University of Illinois College of Law

Law and Economics Working Papers

Year 2004 *Paper* 2

The Economic Case for Cyberinsurance

Jay P. Kesan[*] Rupterto P. Majuca[†]

William J. Yurcik[‡]

[*] University of Illinois College of Law, kesan@illinois.edu

[†] Department of Economics, University of Illinois at Urbana-Champaign

[‡] National Center for Supercomputing Applications, University of Illinois at Urbana-Champaign

The Economic Case for Cyberinsurance

Jay P. Kesan, Rupterto P. Majuca, and William J. Yurcik

Abstract

We present three economic arguments for cyberinsurance. First, cyberinsurance results in higher security investment, increasing the level of safety for information technology (IT) infrastructure. Second, cyberinsurance facilitates standards for best practices as cyberinsurers seek benchmark security levels for risk management decision-making. Third, the creation of an IT security insurance market redresses IT security market failure resulting in higher overall societal welfare. We conclude that this is a significant theoretical foundation, in addition to market-based evidence, to support the assertion that cyberinsurance is the preferred market solution to managing IT security risks.

THE ECONOMIC CASE FOR CYBERINSURANCE[1]

Jay P. Kesan* **Ruperto P. Majuca**** **William J. Yurcik*****

*College of Law;
**Department of Economics;
***National Center for Supercomputing Applications (NCSA)
University of Illinois at Urbana-Champaign
<kesan@law.uiuc.edu> <majuca@uiuc.edu> <byurcik@ncsa.uiuc.edu>

Keywords: cyberinsurance, liability, Internet security

Abstract:

We present three economic arguments for cyberinsurance. First, cyberinsurance results in higher security investment, increasing the level of safety for information technology (IT) infrastructure. Second, cyberinsurance facilitates standards for best practices as cyberinsurers seek benchmark security levels for risk management decision-making. Third, the creation of an IT security insurance market redresses IT security market failure resulting in higher overall societal welfare. We conclude that this is a significant theoretical foundation, in addition to market-based evidence, to support the assertion that cyberinsurance is the preferred market solution to managing IT security risks.

[1] We thank Lauren Gelman, Anupam Chander, and Peggy Radin for organizing a terrific Symposium that featured many insightful presentations. We also like to thank the other participants in the Symposium for their helpful comments and suggestions.

I. INTRODUCTION

The Internet has radically changed the way business is carried out and is fast dominating our professional and personal lives.[2] Internet traffic is growing at between 200-600 percent per year, as tens of millions of people log on to the Internet every day.[3] While U.S. retail sales increased a mere 5.4 percent in 2003, e-commerce sales surged 26.3 percent to $54.9 billion in the U.S.[4] Overall, business-to-business e-commerce sales worldwide is expected to soar from $1.93 trillion in 2002 to $8.53 trillion in 2005.[5]

However, software vulnerabilities are extraordinarily pervasive resulting in the exposure of Internet businesses to a wide array of e-risks[6] as well as potential for e-litigation[7] involving property damage, business interruption, defamation, invasion of privacy, theft of credit card numbers, malpractice and consumer fraud. The rise in available cracker tools makes it easier to exploit these vulnerabilities.[8] High profile firms such as Microsoft, Amazon.com, eBay, Yahoo, CNN.com have been hit by denial-of-service (DoS) attacks, rendering these firms to be unreachable over the Internet for

[2] Brian D. Brown, *Emerging Insurance Products in the Electronic Age*, 31-FALL BRIEF 28 (2001).
[3] Robert Paul Norman, *Virtual Insurance Risks,* 31-FALL BRIEF 14, 15 (2001).
[4] U.S. Department of Commerce, *Retail E-Commerce Sales in Fourth Quarter 2003 Were 17.2 Billion, Up 25.1 Percent From Fourth Quarter 2002, Census Bureau Reports* (For release Feb. 23, 2004), *at* http://www.census.gov/mrts/www/current.html (last visited April 24, 2004).
[5] Matthew Clark, *B2B E-Commerce Sales to Skyrocket* (May 8, 2002), *at* http://www.enn.ie/news.html?code=7426802 (last visited April 24, 2004).
[6] Ernst &Young reported that 34% of the 1400 organizations surveyed admits 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, *Computer Security-Related Insurance Issues* (September 2003), *at* http://www.iii.org/media/hottopics/insurance/computer (last visited April 14, 2004).
[7] Potential e-litigation may also relate to product liability claims (*e.g.,* 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, *supra* note 3, at 15.
[8] Nicholas A. Pascuillo, *Insurance and High Technology: CyberInsurance: Consistency in Claims and Coverage Resolution*, *at* http://www.whitewms.com/CM/Publications/publications141.asp (last visited April 23, 2004).

significant period of time.[9] Likewise the websites of the U.S. Senate, Federal Bureau of Investigation (FBI), the National Aeronautics and Space Administration (NASA), the Department of Defense (DoD), and Environmental Protection Agency (EPA) have been altered or rendered unreachable by crackers.[10] Surveys by Ernst & Young and the Computer Security Institute (CSI) reveal that 90% of businesses and government agencies have detected security breaches and 75% recognized financial loses from the breach.[11] The Love Bug virus (2000) affected 20 countries and 45 million users caused an estimated $8.75 billion in lost productivity and software damage.[12] Overall, InfoWeek estimated that computer viruses and hacking took an estimated damage of $266 billion in the United States and $1.6 trillion on the worldwide economy in 1999.[13]

A particular issue that this symposium is concerned with relates to privacy issues on the Internet.[14] Organizations and businesses that obtain online information should

[9] Nancy Gohring, *Cyberinsurance May Cover Damage of Computer Woes*, SEATTLE TIMES (July 29, 2002), *available at* http://www.landfield.com/isn/mail-archive/2002/Jul/0133.html (last visited April 23, 2004). Timothy A. Vogel, *Dealing With Cyber Attacks on Network Security*, 48 PRAC. LAW 35, 36 (Apr. 2002).

[10] Vogel, *supra* note 9.

[11] Insurance Information Institute, *supra* note 6. Theft of proprietary info brought the highest loss ($70.2 million total loss), an average loss of $2.7 million. The second most expensive was DoS attacks, which resulted in $65.6 million loses, up 250 percent from last year. *Id.;* Susan E. Fisher, *Seeking Full Protection for Net Asset,* INFOWORLD (Oct. 5, 2001), *available at* http://webbytes.com/portfolio/text/iw100501.html (last visited April 23, 2004). The FBI estimated that the average lost from network security breach in 1999 is $142,000. Daintry Duffy, *Prepare for the Worst*, DARWIN MAG. (Dec. 2000), *available* at http://www.darwinmag.com/read/120100/worst.html (last visited April 24, 2004). 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 41percent of total loses. *Id.*

[12] Insurance Information Institute, *supra* note 6.

[13] Tim McDonald, *Report: Year's Hack Attacks To Cost $1.6 Trillion*, ECOMMERCE TIMES (July 11, 2000), *available at* http://www.ecommercetimes.com/perl/story/3741.html (last visited April 24, 2004). Will Knight, *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).

[14] 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. Wendy S. Meyer, Notes, *Insurance Coverage for Potential Liability Arising from Internet Privacy Issues*, 28 J. CORP. L. 335, 337-38 (2003) (citing Martic C. Loesch & David M. Brenner, *Coverage on the Technology Frontier,* CORP. OFFICERS & DIRECTORS LIABILITY LITIG. REP., Feb. 17, 1998, at 9; Joel E. Smith, *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, 773 (1978)).

have a responsibility to protect the confidentiality of the data,[15] yet few have satisfactorily installed sufficient safeguards to protect online data, especially credit card and social security number information.[16] The availability of privacy laws and regulations concerning Internet data suggests that courts will hold firms liable for harm to individuals.[17] The liability claims can arise from: (a) torts action based on privacy violation, (b) breach of an implied contractual duty, (c) violation of regulations intended to safeguard privacy, and (d) federal legislation intended to safeguard personal data online.[18] With the growing concern over security on online data, it can be expected that there will be increased regulation of Internet privacy.[19]

In this symposium, several ideas have been examined as possible solutions to the security and privacy problems. These ideas range from technology-based solutions[20] to a wide array of legal-based approaches (regulation,[21] penal legislation,[22] tort liability,[23]

[15] *Id.* at 335.

[16] *See, e.g., Hawking Cyberinsuranc*e (Mar. 12, 2001), *at* http://www.zdnet.com.au/news/business/0,39023166,20208314,00.htm (last visited April 25, 2004) (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, *supra* note 6 (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).

[17] Meyer, *supra* note 20, at 341.

[18] Meyer, *supra* note 20, at 338-41.

[19] *Id.*

[20] *See, e.g.,* Lance J. Hoffman, *An Architecture to Allow Metadata-Driven Legal and Economic Controls in Privacy Sensitive Systems*, *in* THIS VOLUME (2004) (proposing that surveillance systems be designed to adhere to privacy principles).

[21] *See* Daniel J. Solove, *The New Vulnerability: Data Security and Personal Information*, *in* THIS VOLUME (2004).

[22] *See* Susan W. Brenner, *Should Criminal Liability Be Used to Secure Data Privacy?*, *in* THIS VOLUME (2004) (examining the option of enacting "public welfare" type legislation to impose criminal sanctions for data privacy violation).

[23] *See* Jennifer Chandler, *Tort Liability for Cyber Insecurity: The Case of Distributed Denial of Service Attacks*, *in* THIS VOLUME (2004).

contract law,[24] quasi-contracts,[25] and fiduciary trust law[26]). These solutions all have the following feature in common: they rely primarily on non-market remedies.

In this work, we propose instead a market-based solution for improving Internet security and privacy from an economic incentives approach. Specifically, we articulate the economic rationale for cyberinsurance. Section II argues that traditional insurance policies do not adequately address the new perils of the information economy, while section III, the main part of the paper, discusses the three economic arguments for cyberinsurance. Section IV discusses the current emerging cyberinsurance practice, and Section V wraps our discussions with concluding comments.

II. Traditional Insurance Policies

The insurance policies firms have traditionally relied upon are: (a) business personal insurance (first-party policies); (b) business interruption policies; (c) commercial general liability (CGL) or umbrella liability insurance policies covering damages to third parties (including those arising from privacy violation); and (d) errors and omission insurance policies available to professionals to cover losses arising from the performance of the insured's professional services.[27]

These traditional insurance policies are designed to cover the perils of fires, floods, and other forces of nature and do not expressly cover Internet risks. Cyber-properties are without physical form and damaging attacks on them do not leave any

[24] *See* Raymond T. Nimmer, *Data Control, Privacy and Transactional Information: The Role of Contracts and Markets*, *in* THIS VOLUME (2004).
[25] *See* Marcy E. Peek, *Beyond Contract: Utilizing Restitution to Reach Shadow Offenders and Safeguard Information Privacy, in* THIS VOLUME (2004).
[26] *See* Lilian Edwards, *The Problem with Privacy: A Modest Proposal*, *in* THIS VOLUME (2004).
[27] Anna Lee, Student Notes, *Why Traditional Insurance Policies Are Not Enough: The Nature of Potential E-Commerce Losses and Liabilities*, 3 VAND. J. ENT. L. & PRAC. 84 (2001).

physical damage, thus resulting in disputes between insurers and firms as to what constitutes "tangible" property and "physical" damage.[28] Also, while most CGLs do not have worldwide coverage, most cyber-torts are international.[29] CGL policies usually stipulate a territory for coverage to apply, as well as where the action has to initiated; in contrast, it is an open question which court or state or country has jurisdiction over different Internet-related events.[30] In short, traditional insurance policies use terminology linking physical damage and tangible property and do not consider damage from non-physical property (such data loss) since they are intangible.[31]

Thus, traditional insurance policies do not explicitly cover Internet risks. While the insured want to stretch policies to include their Internet business, insurers consistently insist on the exclusion of cyber-losses from coverage.[32] This has resulted in costly litigation wars between insurers and their policyholders; insurers drafting more ironclad

[28] 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.

[29] Matthew Crane, *International Liability in Cyberspace*, 23 DUKE L. & TECH. REV. 1 (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. *Id.* at 3-4. Moreover, even if a firm's insurance policy expressly stipulate risk coverage, it is uncertain if this encompasses international torts. *Id.* at 9.

[30] Joshua Gold, *Insurance Coverage for Internet and Computer Relate Claims*, 19 NO. 4 COMPUTER & INTERNET LAW 8 (Apr. 2002).

[31] Hazel Glenn Beh, *Physical Loses in Cyberspace*, 8 CONN. INS. J. 55, 55-68 (2002).

[32] Norman, *supra* note 3, at 15 ("Many insurance carriers already have gone on record as saying that Love Bug losses are not covered under traditional insurance products.").

exclusions;[33] and insurers offering new insurance products to stack the case against inclusion.[34] Insurers are increasingly excluding e-risks from traditional insurance coverage.[35] The inadequacy of traditional insurance to deal with the new threats in the cyberworld brings to the fore the need for new insurance products specifically designed to cover the new perils of the Internet world.

III. ECONOMIC ARGUMENTS FOR CYBERINSURANCE

In this section, we present three primary economic arguments for cyberinsurance:

1) cyberinsurance increases IT safety;
2) cyberinsurance facilitates standards for best practices to be set at socially optimal levels; and
3) cyberinsurance solves a market failure and increase welfare in society.

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 case of a cyberattack. E-commerce losses may either be: (a) direct losses from the attack or intrusion, (b) business interruption (loss of productive time) and reputation losses, or (c) third party liability (suits for damages associated with privacy, defamation, etc.). All these potential losses are risks against which the firm would like to be covered for. Hence, it can purchase cyberinsurance that will pay it s in the event that a cyberloss occurs and the price of insurance is γ per dollar of cover. In the bad state (which occurs with probability

[33] Daintry Duffy, *Safety at a Premium,* CSO MAG. (Dec. 2002), *available at* http://www.csoonline.com/read/120902/safety.html (last visited April 23, 2004) ("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.")

[34] Beh, *supra* note 31, at 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.)

[35] Duffy, *supra* note 33.

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: $U(I_1^e\text{-}L^e\text{-}\gamma s\text{+}s)$. In the good state (which occurs with probability *1-p*), the firm has utility associated with its income in the good state minus the expenditure on insurance): $U(I_1^e\text{-}\gamma s)$. Hence, the firm purchases insurance coverage such that it maximizes its expected utility from both the good and bad states:

$$s^* = \arg\max EU = pU(I_1^e - L^e - \gamma s + s) + (1-p)U(I_1^e - \gamma s).$$

As shown in Figure 1, by purchasing insurance coverage of amount *s*, a firm moves from E to F: it spends γ*s* on insurance premiums so that in case a loss occurs, the insurer will pay out *s*. The firm gains from purchasing cyberinsurance since it moves from point E to point F which is on a higher indifference curve. The firm moves from point E (no insurance) to either to point F (full insurance) if $\gamma = p$ (premiums are actuarially fair),[36] or to point P (partial insurance) if $\gamma > p$ (insurance prices are higher).

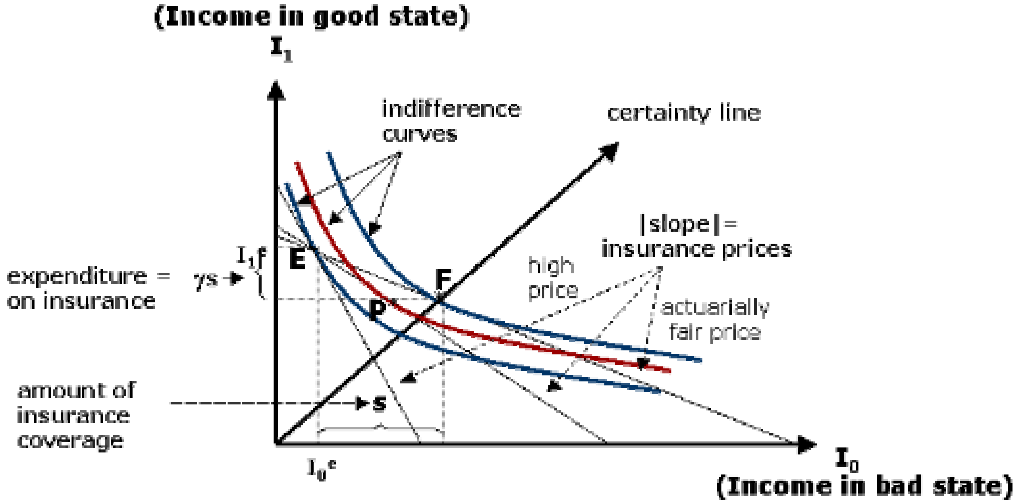

Figure 1: Expenditure on Cyberinsurance and Amount of Coverage

[36] The first-order (optimality) condition equate the slope of the indifference curves and the "budget lines": $\frac{p}{1-p}\frac{U'(I_1^e - L^e + [1-\gamma]s)}{U'(I_1^e - \gamma s)} = \frac{\gamma}{1-\gamma}$. $\gamma = p => U'(I_1^e - L^e + [1-\gamma]s) = U'(I_1^e - \gamma s) => L^e = s$. *i.e.,* the firm will fully insure if the insurance company charges an actuarially fair premium.

A. Cyberinsurance Increases IT Safety

There are three ways a firm can protect itself against damages: (a) self-protection, (b) self-insurance, and (c) outsourced insurance (cyberinsurance). Both self-insurance and cyberinsurance are protection against loss or redistribution of income from "good state" to "bad state", *i.e.,* they are both designed to reduce the *size* of the loss. The difference is that in cyberinsurance, the firm procures insurance from a third party while self-insurance is internal investment dedicated for use in the event of a loss. In contrast, self-protection is an attempt to reduce the *probability* of any losses from occurring in the first place.

Self-protection (which is also called "loss prevention") measures are like burglar alarms that reduce the probability of an illegal house entry. In cyber-security, self-protection may take the following form: authentication processes, anti-virus software, firewalls, virtual private networks, intrusion detection systems, vulnerability scans, system backups, and official security policies explicitly stating unacceptable behaviors.

Self-insurance (also called "loss protection") schemes are like sprinkler systems that reduce the loss from house fires. The following measures reduce the size of a loss in cybersecurity case: 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.

We seek to show that: (a) cyberinsurance and self-protection are "complements", (cyberinsurance increases self-protection),[37] (b) cyberinsurance and self-insurance are "substitutes" (an increase in expenditures on one would decrease the amount spent on the other), and (c) self-insurance decreases self-protection (the "moral hazard problem")[38].

Cyberinsurance results in higher investment in security, increasing the level of safety for IT infrastructure. New insurance products may make the Internet a safer business environment because cyberinsurers can require businesses to undertake loss self-protection activities, as well as tying premiums to claims histories.[39] Like in fire prevention, aviation, boiler and elevator safety where insurance generated safety improvements,[40] cyberinsurers can proactively tie premiums to the insured firm's investment in security processes and create market-based incentives for e-business to increase their level of IT safety.

Thus, contrary to the moral hazard argument that insurance will result in reduction in self-protection, investment in IT security is higher with cyberinsurance than without cyberinsurance, because cyberinsurance and loss prevention activities can be made "complements".[41] That is, the presence of cyberinsurance increases the amount

[37] 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. Isaac Ehrlich & Gary Becker, *Market Insurance, Self-Insurance, and Self-Protection*, 80 J. OF POL. ECON. 623 (1972).

[38] 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. In cyberinsurance, this may arise from the fact that 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 the hackers. Hence, they may be lax in their security efforts, as it may be less expensive to procure insurance than to keep on improving their IT security. Meyer, *supra* note 14, at 347-48. However, this may be prevented by cyberinsurers tying the firm's premium to their level of self-protection.

[39] Beh, *supra* note 31, at 80-81. 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. *Id.*

[40] Jeffrey Kehne, Note, *Encouraging Safety Through Insurance-Based Incentives: Financial Responsibility for Hazardous Waste*, 96 YALE L.J. 43, at n. 12-14 (1986).

[41] *See* Ehrlich & Becker, *supra* note 37.

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. Thus, insurers can insist that software companies deliver safe products and exert pressure on software engineering practices to improve in order to decrease exposure to various claims. In addition, the insurance companies have an incentive to monitor hackers in order to minimize the amount of damage they would have to pay out to its insured firms. Hence, private enforcement by insurance companies would supplement enforcement by the firms and agents of law enforcement.

As shown in Figure 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 of the "law of diminishing marginal returns" to investment in self-insurance products - each additional dollar of good-state income invested on self-insurance is less productive than the previous dollar invested.

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).[42] This demonstrates how self-insurance and cyberinsurance are substitutes.

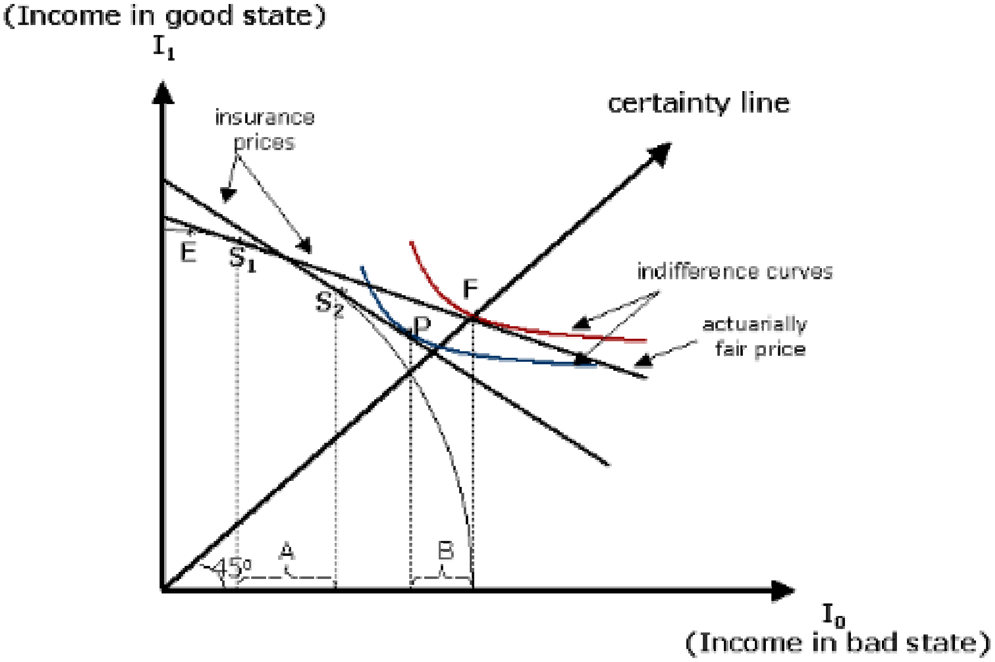

Figure 2: Self-insurance and Cyberinsurance as Substitutes[43]

Self-insurance, unlike cyberinsurance, has been known to create a moral hazard. Generally, if the price of insurance is independent of the expenditures in self protection, the reduction in the probability of the hazard would be exactly offset by the increase in the "loading factor" (roughly, the insurer's profit spread per dollar of coverage), which in turn reduces the demand for self-insurance. In this case, self-insurance and self-protection are likely to be "substitutes," that is, the availability of one discourages the other.[44] Since the price of self-insurance is independent of the probability of loss, one would see either a large demand for self-insurance and a small demand for self-

[42] *Id.* at 636.
[43] The figure is adapted from Ehrlich & Becker, *supra* note 37, at 635.
[44] *Id.* at 642-43.

protection, or the converse.[45] In contrast, cyberinsurance can actually increase self-protection since the price of cyberinsurance can be tied to the level of self-protection by the insured. Figure 3 graphically represents these relationships. We can conclude that since self-insurance creates a moral hazard, and self-insurance and cyberinsurance are substitutes, cyberinsurance is better than self-insurance in increasing Internet security (since cyberinsurance can increase self-protection if premiums are tied to the level of loss-prevention activities as an incentive to encourage higher self-protection care).

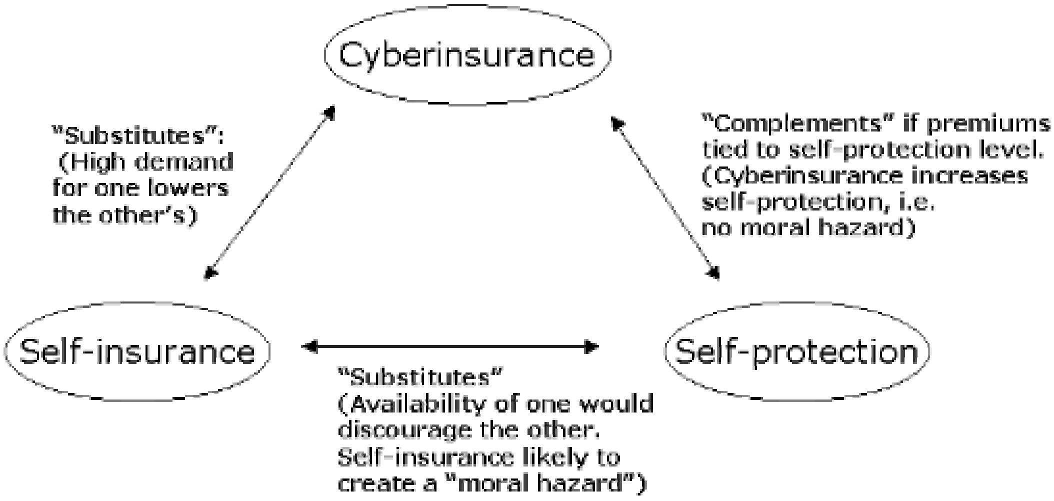

Figure 3: Cyberinsurance, Self-Insurance and Self-protection

B. *Cyberinsurance Facilitates Standard for Liability to be Set at Socially-Optimal Level*

Society can use three separate policy tools to deter accidents or torts: liability rules (which are implemented through the court system), safety standards (which are imposed by regulation), and insurance (a market mechanism). With regard to liability

[45] *Id.*

rules, one objective is that of providing efficient incentives for product safety.[46] On one hand, the liability rules can be used as a Pigouvian tax[47] to deter the harm or internalize the damages caused by the injurer (or faulty product manufacturer) to the victim (or consumer). When one party is made liable for injury caused to another, an externality has been internalized. On the other hand, the imposition of the "liability tax" on suppliers of risky goods and services results in alteration of economic activity; suppliers can be discouraged to innovate or possible new products may be set aside for fear of liability exposure.[48] The question is whether liability has become too expansive.[49]

Because IT security uses up resources in society, which can be utilized in more productive endeavors, more security is not necessarily always better. Figure 4[50] below shows the socially optimal-level of precaution. Thus, if we let p be 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 costs equals the costs of precaution plus the expected cyber-loss: $SC = wx+p(x)L.$

The line $p(x)L$ is downward-sloping because increased precaution decreases expected losses. However, extra precaution also increases costs (that is why the line wx

[46] The other objective is to compensate the victim. Carl Shapiro*, Symposium on the Economics of Liability*, 5 J. OF ECON PERSPECTIVES 3, 5 (1991).

[47] Arthur C. Pigou (1877-1959), a British economist and Professor of Economics at Cambridge University who pioneered welfare economics, wrote in his influential work, THE ECONOMICS OF WELFARE (first published in 1920) about the divergence of social and private costs and benefits. To correct for this, he proposed the imposition of a tax on externalities. Thus, a Pigouvian tax is one enacted to correct the effects of negative externalities. Ronald Coase in *The Problem of Social Cost,* J. L. & ECON. 1 (1960), proposed instead the definition of proprietary rights to correct the externalities problem when transaction costs are low.

[48] For instance, it has been estimated that liability costs represent 17 percent of the Philadelphia mass transit fares and from 15-25 percent of the price of a new ladder. With this, some products or services (such as some park rides and swimming pools diving boards at motels) have just vanished. Kip Viscusi, *Product and Occupational Liability*, 5 J. OF ECON. PERSPECTIVES 71 (1991).

[49] Shapiro, *supra* note 46, at 5.

[50] This graph and subsequent discussions are drawn from ROBERT COOTER & THOMAS ULEN, LAW AND ECONOMICS, 300-316 (3d ed. 2000). *See also* STEVEN SHAVELL, ECONOMIC ANALYSIS OF ACCIDENT LAW (1987).

is upward-sloping). The socially-optimal level, *x**, in Figure 4 (where the total social cost 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:[51]

$$\underset{\text{(marginal social cost)}}{w} \quad = \quad \underset{\text{(marginal social benefit)}}{-p'(x^*)L}$$

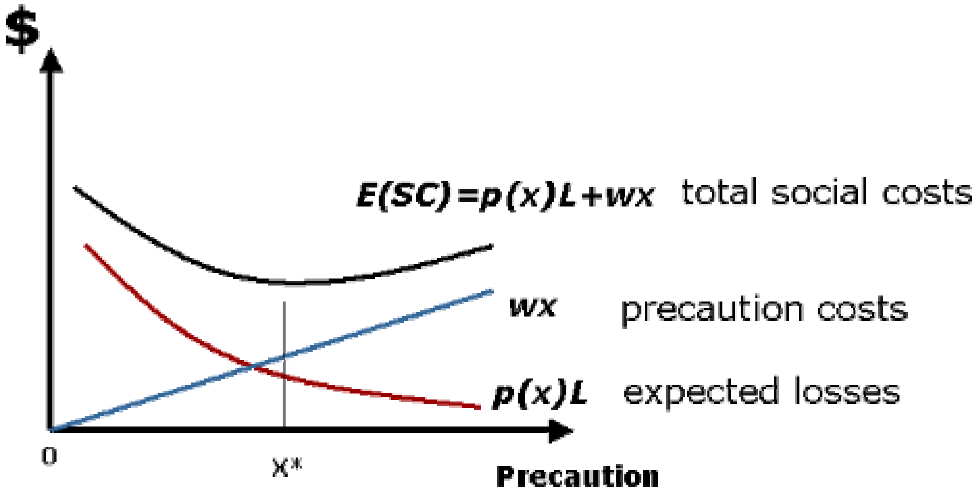

Figure 4: Socially-Optimal Precaution Level

This optimal level can, in theory, be implemented through the use of a liability rule under any of three different regimes: (a) no liability regime,[52] (b) strict liability, and (c) negligence rule. [53] In general, if the potential victim (but not the injurer) can take

[51] One cost of IT security is its trade-off with convenience. The rule in IT is that security is inversely proportional to convenience. Colleen Brush, *Surcharge for Insecurity*, *at* http://www.esmartcorp.com/Hacker%20Articles/ar_surcharge_for_insecurity.htm (last visited April 23, 2004).

[52] § 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 Millenium 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). *Cf. generally infra* n.61.

[53] 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, *supra* note 46, at 6.

precaution, then *no liability* regime is optimal.[54] If, on the other hand, the injurer (but not the victim) can take precaution, *strict liability* with perfect compensation results in efficient precaution, by causing the injurer to internalize the marginal costs and benefits of precaution.[55] However, when *both* the injurer and the victim can take precaution, neither *no liability* nor *strict liability* standard can erase 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.

For example, in the case of a simple negligence rule (illustrated in Figure 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 5 where precaution by the potential injurer is deficient. Hence, whenever $x_i < x^*$, the injurer is liable. Otherwise, if x_i is equal to or in excess of x^*, the injurer is not at fault, and therefore, the injurer is *not* liable (this corresponds to the permitted zone in the figure). Since in most cybersecurity cases, both the potential injurer and victim can take precaution, a negligence rule with the legal standard equal to the efficient level of care

[54] COOTER & ULEN, *supra* note 50, at 302-03. The victim chooses the level of precaution that minimizes his/her total costs *w*hich occurs when his/her marginal costs is equal to his/her marginal benefit. The 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. *Id.* at 303-04.

[55] *Id.* If the injurer (but not the victim) can take precaution, a *no liability* rule yields zero precaution. The injurer externalizes the benefits of precaution. *Id.* A rule of *strict liability* with deficient compensation (*D<L*) results in the injurer externalizing a fraction of the harm, and does not provide incentives for efficient precaution by the injurer. *Id*. at 305, n.8.

> For an example of strict liability regime, *see* Comprehensive Environmental Response, Compensation, and Liability Act (CERLA), 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, *supra* note 14, at 344-45.

results can theoretically result in efficient precaution.[56]

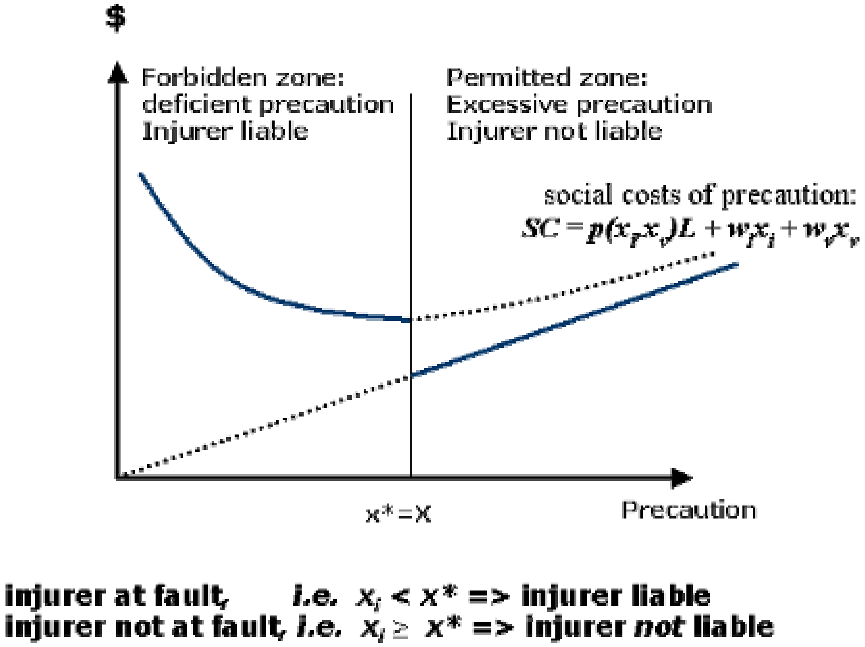

Figure 5: Simple Negligence Liability Rule[57]

In theory, the liability system can result in efficient precaution if x^* is set at just the right amount. However, the costs of bringing a liability suit are high.[58] 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.[59] Liability rules also do not work for many injuries where losses are smaller than the costs of bringing an action.[60] For cybersecurity in particular, litigation costs may be potentially high since the question of whether a victim

[56] *See* Chandler, *supra* note 23 (suggesting the imposition of negligence-based liability against the manufacturer of a software that falls below the standard of security).
[57] The figure is adapted from COOTER & ULEN, *supra* note 50, at 307.
[58] Shapiro, *supra* note 46 at 5.
[59] Shapiro, *supra* note 46, at 7.
[60] Kehne, *supra* note 40, at 410.

of a computer intrusion can be held liable for damage done by the cracker to others, is still not a settled issue.[61] Another danger is that the expansion of liability can coincide with the increased regulatory standards, particularly when liability and regulatory rules are not coordinated.[62]

Yet, 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 right level. Rule-makers are not subject to market pressures for precise risk categorization and are not always exact in their appraisal of long-term latent risks.[63] If the regulation overshoots the estimate, *i.e.* set a standard higher than is socially-optimal, innovation can be dampened. If, on the other hand, the standard is set too low, accidents and products defects will not be sufficiently deterred. Also, regulatory agencies may be susceptible to lobbying by powerful interest groups, as those opposed to stricter standards may obstruct or slow down regulation changes.[64] In addition, the administrative costs of updating regulation are far higher than adjusting premium rates.[65]

[61] For instance in the case where e-commerce sites are being targeted by hacktortionists, some believe that the real party at fault are firms not patching their systems. If network administrators kept tab the security alerts and routinely patch their systems, the impact of these vulnerabilities would be lessened. Lawrence M. Walsh, *On the Cutting Edge* (April 2001), *available at* http://infosecuritymag.techtarget.com/articles/april01/departments_news.shtml (last visited April 23, 2004). 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, *supra* note 51. 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, *supra* note 9, at 39-40. *But cf. generally supra* n.52 (ISPs shielded by legislation from liability).

[62] Viscusi, *supra* note 48, at 72.

[63] Kehne, *supra* note 40, at 410-11.

[64] Kehne, *supra* note 40, at 411 & n. 29, *citing* Noll, *The Economics and Politics of Regulation*, 57 VA. L. REV. 1016, 1028-32 (1971); P. QUIRK, INDUSTRY INFLUENCE IN FEDERAL REGULATORY AGENCIES (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").

[65] *Id.* at 412.

This is where market-based deterrence can offer definite advantages. Because of pooling of information and superior expertise in assigning proper prices to risk as well as in developing safety standards, insurers have better knowledge in setting this level of care as compared to regulators coping with complex technical issues.[66] Since precise risk categorization requires a predictable relationship between safety practices and liability, the use of the insurer's superior information in adopting the right level of reasonable care allows insurers to cause firms to set loss prevention measures to efficient levels. 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.[67] This could be done by cyberinsurers requiring the insured firms to set their loss prevention activities equal to the level that will bring about the socially efficient level of care. Insurance companies can thus facilitate standards for best practices by calibrating the amount of IT security they require the insured to possess to socially-optimal levels.[68]

In sum, because of the high transaction costs associated with the liability system, as well as the problems associated with a regulatory regime (insufficient expertise in characterizing risk, political lobbying, and high administrative costs), market-based incentives such as cyberinsurance are a better alternative than either a liability or regulatory system at deterring harm and setting IT security at the socially-efficient level.

[66] Kehne, *supra* note 40, at 410 ("To operate profitably, insurers must maintain strong incentives for underwriters to assess risks accurately.")

[67] *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 & ULEN, *supra* note 50, at 313-14).

[68] Thus, for instance, insurers have lobbied considerably for mandatory air bags in automobiles and pressured the government to force industries to change. Beh, *supra* note 31, at n. 130 *citing* Robert Kneuper & Bruce Yandle, *Auto Insurers and the Air Bag*, 61 J. RISK & INS. 107 (1994), *available at* 1994 WL 13386236.

C. Cyberinsurance Increases Social Welfare

The current level of uncertainty under traditional insurance policies results in under-investment in insurance, and thus an insufficient amount of profit-smoothing by firms and an inefficient level of risk-sharing throughout society. The absence of markets for bearing 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 bear such risks.[69] Thus, a market failure exists due to "non-marketability" (or the absence of markets for bearing of Internet risks). To overcome the lack of optimality due to non-marketability, a cyberinsurance market can be created. Hence, the creation of cyberinsurance solves a market failure[70] and results in higher welfare for society.

The amount of welfare gains associated with the introduction of cyberinsurance can be calculated in dollar terms for varying levels of risk aversion and the probability of a cyber-attack occurring. By comparing the market value of income in the first-best case with full cyberinsurance with the situation when there is no cyberinsurance, we are able to provide dollar estimates of the value of insurance to society. The market value of income (which, in Table 6 below, 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 "no cyberinsurance" era to that of the "with cyberinsurance" era, we are

[69] Kenneth Arrow, *Uncertainty and the Welfare Economics of Medical Care*, 53 AM. ECON. REV. 941, 946 (1963).

[70] 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 (*i.e.* "marketability" of all goods and services relevant to costs and utilities); (b) existence of some set of prices which will clear all markets (*i.e.,* 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. Creating markets for the bearing of e-risks plugs the loophole.

able to calculate the welfare gains. This approach is similar to that of measuring welfare gains from trade in international macroeconomics.[71]

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

1. *General Methodology for Measuring Welfare Gains from Cyberinsurance*

In Figure 6, 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 γ per dollar of cover. In this case, the firms pay the insurer I^e_1-I^* and if the attack occurs, the cyberinsurer pays the insured firms I^*-I^e_0. By entering into this trade, the firms are able to attain a higher indifference curve by (fully) insuring. A measurement of welfare change is line $\overline{A}\overline{B}$ (the difference between the *y*-axis intercepts of the "budget lines" tangent to those level curves).[72]

[71] *See* Earl L. Grinols & Kar-Yiu Wong, *An Exact Measure of Welfare Change,* 24 No. 2 CAN. J. OF ECON. 428 (1991); Earl L. Grinols, *A Thorn in the Lion's Paw: Has Britain Paid Too Much for Common Market Membership?*, 16 J. OF INT'L ECON. 271 (1984); Douglas A. Irwin, *The Welfare Costs of Autarky: Evidence from the Jeffersonian Trade Embargo, 1807-1809,* DARTMOUTH COLLEGE, MIMEO (2002); Daniel M. Bernhofen & John C. Brown, *Estimating The Comparative Advantage Gains from Trade: Evidence from Japan,* WORKING PAPER (2003); FEENSTRA, ADVANCED INTERNATIONAL TRADE (forthcoming).

[72] 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: $\frac{\partial U / \partial I_0}{\partial U / \partial I_1} = \frac{p \quad du / dI_0(I_0)}{(1-p)\, du / dI_1(I_1)}$ => $\frac{\partial U / \partial I_0}{\partial U / \partial I_1} = \frac{p}{(1-p)}$ 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. *See* CARL P. SIMON & LAWRENCE BLUME, MATHEMATICS FOR ECONOMISTS (1994) for a general discussion of homogenous functions in economics.

Thus, from the figure, we can implement the measurement of welfare gains $\overline{A}\overline{B}$ with the following steps:

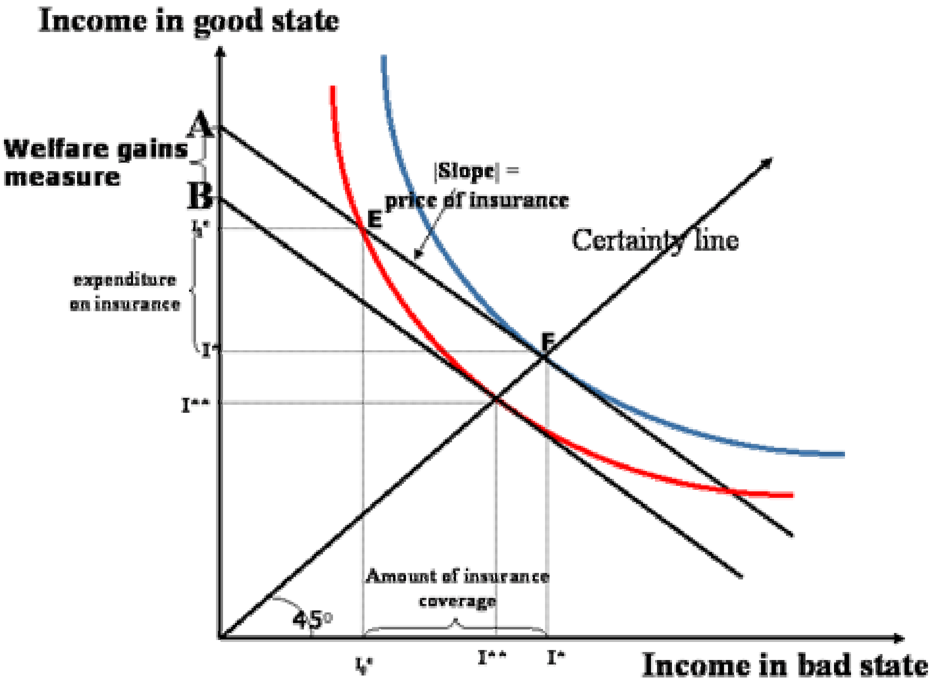

Figure 6: Measuring Welfare Gains

Step 1: Get data on income in good ($I^e{}_0$) and bad ($I^e{}_1$) states.

Step 2: Get data on p (the probability of an attack) and γ (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 $\overline{U}$. As is common in the macroeconomics and finance literatures, we assume a constant relative risk aversion among firms. We calculate the gains for varying levels of risk aversion coefficient.

Step 4: Calculate I^{**}.

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

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	**$ 1,943,507,000**	<= we use this figure as $\boldsymbol{I^e_0}$

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**[73]. This means that **I^e_1 = $ 3.143 billion** (I^e_0 + the $ 1.2 billion damages).

Step 2: Since industry reports indicate that cyberinsurers charge premiums which range from $5,000 to $ 60,000 per $ 1 million of cover (depending on the extent of the risk and the assets and protection extended), [74] we calculated for $p=\gamma$ = 0.005, 0.01, .002, 0.03, 0.04, 0.05, and 0.06. As an example, in the case where $p=\gamma$ = .06, $I^e_1 = A - 0.06\, I^e_0$ => *$ 3.1435 Billion = A – 0.06*\$ 1.9435 Billion* => A = $ 3.2407 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:[75]

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

[73] Russ Banham, *Hacking It (Cyberinsurance)(Statistical Data Included),* CFO, MAG. FOR SENIOR FIN'L EXEC. (Aug. 2000), *available at* http://www.findarticles.com/cf_dls/m3870/9_16/63916347/p1/article.jhtml (last visited Apr. 24, 2004). Gohring, *supra* note 9.

[74] *See* Becca Mader, *Demand Developing for Cyberinsurance,* BUS. J. OF MILWAUKEE (Oct. 11, 2002), *available at* http://www.milwaukee.bizjournals.com/milwaukee/stories/2002/10/14/focus2.html (last visited Apr. 24, 2004).

[75] Note that for σ=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-ρ)* is equal to the reciprocal of the risk aversion coefficient, and the log-utility case (*σ=1*) correspond to the Cobb-Douglas level sets: CRRA: $U = p\dfrac{I_0^{1-\sigma}}{1-\sigma} + (1-p)\dfrac{I_1^{1-\sigma}}{1-\sigma} = \overline{K}$.

CES: $[a_1 I_0^{\rho} + a_2 I_1^{\rho}]^{\frac{1}{\rho}} = K \Rightarrow a_1 I_0^{\rho} + a_2 I_1^{\rho} = \overline{K}$.

This means 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 bear risks is determined by the curvature of the utility function, $\sigma = -\frac{u''(I)}{u'(I)} I,$ which is known in the literature as the Arrow-Pratt[76] coefficient of (relative) risk aversion. Higher σ's are associated with higher risk aversion.[77] The general consensus in the literature is that reasonable levels of risk aversion is such that σ is anywhere from 1 to 3, so we calculate the welfare gains (and the premiums) for varying levels of risk aversion within that range, *i.e.* for σ = 1,1.5, 2, 2.5, 3.

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

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

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

$$\overline{U} = .06\frac{I^{**(1-2)}}{1-2} + (1-.06)\frac{I^{**(1-2)}}{1-2} = -0.33 \quad => I^{**-1} = -\overline{U}$$

$$=> \; I^{**} = -\frac{1}{\overline{U}} = \$3.0312\,billion\,.$$

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

⇨ *B= 1.06 (I*) = 1.06* $3.0312* billion = *$ 3.2131* billion

⇨ *Welfare gains* = A-B = *$ 47,040,870.76.*

[76] John W. Pratt, *Risk Aversion in the Small and in the Large,* 32 ECONOMETRICA 122 (1964).

[77] For a general introduction on the economics of uncertainty, *see* HAL R. VARIAN, MICROECONOMIC ANALYSIS (3d ed. 1992), at 173-192.

We performed the same calculations for σ=1, 1.5, 2, 2.5, 3 and p=γ=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 the tables 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 by as much as $78.7 million for a firm with a high degree of risk aversion (σ=3) facing a high probability of an attack (p=γ=0.06). Overall, we calculate that had cyberinsurance been available, the welfare gains associated with insuring worldwide security breaches and virus attacks in 2000 would be had been as much as $13.16 billion. Our calculations of the welfare gains are broken down for various levels of risk aversion and probabilities of cyber-attack occurring.

3. *Calculating Cyberinsurance Premiums*

We also calculate the total premium that the insured would be willing to pay for varying levels of risk aversion and attack probabilities. Following Cochrane (1997),[78] the premiums may be calculated as follows: $(I_m - \prod)^{(1-\sigma)} = p \cdot I_0^{e(1-\sigma)} + (1-p) \cdot I_1^{e(1-\sigma)}$ where $I_m = p \cdot I_0^e + (1-p) \cdot I_1^e$. Solving for Π, we have:

$\prod = I_m - \left[p \cdot I_0^{e(1-\sigma)} + (1-p) \cdot (I_1^{e(1-\sigma)}\right]^{\frac{1}{1-\sigma}}$. As for the case of the welfare gains

[78] John H. Cochrane, *Where is the Market Going? Uncertain Facts and Novel Theories*, 21 ECON. PERSPECTIVES 3 (1997).

calculations, we calculated the premiums for σ=1, 1.5, 2, 2.5, 3 and $p=\gamma$ = 0.005, 0.01, 0.02, 0.03, 0.04, 0.05, 0.06. Our results are presented in Tables 1 and 2.

Table 1: Premiums and Welfare Gains: Year 2000 DoS Attacks (in $Mn)

	Risk Aversion Parameter σ =	**1**	**1.5**	**2**	**2.5**	**3**
Premiums	**p=γ=0.005**	$1.55	$2.54	$3.67	$5.03	$6.62
	0.01	$3.08	$5.02	$7.29	$9.96	$13.10
	0.02	$6.09	$9.90	$14.34	$19.54	$25.60
	0.03	$9.03	$14.64	$21.17	$28.75	$37.54
	0.04	$11.90	$19.25	$27.76	$37.60	$48.93
	0.05	$14.69	$23.72	$34.14	$46.10	$59.79
	0.06	$17.42	$28.07	$40.30	$54.26	$70.15
Welfare Gains	**p=γ=0.005**	$1.59	$2.57	$3.73	$5.09	$6.69
	0.01	$3.23	$5.19	$7.49	$10.18	$13.35
	0.02	$6.69	$10.58	$15.12	$20.41	$26.60
	0.03	$10.37	$16.17	$22.89	$30.70	$39.75
	0.04	$14.28	$21.95	$30.80	$41.03	$52.81
	0.05	$18.41	$27.92	$38.85	$51.41	$65.79
	0.06	$22.76	$34.08	$47.04	$61.84	$78.69

Table 2: Worldwide Cyberinsurance Premiums and Welfare Gains (in $Bn)

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

IV. EMERGING CYBERINSURANCE MARKET

The emerging practice in the new cyberinsurance market[79] seems to match our

[79] The new cyberinsurance products can cover several areas including loses 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. Preston Gralla, *Electronic Safety Net: Cyberinsurance Policies Can Offer Protection When Technology Fails*, CIO MAG. (Dec. 1, 2001), *available at* http://www.cio.com/archive/120101/et_article.html (last visited Apr. 22, 2004). Some examples of these products include NetSecure by Marsh (*see Hawking Cyberinsurance* (Mar. 12, 2001), *available at* http://www.zdnet.com.au/news/business/0,39023166,20208314,00.htm (last visited Apr. 25, 2004); American International Group (AIG), Inc.'s NetAdvantage Security (covering damages arising from

theoretical predictions. For example, related to our discussion on IT security and premium-induced self-protection, cyberinsurers in developing coverage have required applicants to provide either: (a) costly top-to-bottom physical and technical analysis of security, networks, and procedures,[80] or (b) fill in a detailed online questionnaire comprising of about 250 queries,[81] to assess an applicant's security risks and cyberprotections (technology budget, security infrastructure, virus-protection programs, testing and safety procedures, and outsourcing). This allowed firms to assess their risks and become better aware of their security needs and also allowed insurers to engage in an ongoing dialogue with the firms about their security risks. Insurance coverage to firms with less cyberprotections, with a greater percent of its business online, or in a highly-

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, *supra* note 27, at 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, *supra* note 2, at 33), and products by St. Paul Companies, CNA, InsureTrust.com (*See* Lee, *supra* note 27), and Zurich North America (*See* Russ Wiles, *Cybercrime Insurance Growing*, ARIZ. REP. (Sept. 15, 2003), *available at* http://www.azcentral.com/arizonarepublic/business/articles/0915insure15.html (last visited April 23, 2004). 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.

[80] 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* Eileen Mullin, *Project Map: Hedging Your Security Bets with Cyberinsurance* BASELINE MAG. (Aug. 9, 2002), *in* http://www.baselinemag.com/article2/0,3959,656097,00.asp (last visited Apr. 24, 2004). 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, *supra* note 73).

[81] Realizing that a stringent underwriting strategy can be onerous for buyers, insurers have recently toned down their rigorous stance. For example, AIG introduced a three-level underwriting process: (1) online application and, if the firm passes the criteria, a conditional price quote within 2 days, (2) online assessment upon completion of the security questionnaire and remote evaluation of its security by the technology partners, (3) full-blown physical assessment. Insuredotcom.com developed an online questionnaire, comprising as many as 250 queries for CIOs, CFOs and legal counsels to fill out and get an idea of the price and how comprehensive the insurance will be, and decide whether to procure e-insurance or not. The downside of a remote scan is that it doesn't take into account the human-element issues and it doesn't allow for an in depth inspection of the computer systems. *Id.*

regulated business subject to high penalties like financial firms, are considered to be higher risk.[82] 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 those who have installed a professional security system.[83] Insurers also use monitoring of the firm's security processes,[84] third-party security technology partners,[85] rewards for information leading to the apprehension of hackers,[86] and expense reimbursement for post-intrusion crisis-management activities.

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.[87] 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.[88] This premium has the result of encouraging software manufacturers to produce better software products.

With regard to our theoretical discussions on cyberinsurance creating surplus for both insured and insurers, current industry estimates reveal a growing demand for cyberinsurance products The Insurance Information Institute (I.I.I.) estimates that

[82] Mullin, *supra* note 80.
[83] 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, *supra* note 73.
[84] Engaging in dialogue between insurer and insured about their risks is important to developing coverage.
[85] 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.
[86] AIG's NetAdvantage Security offers up to $50,000 for leads which result in the apprehension and conviction of a cybercriminal. Duffy, *supra* note 11.
[87] Marcia Savage, *Tripwire, Lloyd's Partner for Cyberinsurance* (Sept. 11, 2000), *available* at http://www.techweb.com/wire/story/TWB20000911S0008 (last visited Apr. 22, 2004). Gralla, *supra* note 79; Lee, *supra* note 27. Safeonline also agreed to provide premium discounts of 10 to 20 percent to customers of Recourse Technologies. Walsh, *supra* note 61.
[88] *Id.*

cyberinsurance could become a $2.5 billion market by 2005.[89] IT-related policies, for instance, form 30%-40% of the policy mix for InsureHiTech. As more insurers enter the market, driving down prices, coverages will broaden and user-friendliness will increase.

However, the newly-introduced cyberinsurance schemes are not without problems. The market has yet to reach its potential. First, high costs -- premiums can range from $5,000 to $60,000 per $1 million of coverage -- makes it relatively beyond reach of small and medium-sized companies.[90] Second, underwriting qualifications lack standardization and remain complex and time-consuming. Unlike traditional insurance where decades of information are available, e-risks have scant precedent.[91] Lack of actuarial or event data on all types of losses uncertainty as well as information over the potential worst-case damage liability present problems associated with calculation of risks and premium pricing. Since insurers rely on measures of predictability to forecast probable risk and set prices, the absence of enough historical and actuarial data for Internet risks makes it harder to determine prices.[92] It takes both time and stability to develop statistical data for actuarial tables; at the Internet new ventures are developed at a fast pace, flaws in software change dynamically, and new attacks are released daily. Furthermore, future risks are unknown since both hackers and anti-hacking technology are getting better.[93]

One possible solution to the risk-assessment problem is the partnering of

[89] Mader, *supra* note 74; Gohring, *supra* note 9.

[90] Insurance coverage is not offered to individuals although they can purchase identity-theft coverage. Wiles, *supra* note 79.

[91] Gohring, *supra* note 11.

[92] Anya Martin, *Cyberinsurance Offers Affordable Security,* ATLANTA BUS. CHRONICLE (Mar. 22, 2002), *available at* http://www.bizjournals.com/atlanta/stories/2002/03/25/focus10.html (last visited April 24, 2004). Walsh, *supra* note 11.

[93] *Hawking Cyberinsurance*, *supra* note 16.

insurance brokers with security service providers.[94] Another possibility is the coordination of 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.[95] The Critical Infrastructure Protection Board (CIPB) which was established by President Bush in October 2001, has developed a partnership with insurers to try to pool the data that exists in many sources within government and insurance industry to develop actuarial tables, a process that's expected to continue into 2005.[96] Along the same lines, the CyberInsurance Institute has found two non-profit organizations (RAND and CERT) which are in the forefront on cybercommerce insurance standard developing methods for assessment of threats and vulnerabilities.[97] One other option to spur the widespread adoption of cyberinsurance is for the federal government to subsidize insurance for cyber-activities.[98]

IV. SUMMARY AND CONCLUSIONS

The advent of the Internet has brought about new risks that traditional insurance policies do not satisfactorily cover. The creation of new insurance products that specifically deals with Internet perils results in: (a) better IT safety infrastructure and increased Internet security; (b) the standards for best practices and amount of due care to be set to optimal levels; and (c) providing a solution to a salient market failure which in turn brings overall welfare gains to society. Our survey of the nascent and immature

[94] Walsh, *supra* note 16.

[95] Lee, *supra* note 27.

[96] Duffy, *supra* note 33.

[97] Wiles, *supra* note 79.

[98] Lee, *supra* note 27, at 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.

cyberinsurance market provides a confirmation of the above-mentioned advantages that cyberinsurance can potentially generate for society at large.