 2005. An Economic Analysis of the Private and Social Costs of the Provision of Cybersecurity and other Public Security Goods. *Supreme Court Economic Review* 14.
- Laurie, Ben, and Richard Clayton. 2004. Proof-of-Work Proves Not to Work. *Conference Papers in Proceedings of the Third Annual Workshop on Economics of Information Security*, available at <http://www.dtc.umn.edu/weis2004/clayton.pdf>.
- Lee, Anna. 2001. Student Notes, Why Traditional Insurance Policies Are Not Enough: The Nature of Potential E-Commerce Losses and Liabilities. *Vanderbilt Journal of Entertainment Law & Practice* 3:84.
- Lemos, Robert. 2004. Microsoft Probes Windows Code Leak. *CNET News.com*. February 12, at [http://news.com.com/2100-7349\\_3-5158496.html](http://news.com.com/2100-7349_3-5158496.html) (last visited August 3, 2006).
- Lichtman, Douglas. 2005. How the Law Responds to Self-help. *Journal of Law, Economics, and Policy* 1:215-258.
- Lichtman, Doug, and Eric Posner. 2004. Holding Internet Service Providers Accountable. *Conference Papers in Proceedings of The Law and Economics of Cyber Security*, June 11, 2004.
- Littlechild, S. 1974. A Simple Expression for the Nucleolus in a Special Case. *International Journal of Game Theory* 3: 21-29.

- Littlechild, S., and G. Owen. 1973. A Simple Expression for the Shapley Value in a Special Case. *Management Science* 20:370-372.
- Lloyd's of London. 2002. *e-Comprehensive*,  
<http://www.insuretrust.com/pdfs/eComp2002wording.pdf>.
- Loesch, Martin C., and David M. Brenner. 1998. Coverage on the Technology Frontier. *Corp. Officers & Directors Liability Litig. Rep.*, February 17.
- Mader, Becca. 2002. Demand Developing for Cyberinsurance. *Business Journal of Milwaukee*, October 11, available at  
<http://www.milwaukee.bizjournals.com/milwaukee/stories/2002/10/14/focus2.html>  
 (last visited Apr. 24, 2004).
- Mangla, Anoop. 2004. File-Integrity Checkers: GFI Languard for Win, Tripwire for Lin. Keep a Tab of Key System Files, available at  
[www.pcquest.com/content/depth/104013104.asp](http://www.pcquest.com/content/depth/104013104.asp), Jan. 31, 2004.
- Mankins, D., R. Krishnan, C. Boyd, J. Zao, and M. Frenzt. Mitigating Distributed Denial of Service Attacks with Dynamic Resource Pricing. In *Proceedings of 17th Annual Computer Security Applications Conference*.
- Martin, Anya. 2002. Cyberinsurance Offers Affordable Security. *Atlanta Business Chronicle*, March 22, available at  
<http://www.bizjournals.com/atlanta/stories/2002/03/25/focus10.html> (last visited April 24, 2004).
- Mas-Collell, Andrew, Michael D. Whinston, and Jerry R. Green. 1995. *Microeconomic Theory*. New York, N.Y.: Oxford University Press.
- McDonald, Tim. 2000. Report: Year's Hack Attacks To Cost \$1.6 Trillion. *ECommerce Times*, July 12, available at  
<http://www.ecommercetimes.com/perl/story/3741.html> (last visited April 24, 2004).
- McGowan, David. 2005. The Trespass Trouble and the Metaphor Muddle. *Journal of Law, Economics, and Policy* 1:109-146.
- Megiddo N. 1978. Cost Allocation for Steiner Trees. *Networks* 8:1-6.
- Meyer, Wendy S. 2003. Notes, Insurance Coverage for Potential Liability Arising from Internet Privacy Issues. *Journal Corp. Law* 28:335.
- Moriarty, Kathleen M. 2003. Distributed Denial of Service Incident Handling: Real Time Inter-Network Defense.  
<http://www.watersprings.org/pub/id/draft-moriarty-ddos-rid-05.txt>

- Moukheiber, Z. 1998. Got a Hacker Policy? *Forbes*.
- Mullen, Timothy M. 2002. Defending Your Right to Defend: Considerations of an Automated Strike-Back Technology, at <http://www.hammerofgod.com/strikeback.txt>.
- Mullin, Eileen. 2002. Project Map: Hedging Your Security Bets with CyberInsurance. *Baseline Magazine*, August 9, at <http://www.baselinemag.com/article2/0,3959,656097,00.asp> (last visited Apr. 24, 2004).
- Myers, G. J. 1979. *The Art of Software Testing*.
- Nash, John. 1950. Equilibrium Points in n-Person Games. *Proceedings of the National Academy of Sciences* 36:48-49.
- National Institute of Standards and Technology. 2002. The Economic Impacts of Inadequate Infrastructure for Software Testing, available at <http://www.nist.gov/director/prog-ofc/report02-3.pdf>.
- Nelson, M. G. 2000. Attacks on E-Businesses Trigger Security Concerns. *InformationWeek*, February 14, pp. 28-30.
- Nelson, M. 1998. ICSA Insures Against Attacks by Hackers. *Infoworld*, September 25.
- Nimmer, Raymond T. 2005. Data Control, Privacy and Transactional Information: The Role of Contracts and Markets. In *Securing Privacy In The Internet Age*, Stanford University Press.
- Noll. 1971. The Economics and Politics of Regulation. *Va. Law Review* 57:1016.
- Norman, Robert Paul. 2001. Virtual Insurance Risks. *Fall Brief* 31:14.
- Ogut, H, N. Menon, and S. Raghunathan. 2005. Cyber Insurance and IT Security Investment: Impact of Interdependent Risk. *Workshop on the Economics of Information Security (WEIS)*, Harvard University.
- Oram, Andy. 2004. Symbiot on the Rules of Engagement, <http://www.onlamp.com/lpt/a/4691>.
- Organisation for Economic Co-operation and Development. 1992a. *Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data*.
- Organisation for Economic Co-operation and Development. 1992b. *Security of Information Systems*.

- Ortzag, Peter R. and Joseph Stiglitz. 2002. Optimal Fire Departments: Evaluating Public Policy in the Face of Externalities. Working Paper, *available at* <http://www.brookings.org/views/papers/orszag/20020104.pdf>.
- Ozment, Andy. 2004. Bug Auctions: Vulnerability Markets Reconsidered. *Conference Papers in Proceedings of the Third Annual Workshop on Economics of Information Security*, May 4, *available at* <http://www.dtc.umn.edu/weis2004/ozment.pdf>.
- Pascuillo, Nicholas A. Insurance and High Technology: CyberInsurance: Consistency in Claims and Coverage Resolution, *available at* <http://www.whitewms.com/CM/Publications/publications141.asp> (last visited April 23, 2004).
- Paulson, Linda Dailey. 2004a. Researchers Develop Network-Security Visualization Tools. *Computer*, April, *available at* <http://www.computer.org/computer/homepage/0404/briefs/>.
- Paulson, Linda Dailey. 2004b. Spam Hits Instant Messaging. *Computer*, April, *available at* <http://www.computer.org/computer/homepage/0404/briefs/>.
- Pauly, Martin V. 1970. Cores and Clubs. *Public Choice* 9:53-65.
- Pauly, Martin V. 1967. Clubs, Commonality, and the Core: An Integration of Game Theory and the Theory of Public Goods. *Economica* 34:314-24.
- Peek, Marcy E. 2005. Beyond Contract: Utilizing Restitution to Reach Shadow Offenders and Safeguard Information Privacy. In *Securing Privacy In The Internet Age*, Stanford University Press.
- Peltzman, Sam. 1973. An Evaluation of Consumer Protection Legislation: The 1962 Drug Amendments. *Journal of Political Economy* 81(5):1049-1091.
- Pfleeger, Charles P. and Shari Lawrence Pfleeger. 2003. *Security in Computing*.
- Poletti, T. 1998. First-Ever Insurance Against Hackers. [http://www.infowar.com/hacker/hack\\_061798b\\_j.html-ssi](http://www.infowar.com/hacker/hack_061798b_j.html-ssi).
- Posner, Richard A. 1971. Killing or Wounding to Protect a Property Interest. *Journal of Law and Economics* 14:201-32.
- Powell, Benjamin. 2005. Is Cybersecurity is a Public Good? Evidence from the Financial Services Industry. Working Paper No. 57. Independent Institute, Oakland, CA.
- Pratt, John W. 1964. Risk Aversion in the Small and in the Large. *Econometrica* 32:122.

- Prosser, William L. 1943. The Implied Warranty of Merchantable Quality. *Minn. Law Review* 27:117.
- Quirk, P. 1981. *Industry Influence in Federal Regulatory Agencies*.
- Radacati Group. 2004. Market Numbers Quarterly Update, Q4 2003; Brightmail Inc. Spam Percentages and Spam Categories, February, at <http://www.brightmail.com/spamstats.html>.
- Radcliff, Deborah. 2000. Should You Strike Back?. *Computerworld*, <http://www.computerworld.com/governmenttopics/government/legalissues/story/0,10801,53869,00.html>.
- Radin, Margaret Jane. 2001. Distributed Denial of Service Attacks: Who Pays? *Cyberspace Law* 6(9):2, available at [http://www.mazunetworks.com/white\\_papers/radin-print.html](http://www.mazunetworks.com/white_papers/radin-print.html).
- Raul, Alan Charles, Frank R. Volpe, and Gabriel S. Meyer. 2001. Liability for Computer Glitches and Online Security Lapses. *BNA Electronic Commerce Law Report* 6(31), August 8.
- Rescorla, Eric. 2004. Is Finding Security Holes A Good Idea?, *Conference Papers in Proceedings of the Third Annual Workshop on Economics of Information Security*, available at <http://www.dtc.umn.edu/weis2004/rescorla.pdf>.
- Rothschild, Michael, and Joseph Stiglitz. 1976. Equilibrium in Competitive Insurance Markets: An Essay on the Economics of Imperfect Information. *Quarterly Journal of Economics* 90:629-649.
- Russell, D., and G. T. Gangemi. 1992. *Computer Security Basics*.
- Salkever, A. 2002. E-Insurance for the Digital Age. *BusinessWeek*, April.
- Savage, Marcia. 2000. Tripwire, Lloyd's Partner for Cyberinsurance. September 11, available at <http://www.techweb.com/wire/story/TWB20000911S0008> (last visited Apr. 22, 2004).
- Schechter, Stuart. 2002. Quantitatively Differentiating System Security. *Conference Papers in Proceedings of the 1st Annual Workshop on Economics of Information Security*, May 17, available at <http://www.sims.berkeley.edu/resources/affiliates/workshops/econsecurity/econws/31.pdf>.



- Schneier, Bruce. 2002. Computer Security: It's the Economics, Stupid. *Conference Papers in Proceedings of the 1st Annual Workshop on Economics of Information Security*, available at <http://www.cl.cam.ac.uk/users/rja14/econws/18.doc>.
- Schneier, Bruce. 2001. Insurance and the Computer Industry. *Communications of the ACM* 44(3):114-115.
- Schneier, Bruce. 2000. *Secrets and Lies: Digital Security in a Networked World*. New York: John Wiley & Sons, Inc.
- Schwartz, Winn. 1999. Striking Back. *Network World*, <http://www.networkworld.com/news/0111vigilante.html>.
- SecurityWizardry. File Integrity Checkers, available at <http://www.networkintrusion.co.uk/integrity.htm> (last visited August 9, 2004).
- Shapiro, Carl. 1991. Symposium on the Economics of Liability. *Journal of Economic Perspectives* 5:3.
- Shapiro, Jonathan S. Understanding the Windows EAL4 Evaluation, at <http://eros.cs.jhu.edu/~shap/NT-EAL4.html>.
- Shapley, Lloyd. 1953. A Value of  $n$ -person Games. *Annals of Mathematics Studies* 28:307-318.
- Shavell, Steven. 1991. Individual Precautions to Prevent Theft: Private Versus Socially Optimal Behavior. *International Review of Law and Economics* 11:123-132.
- Shavell, Steven. 1987. *Economic Analysis of Accident Law*. Harvard University Press.
- Shavell, Steven. 1979. On Moral Hazard and Insurance. *Quarterly Journal of Economics* 93(4):541-562.
- Smedinghoff, Thomas J. 2005. Defining the Legal Standard for Information Security. In *Securing Privacy In the Internet Age*. Stanford University Press.
- Smith, Bruce P. 2005. Hacking, Poaching, and Counterattacking: Digital Counterstrikes and the Contours of Self-help. *Journal of Law, Economics, and Policy* 1:171-196.
- Smith, Joel E. 1978. Invasion of Privacy by Sale or Rental of List of Customers, Subscribers, or the Like, to One Who Will Use It for Advertising Purposes, 82 A.L.R. 3d 772.
- Solove, Daniel J. 2005. The New Vulnerability: Data Security and Personal Information. In *Securing Privacy In The Internet Age*. Stanford University Press.

- Sutton, Michael, and Frank Nagle. 2006. Emerging Economic Models for Vulnerability Research. *5<sup>th</sup> Workshop on the Economics of Information Security (WEIS)*, Cambridge University, available at <http://weis2006.econinfosec.org/docs/17.pdf> (last visited August 3, 2006).
- Suzuki, Mitsuo, and Mikio Nakayama. 1976. The Cost Assignment of the cooperative water resource development: A Game Theoretical Approach. *Management Science* 22:1081-1086.
- Symantec Internet Security Threat Report. 2004. Available at [www.symantec.com](http://www.symantec.com), <https://enterprisesecurity.symantec.com/Content/displaypdf.cfm?SSL=YES&EID=0&PDFID=665&promocode=ITR>.
- Symbiot, Inc. 2004a. On the Rules of Engagement. <http://www.symbiot.com/pdf/iwROE.pdf>.
- Symbiot, Inc. 2004b. Symbiot Security Announces World's First Solution to Strike Back Against Network-Based Attackers. <http://www.symbiot.com/pdf/pr.030404pdf>
- Tiebout, Charles M. 1956. A Pure Theory of Local Expenditures. *Journal of Political Economy* 64(5):416-424.
- Thurrott, Paul. 2004. Source Code Leak Prompts Vulnerabilities, Warning from Microsoft. *Windows IT Pro*, February 18, at <http://www.windowsitpro.com/Articles/Index.cfm?ArticleID=41788&DisplayTab=Article> (last visited August 3, 2006).
- Trachtman, Joel P. 2004. Global Cyberterrorism, Jurisdiction, and International Organization. *Conference Papers in Proceedings of The Law and Economics of Cyber Security*.
- University of Illinois at Urbana-Champaign. 2006. Virtual Private Networking at UIUC. <http://www.cites.uiuc.edu/vpn/> (last updated August 18, 2006).
- United States Catholic Conference. 1997. *Catechism of the Catholic Church*. 2d ed. Washington, DC: USCC Publishing Services.
- United States Department of Commerce. 2004. Retail E-Commerce Sales in Fourth Quarter 2003 Were 17.2 Billion, Up 25.1 Percent From Fourth Quarter 2002, Census Bureau Reports, at <http://www.census.gov/mrts/www/current.html> (last visited April 24, 2004).
- Varian, Hal R. 2002. System Reliability and Free Riding, *Conference Papers in Proceedings of the 1st Annual Workshop on Economics of Information Security*, available at

<http://www.sims.berkeley.edu/resources/affiliates/workshops/econsecurity/econws/49.pdf>.

- Varian, Hal R. 2000. Managing Online Security Risks. *New York Times*, June 1, available at <http://www.nytimes.com/library/financial/columns/060100econscene.html>.
- Varian, Hal R. 1992. *Microeconomic Analysis*. 3d ed. W. W. Norton & Company.
- Vernon, Dan. 2003. Cybersecurity Consortium Gets Insurer's Backing. *Computerworld: Security*, available at <http://www.computerworld.com/securitytopics/security/story/0,10801,86209,00.html> (last visited August 2, 2006).
- Vijayan, Jaikumar. 2005. Citadel Security to Offer Software Insurance for Companies. *Computerworld: Security*, available at <http://www.computerworld.com/securitytopics/security/story/0,10801,104647,00.html?source=x73> (last visited August 2, 2006).
- Viscusi, Kip. 1991. Product and Occupational Liability. *Journal of Economic Perspectives* 5:71.
- Vogel, Timothy A. 2002. Dealing With Cyber Attacks on Network Security. *Practical Lawyer* 48(3): 35, April.
- Walsh, Lawrence M. 2001. On the Cutting Edge. *Information Security Magazine*, April, available at [http://infosecuritymag.techtarget.com/articles/april01/departments\\_news.shtml](http://infosecuritymag.techtarget.com/articles/april01/departments_news.shtml), April 2001.
- Washington Technology. 1998. *Selected Security Events in the 1990s, Vol. 13(18)*, December 10, available at [http://www.wtonline.com/news/13\\_18/special\\_report/277-1.html](http://www.wtonline.com/news/13_18/special_report/277-1.html) (last visited August 5, 2004).
- White House, The. 2003. *The National Strategy to Secure Cyberspace*, [www.whitehouse.gov/pcipb](http://www.whitehouse.gov/pcipb).
- Wiles, Russ. 2003. Cybercrime Insurance Growing. *Arizona Republic*, September 15, available at <http://www.azcentral.com/arizonarepublic/business/articles/0915insure15.html> (last visited April 23, 2004).
- World Bank Group, The. 2004. *Data and Statistics: World Development Indicators*, available at <http://www.worldbank.org/data/wdi2004/index.htm>.
- Young, H., N. Okada, and T. Hashimoto. 1982. Cost Allocation in Water Resources Development. *Water Resources Research* 18:463-475.

*ZDNet*. 2001. Hawking Cyberinsurance, March 12.

<http://www.zdnet.com.au/news/business/0,39023166,20208314,00.htm> (last visited April 25, 2004).

**APPENDIX A:**

**TABLE ON THE SALIENT PROVISIONS OF CYBERINSURANCE POLICIES**

	Net Advantage Security	e-Comprehensive	Webnet Protection
<b>COVERAGES</b>			
<b>First Party Coverages</b>			
Destruction, disruption or theft of information assets	Y	Y. Expressly covers malicious alteration or malicious destruction of information by any person, of information as a result of malicious code, of computer programs owned or licensed. (This may be covered under definition of "computer system" (includes "computer software accessible through the Internet") of netAdvantage	Y. Includes coverage for losses due to malicious codes ("Malicious code" defined as "software program that maliciously introduced into the computer the Insured's Information Processing System and/or networks, and propagates itself from one computer to another without the authorization of the Insured Company". Are viruses excluded from coverage?) Includes computer programs and trade secrets. <i>Proviso that information and computer program be subject to regular network <u>back-up</u> procedures.</i> Payment of actual and necessary expenses incurred to replace or restore info assets to the level which they existed prior to the loss.
Internet Business Interruption	Y	Y. Dependent business interruption covered by endorsement.	Y. Includes dependent income loss.
Cyberextortion	Y	Y. "The Insured shall use its best efforts at all times to ensure that	Y

		knowledge regarding the existence of the Extortion coverage afforded by this Policy is restricted as far as possible.”	
Fraudulent electronic transfers	N. Expressly excluded.	Y. Express covered: Insured having transferred fund or property as direct result of fraudulent: input of data, modification or destruction of information, preparation or modification of computer program, alteration or destruction of information due to malicious code.	Not expressly covered. (Probably not covered under definition of e-business information assets (=electronic information and computer programs). Not a qualifying cause.
Denial of service attack		Expressly covered	Y. Expressly stated as a “qualifying cause”
Rehabilitation expenses		Y. Reimbursement for expenses incurred to Reestablish the reputation of the insured (including public relation expenses)	Y. Public relations expenses
<b>Third Party Liability Coverages<sup>198</sup></b>			
Internet Content	Y	Y (Libel, invasion of privacy (“the right of individual to control the disclosure of Information that identifies the individual,) copyright infringement, plagiarism, etc. Emotional distress excluded.	Y. Libel, invasion of privacy, plagiarism, infringement of IP (except patent)
Internet Security	Y. For claims arising from “failure of security” (defined as: failure of insured’s	Y	Y

<sup>198</sup> For claims made during the policy period or extended reporting period for acts committed by the insured on or after the Retroactive Date and before the end of the Policy Period.

	hardware, software or firmware (including firewalls, filters, DMZs, anti-virus) including theft of passwords or access codes which results in a computer attack). Note: Unintentional programming and/or operational error does not constitute failure in security.		
Defense Costs	Y	Y. Insurer has right and duty to defend. Limit: up to payment of "all reasonable and necessary legal costs".	Y
<b>EXCLUSIONS</b>			
Failure to back-up	Y	Y	Y
Failure to take reasonable steps to maintain and upgrade security	Y	Y. Always includes proviso on its coverages: "Provided always that the Insured Company maintain System Security levels that are equal to or superior to those in place as at the inception date of this Policy"	In "Policy Conditions": "You agree to protect and maintain your computer system and your e-business information assets and e-business communications to the level or standard at which they existed and were represented..."
Fraudulent, dishonest and criminal acts of insured	Y	Y	Y
Inability to use or lack of performance of software programs	Y. Due to expiration, cancellation, withdrawal, or have not been released from development stage, or have not passed test runs; or due to installation or failure to install software; or due to	Y. Any "malfunction or error in programming or errors or omissions in processing" (in computer programs) excluded.	Implied exclusion: lack of performance of software programs not part of "qualifying cause".

	configuration problems.		
Wear and tear of insured's information assets	Y	Y. "Loss resulting from (a) mechanical failure, (b) faulty construction, (c) error in design, (d) latent defect, (e) wear and tear, (f) gradual degradation, (g) electrical disturbance, (f) failure, breakdown or defect within the medium upon which any electronic record may be stored"	"Based upon or arising out of ordinary wear and tear, gradual deterioration of; or failure to maintain [e-information] assets and computer systems on which they are processed..."
Electric and telecommunication failures	Y	Y (see above). (Also: "The failure or interruption of the infrastructure of the Internet or other telecommunications system, except where such infrastructure was under the operational control of the insured.	Failure of: telephone lines, data transmission or wireless connections, telecommunications equipments or electronic infrastructure not under the insured's control, malfunction of satellite, failure of power or utility service
Breach of patents or trade secrets	First party: Trade secrets covered provided valuation agreed upon; 3 <sup>rd</sup> party both patents and trade secrets excluded		1 <sup>st</sup> party covered –as part of "electronic information". Third party: Patent infringement excluded
Loss or claim notified a prior insurer	Y	Y	Y
Claim arising out of liability to related parties	Y	Y	Y
(1 <sup>st</sup> and 3 <sup>rd</sup> party: failure of any computer or software to correctly assign any date)		Y	
<b>OTHER RELEVANT PROVISIONS</b>			
Retentions	Retention same as in liability limits below + retention	There is only single loss retentions ("arising out of any single event	Waiting period specified for business interruption.



	waiting hours for business interruption and internet extra expense coverages.	or series of related event"). Any recovery (net of expenses) of property, money, etc., applied according to (1) loss of insured on top of single loss or aggregate policy limits (2) reimbursement of amount paid by insurer (3) single loss retention.	Each loss deductible, and each claim deductible, for any loss or claim arising from the same interrelated qualifying cause.
Liability Limits	Limit for each wrongful act or related acts, each for (a) internet content liability, (b) internet security liability, (c) cyber-extortion; and for each failure or series of related failures of security: (d) asset and income protection.	Insurer liable only after insured satisfies retention and shall not exceed policy limit. Aggregate limits for (a) 1 <sup>st</sup> party (b) 3 <sup>rd</sup> party; with applicable single loss limit for each; sub-limit if contingent business interruption (one resulting from failure of computer not operated by insured but upon which insured depends upon) if endorsement opted.	Aggregate Policy Limit (for 1 <sup>st</sup> and 3 <sup>rd</sup> party losses). Separate limits for each coverage parts (3 3 <sup>rd</sup> party coverages, and 6 1 <sup>st</sup> party coverages). With stipulation for hourly loss limit and total limit for business interruption and dependent business interruption.
Criminal Reward Fund	Y		Investigative expenses by insured expressly covered.
Fees and expenses incurred by the insured for the services by the Information Risk Group in order to mitigate the impact of 1 <sup>st</sup> party loss		Covered as 1 <sup>st</sup> party coverage. The services of the group shall be engaged only "if the Named Insured is unable to prevent the effects of the loss by its own diligent terms".	
Representations Relied Upon	Y	Y	Y
Surveys	Y. At any time.	Y. Annual: Insurer has right to survey operations and premises; costs born by insurers.	Y. At option of insurer: as part of underwriting, in deciding whether to continue/modify coverage, or processing of loss/claim.
Insurer liable only for transcription or	Definition of "Loss" ("actual and	1 <sup>st</sup> Party loss of info, etc.: insurer shall be	1 <sup>st</sup> party insurance is for "restoration costs" (that

replacement cost	necessary costs incurred by the insured for replacing, reproducing, recreating, or restoring the insured's information assets".	liable only for (a) labor for the transcription or copying of information, programs, or e-record, or the purchase of hardware and software for actual reproduction of info, program or e-record.	is, "actual and necessary expenses [incurred] to replace, restore, or recreate [e-assets] to the level or condition in which they existed prior to the loss").
Additional offices covered		Establishment of additional offices or information processing system (other than consolidation, merger or purchase of assets of another company) covered provided insured employs "at least the same level of system security as were in place for the existing systems and offices at the inception of this policy".	
Notice required for change of control		Insured shall notify insurer of change in power to determine management by virtue of ownership, voting rights, or contract; otherwise coverage terminated for loss or claim "after the date of change of control"	
Termination of policy	Y. 30 days notice from insurer.	Y. 60 notice from insurer, or immediate upon receipt of notice from insured; refund of unearned premiums computed pro-rata. Insurers not liable for loss not discovered prior to the effective date of termination.	30 days within after notice from insurer, 10 days in case of non-payment of premium). Pro-rata premium.

## CURRICULUM VITAE

### EDUCATION

*Ph.D. Economics*, University of Illinois at Urbana-Champaign, Nov. 2006

*Dissertation*: "Three Essays on the Law and Economics of Information Technology Security"

*Dissertation Chair and Adviser*: Prof. Thomas Ulen

*Field Courses*: Development, International, Public Economics, Macroeconomics

*J.D.*, with honors, Ateneo de Manila University, Philippines, 1996

*B.S. Economics, cum laude*, University of the Philippines at Diliman, Philippines, 1992

### CURRENT POSITION

Assistant Professor, Department of Economics, Weber State University, Fall 2006-

### RESEARCH AND TEACHING INTERESTS

- Research: Law and Economics, Economics of Internet Security, Law and Development
- Teaching: Law and Economics, Game Theory and the Law, Statistics/Quantitative Methods, Microeconomics/Macroeconomics

### PUBLICATIONS

"Hacking Back: Optimal Use of Self-Defense in Cyberspace," with J. Kesan, *Journal of Legal Studies* (peer-reviewed), 2006 (in progress).

"Cyberinsurance as a Market-Based Solution to the Problem of Cybersecurity," with J. Kesan and W. Yurcik, to be submitted to law reviews, 2006 (in progress).

"Optimal Mix of Individual Precautions and Police Enforcement When Risks are Interrelated: The Case of Cybercrimes," 2006 (in progress)

"The Economic Case for Cyberinsurance," with J. Kesan and W. Yurcik, in *Securing Privacy in the Internet Age* (peer-reviewed), edited by Anupam Chander, Lauren Gelman, and Margaret Jane Radin. Stanford: Stanford University Press, 2006 (forthcoming).

"Cybercrimes and Cyber-Attacks: Technological, Economic, and Law-Based Solutions," with J. Kesan, in vol. 4 of *Cybercrime & Security*, edited by Pauline C. Reich. Dobbs Ferry, N.Y.: Oceania Publications, 2006.

"Balance-of-Payments Crises: Timing the Collapse of the Philippine Peso," *The Philippine Review of Economics and Business* (peer-reviewed), 1992.

### CONFERENCE PRESENTATIONS

The Telecommunications Policy Research Conference (TPRC), "Public Goods and Externalities Aspects of Internet Security: Modeling the Spill-over Effects of Interrelated Risks and Solutions," Sept. 29-Oct. 1, 2006, George Mason University School of Law, Arlington, VA.

Oxford University, "Hacking Back: Optimal Use of Self-Defense in Cyberspace," Safety and Security in a Networked World, Sept. 8-10, 2005, Oxford, UK.

Harvard University, "Cyberinsurance as a Market-Based Solution to Cybersecurity," Workshop on Economics of Information Security, June 2-3, 2005, Cambridge, MA.

Stanford Law School, "The Economic Case for Cyberinsurance", Securing Privacy in the Internet Age, March 13-14, 2004, Stanford, CA.

### **RESEARCH AND PROFESSIONAL EXPERIENCE**

#### **UNIVERSITY OF ILLINOIS, URBANA-CHAMPAIGN**

*Research Assistant*, College of Law, Fall 2003 - Summer 2005

- Did research on law and economics of cybersecurity
- Presented in and attended various conferences in law and economics, and economics of Internet security
- Maintained office in National Center for Supercomputing Applications (NCSA) and the Coordinated Science Laboratory (CSL) in order to collaborate with computer experts to gain more knowledge on the technology side of the projects.
- Co-authored published papers and conference submissions; prepared and gave conference presentations and poster sessions.
- Prepared research proposals for review and submission by research supervisor.

### **OTHER INSTITUTIONS**

*Economist*, Corporate Planning Division, San Miguel Corporation, 1998

*Tax Lawyer*, Arthur Andersen, Manila Office, 1996-97

- Did transfer pricing and international taxation work
- Performed corporate and tax law work for the biggest corporations in the Philippines.

*Planning Officer*, Department of Science and Technology, Philippines, 1992-1995

- Assessed and generated novel indicators for measuring science and technology resources.

### **TEACHING EXPERIENCE**

#### **WEBER STATE UNIVERSITY**

*Assistant Professor of Economics*,

Principles of Microeconomics (Fall 2006), 2 sections

Law and Economics (Fall 2006)

- Employs the Socratic Method

#### **UNIVERSITY OF ILLINOIS, URBANA-CHAMPAIGN**

*Lecturer*,

Business Statistics 1 (Summer 2003)

*Teaching Assistant*,

Principles of Microeconomics (Fall 2000, Spring 2001)

Business Statistics 1 (Fall 2001, Fall 2005)

Business Statistics 2 (Spring 2002, Fall 2002, Spring 2003)

- Listed in teachers ranked as excellent by their students (Spring 2002, Fall 2002, Spring 2003).

### **HONORS AND AWARDS**

- Fulbright scholar (2 years)
- Second Honors Silver Medal, Ateneo de Manila University School of Law
- Rank #27 out of ~ 4,000 bar examinees (#2 in criminal and civil procedure)
- G.P. Sicat Award for best undergraduate thesis in economics

- Member, Phi Kappa Phi International Honor Society
- Member, Pi Gamma Mu International Honor Society for the Social Sciences
- 99+ percentile ranking in national college entrance examinations (class valedictorian)