CYBERINSURANCE AS A MARKET-BASED SOLUTION TO THE PROBLEM OF CYBERSECURITY—A CASE STUDY

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 conduct a case study of the cyberinsurance industry. We examine the developing cyberliability legislation and the emerging cyberinsurance market. We conclude that cyberinsurers are able to find ways to deal with several problems that could result in the failure of market solution. Although some issues still need to be worked out, we suggest that the direction to be taken should be towards resolving these issues, rather than giving up the market solution. When these obstacles are fully worked out, the full market solution can result in the following benefits. First, cyberinsurance would result in higher security investment, increasing the level of safety for information technology (IT) infrastructure. Second, cyberinsurance can facilitate standards for best practices as cyberinsurers seek benchmark security levels for risk management decision-making. Third, the creation of an IT security insurance market will result in higher overall societal welfare.

INTRODUCTION

Some commentators, including ourselves, have proposed using liability rules and cyberinsurance as solution to Internet security (see e.g. Varian 2002, Schneier 2000, Yurcik 2000, Kesan, Majuca and Yurcik 2004). In this paper, we perform a case study of recent cyberliability laws and the emerging cyberinsurance market, in order to shed light on such issues as: What is the relationship between cyberinsurance, liability rules, and social welfare?; What potential problems can beset the market solution from being fully implemented? How are the market participants dealing with such obstacles?; and What is the effect of cyberinsurance, and these market hindrances, to social welfare?. The approach we take is first to know what the cyberinsurers are actually doing, and how are they doing it. We can infer actual cyberinsurance industry practice from the various policies being offered by the insurers (what they cover, what they exclude, what other relevant provisions do they incorporate), as well as several aspects of the practice from various sources (what is the application process, what security checks are asked the applicants, how much are the premiums, and whether they are tied to the risk classification, etc.) Secondly, we can use theory to infer why the cyberinsurance practices is done that way, as well as to use the stylized facts to test which theories are more applicable and have more predictive power in the actual cyberinsurance and cyberliability environment. We also investigate how cyberinsurers are dealing with potential adverse selection, moral hazard, and other problems in the industry, and perform social welfare calculation of the gains from cyberinsurance, and the social loss from market failures.

The next section discusses what factors contributed to the emergence of new Internet insurance products. Section 2 discusses actual practice by cyberinsurers as can be gleaned from the cyberinsurance policies, and other industry practice. Section 3 uses theory to explain these practices and discuss the effect of cyberinsurance on Internet security and social welfare. Section 4 performs social welfare calculations on a fully developed market solution, as well as the social welfare loss that could result from market failures (e.g., asymmetric information). Section 5 wraps up our discussions with the summary and concluding comments.

I. FACTORS CONTRIBUTING TO THE EMERGENCE OF CYBERINSURANCE

Three factors helped contribute to the advent of new cyberinsurance products:

-- pervasive Internet risks;

-- the inadequacy of traditional insurance to cover these risks; and

-- the developing clarity in cyberliability law.

A. Pervasive Internet Risks

Although the Internet has increasingly dominated the modern era (Brown 2001), software vulnerabilities remain extraordinarily pervasive. They expose Internet businesses to both risks and liability for property damage, business interruption, defamation, invasion of privacy, theft of credit card numbers, malpractice and consumer fraud. Surveys by Ernst & Young and the Computer Security Institute (CSI) reveal that 90% of businesses and government agencies have detected security breaches, 75% of these businesses suffered a resulting financial loss, 34% of organizations admit of less-

than-adequate ability to identify if their intrusions in their systems, and 33% admit of lack of ability to respond (Insurance Information Institute 2003). The increase in the availability of cracker tools has made it easier for criminals to exploit these vulnerabilities. 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). Also, crackers have interfered with 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 the Environmental Protection Agency (EPA) (Vogel 2002, Insurance Information Institute 2003).

The FBI estimated that the average lost from network security breach in 1999 is $142,000. 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 loses (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). During the 2001 World Economic Forum, crackers who espouse the globalization cause had breached databases acquiring the participants' confidential data, including those of Bill Gates and former U.S .Secretary of State Madeline Albright, and accessed credit card numbers for 1,400 people. Overall, InfoWeek estimated that computer viruses and hacking caused damages of $266 billion in the United States and $1.6 trillion worldwide in 1999 (McDonald 2000, Knight 2000).

Clearly, the emergence of these new Internet risks results in a demand for insurance products addressing them.

B. The Inadequacy of Traditional Insurance Policies

The insurance policies which firms traditionally rely upon – (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; and (4) errors and omissions insurance (Lee 2001) – cover the traditional perils of fires, floods, and other forces of nature. The fact that they do not expressly cover Internet risks has resulted in: (1) costly litigation between insurers and their policyholders; (2) insurers drafting more ironclad exclusions (Duffy 2002); and (3) insurers developing new insurance policies to prevent inclusion of cyber-losses (Beh 2002). As an example, because cyber-properties do not necessarily have a physical form, attacks on them may not result in any physical damage. Accordingly, many disputes between insurers and firms have arisen, e.g., as to what constitutes "tangible" property and "physical" damage.[1] Additionally, although most CGLs (Commercial General Liability policy) do not have worldwide coverage, most cyber-torts are international (Crane 2001). Even if a

[1] Thus, 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.

firm's insurance policy stipulates risk coverage, it is uncertain if this encompasses international torts (Crane 2001).

The inability of traditional insurance to deal with the new cyber-threats again underscores the need to develop insurance products specifically designed to cover the new Internet risks.

C. Developing Clarity in Cyberliability Law

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 (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]). 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).

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. The HIPAA Security Regulations, issued in 2003, required health care providers to institute practically the same safeguards GLB security regulations:

> "(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.

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 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). So too, several commentators, as well as the *National Strategy to Secure Cyberspace* (www.whitehouse.gov/pcipb),[2] suggest that other firms not specifically covered by the regulations may have a general common law duty to protect the information under their control (Smendinghoff 2005 citing Radin 2001; Kiefer and Sabett 2002; Raul, Volpe and Meyer 2001; Kenneally 2000).

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

[2] 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".

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.

Because of these developments, insurance products specifically targeting the cyberspace have recently sprouted. The next section examines actual practice in the nascent cyberinsurance market

II. ACTUAL CYBERINSURANCE PRACTICE

A. Coverage

Some examples of the new Internet insurance products that have sprung up include NetSecure by Marsh; American International Group (AIG), Inc.'s NetAdvantage; J.H. Marsh & McLennan's NetSecure; Sherwood's e-Sher; Chubb's SafetyNet; Lloyds of London's e-Comprehensive and products by St. Paul Companies, CNA, InsureTrust.com, and Zurich North America (see Wiles 2003). Premiums can range from $5,000 to $60,000 per $1 million of coverage, depending on the type of business and the extent of insurance coverage.

First party coverages typically cover destruction or loss of information assets, internet business interruption, cyberextortion, loss due to denial of service attacks,

reimbursement for public relation expenses, and even fraudulent electronic fund transfers (see summary table on cyberinsurance products), while third party coverages typically cover claims arising from Internet content, Internet security, technology errors and omissions and defense costs.[3] Most policies explicitly exclude from computer software malfunction due to errors in programming and the like, as well as ordinary wear and tear of the insured e-business assets. Another common exclusion relates to losses due to failures of electric and telecommunication facilities, including electronic failure and satellite malfunction. Table 1 summarizes the different coverages of several prominent cyberinsurance products with the most complete coverages (see the Appendix for a more detailed examination of the salient provisions of the insurance policies).

Table 1: Summary Table of Typical Cyberinsurance Policies

	Net Advantage Security	e-Comprehensive	Webnet Protection
First Party Coverages			
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
Third Party Liability Coverages[4]			
Internet Content	Y	Y	Y
Internet Security	Y	Y	Y
Defense Costs	Y	Y	Y
EXCLUSIONS			

[3] Many cyberinsurers have different coverages to target different kinds of consumers. For example, there are products designed for people who are only interested in their own Internet security, products designed for firms who only want third party coverages, products designed to cover media liability, etc. (See, e.g., the different Net Advantage products. For instance the enactment of HIPAA resulted in healthcare companies being targeted cyberinsurance products (see http://www.aignetadvantage.com/content/netad/AIGhealthcareflyer.pdf). Some policies cover some specific risks (e.g. loss or claim associated with breach of patents or trade secrets, or bulletin boards), which other products exclude (see generally table in the Appendix for differences in coverage).

[4] 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.

Inability to use or lack of performance of software programs	Y	Y	Y
Ordinary wear and tear of insured's info assets	Y	Y	Y
Electric and telecommunication failures	Y	Y	Y

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. Current industry estimates reveal a growing demand for cyberinsurance products, as well. In fact, the Insurance Information Institute (I.I.I.) estimates that cyberinsurance could become a $2.5 billion market by 2005 (Mader 2002; Gohring 2002). IT-related policies, for instance, form 30%-40% of the policy mix for InsureHiTech.

B. Risk Assessment

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. Cyberinsurers require applicants to fill in a detailed online questionnaire, some consisting of about 250 queries, to assess the applicants' security risks and cyberprotections (technology budget, security infrastructure, virus-protection programs, testing and safety procedures, and outsourcing), and well as conduct a top-to-bottom physical and technical analysis of security, networks, and procedures. 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 (Mullin 2002).

The security health check starts with the applicant filling in an application form with the detailed security questionnaire. General background questions include information on the applicant's SIC [5] 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 Internet activities conducted (e.g., 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: (a) content;[6] (b) what professional services are offered;[7] and (c) network security.[8] Also, 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.

[5] Standard Industrial Classification.
[6] E.g., applicant's monitoring of its website's content, including the availability of a qualified intellectual property attorney, or a written policy for removing controversial items.
[7] E.g., 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.
[8] E.g., whether company policy on IT security, privacy, and allowable email/internet use are in place; 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 baseline risk assessment starts with information requests on: (a) the applicant's physical security;[9] (b) network diagram[10] and (c) description of network activities.[11] The physical reviews include 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 monitory 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 (see, e.g., InsureTrust's Network Security Services Baseline Risk Assessment).

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). Thus, 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. (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)). Insurers also utilize

[9] 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.

[10] Pinpointing the locations of systems and OSes, 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.

[11] E.g., 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.

monitoring of the firm's security processes, third-party security technology partners,[12] rewards for information leading to the apprehension of hackers,[13] and expense reimbursement for post-intrusion crisis-management activities. So also, 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).[14]

C. Mechanisms to Check Moral Hazard

We find that insurance policies incorporate several provisions designed to address the potential moral hazard problems (see Table 2 below summarizing insurance policy provisions on this regard). For example, as an inducement to have good security, insured firms cannot claim payment for loss or claim associated with failure to take reasonable actions to maintain and improve their security. 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

[12] 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.

[13] AIG's NetAdvantage Security offers up to $50,000 for leads which result in the apprehension and conviction of a cybercriminal (Duffy 2000).

[14] e-Comprehensive covers additional offices or information system established by the insured during the policy period, so long as the insured employs "at least the same level of security as we in place for the existing systems and offices at the inception of this policy". Moreover, the insured is required to notify the insurer for any change of control of the insured, and mergers and consolidations are excluded from coverage.

as at the inception of this Policy."[15] Also, 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 a first party loss. 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. 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".[16] Also, 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.

Table 2: Summary Table of Typical CyberInsurance Policies, Cont'd.

EXCLUSIONS	Net Advantage Security	e-Comprehensive	Webnet Protection
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
Claim arising out of liability to related parties	Y	Y	Y
OTHER RELEVANT PROVISIONS			
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 1st party loss, covered		Y	

[15] See also, Webnet policy condition, which states: "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…"

[16] See also, e.g., E-comprehensive's first party coverage of "malicious copying, malicious recording, or malicious sending of any information that constitutes a Trade Secret... provided the Insured has taken reasonable measures to prevent such copying, recording or sending of such Information."

Representations Relied Upon	Y	Y	Y
Regular/Annual Surveys of Insured's Facilities	Y	Y	Y

D. Some Issues

Some problems still beset the emerging cyberinsurance market. Aside from premium being too high[17] to be within the range that small and medium-sized companies or individuals can afford,[18] another problem with the developing cyberinsurance industry is the 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).[19] 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).[20] Also, some authors have suggested that the interrelatedness of risks in the Internet may somehow hinder the

[17] Since internet risks and security are complex, an assessment of a company's security can cost thousands of dollars, and that's before affixing the insurance premium. For example, AlphaTrust Corp.'s (insured by Insuretrust) security assessment cost about $20,000, while Marsh's security assessment cost $25,000 (Banham 2000). 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 assessment based on the questionnaire and a remote evaluation of the firm's security, and physical assessment (Banham 2000).

[18] Insurance coverage is not offered to individuals although they can purchase identity-theft coverage (Wiles 2003).

[19] 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.

[20] One possible solution to the risk-assessment problem is partnering insurance brokers with security service providers (Walsh 2001). Another possibility is coordinating 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, 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 industry (see Bohme 2005, Ogut, et al 2005).

We now turn our discussions to the theory behind cyberinsurance.

III. ECONOMIC THEORY AND CYBERINSURANCE

In this section, we explain the emergence of the cyberinsurance market, discuss the theory behind the practices of cyberinsurers, and talk about the role of cyberinsurance and liability rules in achieving IT security.

Without markets for Internet risk-bearing, the welfare of those wishing to transfer those risks, as well as those who, because of pooling and superior expertise, are willing to assume such risks, are reduced (see, e.g., Arrow 1963). Thus, the creation of new cyberinsurance products enables firms to transfer their e-risks and increase their utility level. Suppose that a 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. A firm can purchase an insurance coverage of amount s, at the price of γ per dollar of cover, i.e., the firm can spend γs on insurance premiums so that in the event a loss occurs, the insurer will pay out s. 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. Hence, the firm purchases insurance coverage such that it maximizes its expected utility from both the good and bad states:

$s^* = \arg\max EU = pU(I_1^e - L^e - \gamma s + s) + (1-p)U(I_1^e - \gamma s)$. 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: $U(I_1^e - L^e - \gamma s + s)$. If the insurance company charges an actuarially fair premium, the first-order (optimality) condition implies that:

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

i.e., the firm will fully insure. This enables the firm to move up to a higher indifference curve and increase its welfare.[21] However, as Internet risks become more prevalent, and given that traditional insurance do not adequately cover these risks, the demand for new cyberinsurance products becomes more pronounced.

We discuss next the potential problems to the full development of the cyberinsurance market, and how insurers are dealing with them.

A. Adverse Selection

In an ideal world, as the one depicted above, firms are able to fully insure. However, in certain instances, there are obstacles to the attainment of this first best solution. One problem that could arise is when insurers cannot distinguish between high and low risk applicants. When there is asymmetric information, adverse selection problems could arise, causing the first best solution to be unattainable (Rothschild and Stiglitz 1976). Only the second best solution – the best solution under incentive constraint – is feasible. Under this scenario, the insurer offers different 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 (Rothschild and Stiglitz 1976). Adverse selection problems therefore results in dissipative social welfare lost and unfair to the low

[21] These social welfare gains associated with the creation of cyberinsurance can be calculated, which we do in the next section.

risk firms. The low risk firms are the ones who suffer, because the high risk firms get full coverage, but low risk firms do not.

The rigorous *ex ante* security assessment allowed insurers to identify the applicants' risk types, and prevented the adverse selection problem to occur. Thus, cyberinsurers were apparently able to work around the adverse selection problem by requiring thorough, detailed, and extensive examination of the applicant firms. This way, they can distinguish between low risk firms and high risks ones, and charge premium according to the risk classification. By doing so, they avoid market failure that results in social welfare lost. We calculate in the next section the welfare gains that have resulted from this tactic of requiring a thorough health check of the applicants' security.

B. Moral Hazard

Another potential problem is the so called "moral hazard" problem (also known as the *hidden action* or *principal-agent* problem). This problem relates to the possibility that firms may slack in their security work, since it may be more cost effective for them to just buy insurance to cover their e-risks. This happens if the insurer is unable to observe the actions of the insured firm, which could result in negligence by the latter. However, as is well-known in the insurance literature, a solution to this problem involves observation by the insurer of the level of care taken by the insured to prevent the loss (see, e.g., Shavell 1979). Thus, as Ehrlich and Becker (1972) have shown, insurance and self-protection[22] can be "complements", i.e., insurance encourages self-protection, if the insurer can observe the protection level of the insured and the price of insurance is

[22] "Self-protection" expenditures are those made by the firm that reduces the *probability* of the loss. 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.

negatively related to the amount of self-protection.[23, 24] Thus, moral hazard may be prevented by cyberinsurers tying the firm's premium to their level of self-protection.

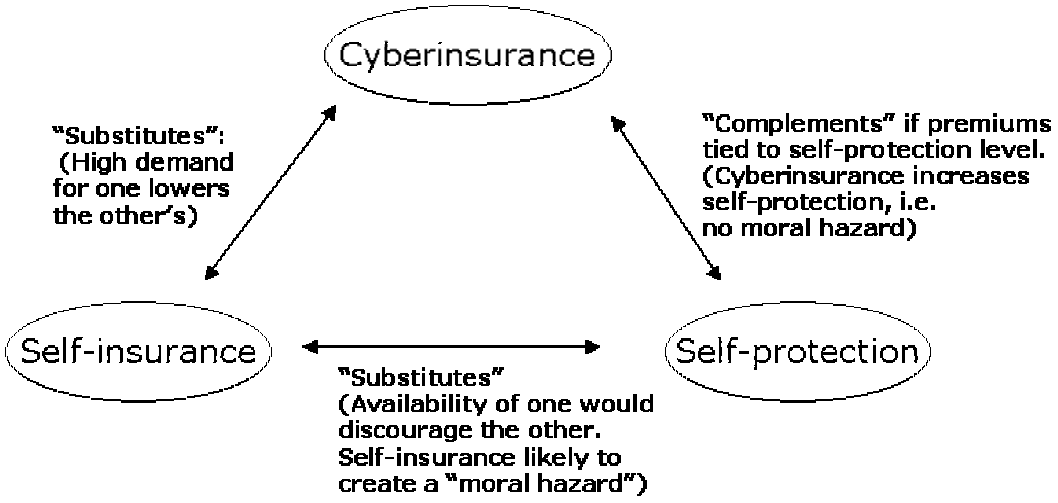

Figure 1: Cyberinsurance, Self-Insurance and Self-protection

The current industry practice is that cyberinsurers tie the premium to their *ex ante* assessment of the insured's risk classification. *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. They also 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. Also, as mentioned, insurers explicitly state that no coverage will be given to firms who fail to back up their

[23] 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).

[24] Ehrlich and Becker (1972) have also shown that, "self-insurance" (or investment designed to minimize the *amount* of the loss), unlike cyberinsurance, creates a moral hazard, i.e., self-insurance and self-protection act as substitutes. That is, 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). See Figure 1, for a summary of the relationships between cyberinsurance, self-insurance, and self-protection.

files. Cyberinsurers are therefore 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. Thus, cyberinsurance results in higher investment in security, increasing the level of safety for IT infrastructure (see also Kehne 1986 [insurance caused increased safety in fire prevention, aviation, boiler and elevators]). New insurance products can make the Internet a safer business environment because cyberinsurers can require businesses to minimize losses using economic incentives (Beh 2002).[25]

Thus, in contrast to the moral hazard argument that insurance will result in a reduction of self-protection, we believe that 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). If the security level can be perfectly observed either *ex ante* or *ex post*, 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. Also, cyberinsurance can give incentives to software companies to 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.[26]

---

[25] 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).

[26] Also, 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. 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. By using cyberinsurance, firms benefit consumers in several distinct ways. First,

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 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 lost (see, e.g., Shavell 1979).[27] 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.

C. Externalities

In the Internet world, externalities arise because of interdependencies. Computer systems have interdependent security such that a security event on one system affects all its peers even if they are under different administrative control. For example, if a malicious code penetrates the system through an compromised machine, it has an easier access to the remaining computers (Heal and Kunreuther 2003).[28] The lack of security in a computer or network can thus damage not only to that machine or network, but also all of the machines linked to the network. Hence, externalities arise because the action of one agent unavoidably affects the welfare of another agent. This externality problem often results in a security investment's private return that is lower that the social return

---

insurers that offer third-party cyberinsurance will pressure firms to fix security problems such as data leaks. As mentioned, right now, there exist specific security regulations requiring firms in the financial and health care 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 as well as several commentators suggest that there is a general duty to protect the information under their control (Smedinghoff 2005).

[27] Note that 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 applies to each loss.

[28] Thus, if an individual or firm does not use an anti-virus software, for example, it can cause infection other agents or leave them more vulnerable to losses. Hackers can also use compromised computers to launch attacks against other computers, as in the case of DDOS attacks.

(Heal and Kunreuther 2003). Since the firm takes into account only its private costs, the resulting level of security associated with the firm's profit-maximizing behavior diverges from the socially-optimal solution.

In studying interrelated risks, externalities, and insurance, Ortzag and Stiglitz (2002) has concluded that when the insurer cannot observe the level of precaution of the insured, moral hazard results in both the lowering of the level of care (relative to the socially-optimal level), and partial insurance coverage. Thus, there are two distortions that cause the level of care to be below the social optimum: the interdependence of the risks (externality), which results in a care below the social optimum, and the insurance coverage, which reduces the level of precaution even if risks were not interrelated. However, when the level of precaution can be fully observed and the insurer charges an insurance premium commensurate to the precaution level, the moral hazard problem disappears and there will be full insurance coverage.

D. Liability Rules, Cyberinsurance, and Information Security

We now turn to the discussion on the role of cyberinsurance and liability rules in achieving optimal levels of IT security in society.

As is true with other goods, there is an optimal amount of security. Figure 2 [29] below shows the socially-optimal level of precaution. Thus, if p is the probability of a cyber-loss, 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: $SC = wx+p(x)L$. The line $p(x)L$ is downward-sloping because increased precaution decreases expected losses. Extra

[29] This graph and subsequent discussions are drawn from Cooter and Ulen (2004); see also Shavell (1987).

precaution, however, also increases costs (that is why the line *wx* is upward-sloping). The socially-optimal level, *x*,* in Figure 2 (where the total social cost costs are at minimum), is achieved by equating the gain from the additional investment in security with the cost associated with extra security:[30]

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

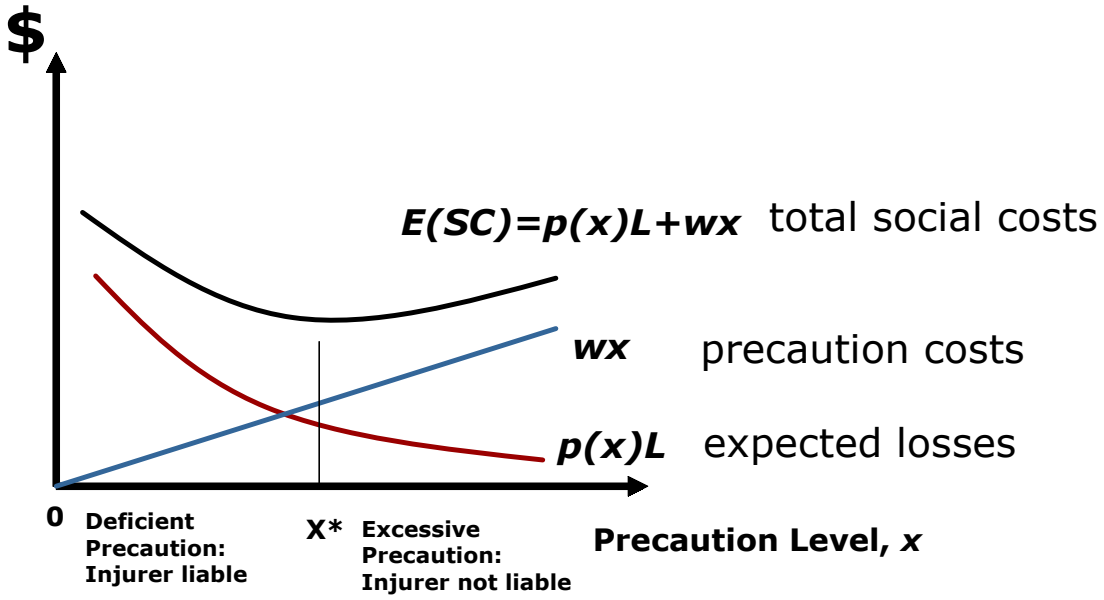

Figure 2: Socially-Optimal Precaution Level

The government must thus strike a balance in its design of liability rules.[31] On the one hand, liability laws can provide efficient incentives for product safety by functioning as a Pigouvian tax that deters harm or internalizes damages caused by the injurer to the victim (see Shapiro 1991). On the other hand, a liability tax imposed on suppliers of

[30] For example, one cost of IT security is its trade-off with convenience. The rule in IT is that security is inversely proportional to convenience (see, e.g., Brush 1991).
[31] In general, the government can use three distinct liability regimes to achieve a socially-optimal level of precaution: (1) no liability; (2) strict liability; and (3) negligence rule.

risky goods may discourage the suppliers from developing new, safer products out of a fear of exposing themselves to liability (Viscusi 1991).[32]

In general, if the potential victim, but not the injurer, can take precaution, the no liability regime is optimal. 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 gains and costs of precaution (Cooter and Ulen 2004). 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).[33]

How can cyberinsurance facilitate the design of optimal liability rules? Shavell (1982) has shown that, in the absence of insurance markets, the socially-optimal level of precaution is not achieved with the use liability rules alone, given that injurers are risk averse. However, when insurance markets are present, and insurers can observe the level of precaution, the optimal level of precaution can be achieved.[34] This is because injurers will be induced by their insurance policy to adopt the first-best precaution level. Hence, with cyberinsurers requiring insured firms to set their loss prevention activities equal to the level that will bring about the socially-optimal level of care, market-based pricing of risk and precaution can at least augment liability standards to achieve the first best

[32] 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).

[33] In the case of a simple negligence rule,[33] the optimal level of precaution is x^* (see Figure 2). Society can set the rule that the injurer is at fault whenever x_i falls below x^*. This is the forbidden zone 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 greater than x*, the injurer is not at fault, and therefore, the injurer is not liable (Cooter and Ulen 2004).

[34] Furthermore, under the negligence liability regime, this is achieved when the standard of care is set equal to the first best.

solution.[35] Also, because of pooling of information and superior expertise in assigning proper prices to risk, insurers have better information than – and can therefore at least assist – regulators coping with complex technical issues (Kehne 1986).

IV. SOCIAL WELFARE CALCULATIONS

We now calculate welfare gains that can accrue to society with the creation of cyberinsurance markets. Without markets for the bearing for cyber-risks, a market failure exists because of the "non-marketability" of Internet risks.[36] This results in a reduction in welfare below that fully-obtainable by society. Creating markets for the bearing of e-risks plugs the loophole. A cyberinsurance market would address this problem and create greater societal welfare.

The amount of welfare society gains from cyberinsurance can be estimated for varying levels of risk aversion and the probability of a cyber-attack occurring. The market value of income, which, in Figure 3 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. This is similar to the international macroeconomic approach of measuring welfare gains from trade (Grinols and Kar-yiu 1991; Grinols 1984; Irwin 2002; Bernhofen and Brown 2003; Feenstra forthcoming).

---

[35] In the automobile industry, for instance, insurers have lobbied for mandatory air bags in automobiles and pressured the government to force change in industries (Beh 2002, citing Kneuper & Yandle 1994).

[36] (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 (Arrow 1963).

We develop here a general methodology for calculating welfare gains from cyberinsurance and perform calculations for specific examples.

A. General Methodology for Measuring Welfare Gains from Cyberinsurance

Figure 3 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 γ per dollar of coverage. In Figure 3, the firm pays the insurer I_1^e-I^* and if the loss occurs, the cyberinsurer pays the insured I^*-I_0^e. By entering into this trade, the firm is able to attain a higher indifference curve by fully insuring. The change in welfare can be measured by the line $\overline{AB}$ (the difference between the *y*-axis intercepts of the "budget lines" tangent to those level curves).

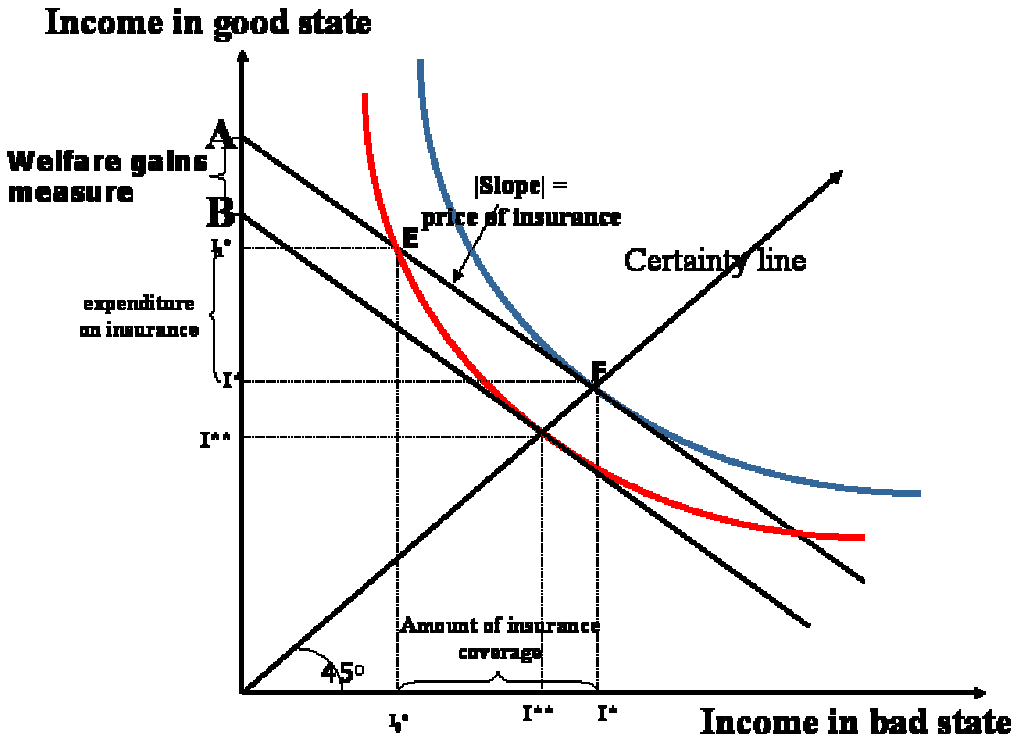

Figure 3: Measuring Welfare Gains

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: $\frac{\partial U / \partial I_0}{\partial U / \partial I_1} = \frac{p \quad du / dI_0(I_0)}{(1-p)\, du / dI_1(I_1)} \Rightarrow \frac{\partial U / \partial I_0}{\partial U / \partial I_1} = \frac{p}{(1-p)}$ 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 Simon and Blume 1994).

The following steps can thus be used to measure welfare gains $\overline{AB}$:

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. (Assume actuarially fair premiums.)

Step 3: Assume a particular parametric form of the utility function, and then calculate $\overline{EU}$ (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.

Step 4: Calculate I^{**}.

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

B. 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** (see, e.g., Banham 2000). This means that $\boldsymbol{I^e_1}$ **= $ 3.1435 billion** (I^e_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.[37]

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

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

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 ($\sigma=1$) correspond to the Cobb-Douglas level sets: CRRA: $EU = p\dfrac{I_0^{1-\sigma}}{1-\sigma} + (1-p)\dfrac{I_1^{1-\sigma}}{1-\sigma} = \overline{K}$.

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

[37] As an example of how to calculate *A*, in the case where $p = \gamma = .06$, $I^e_1 = A - 0.06\, I^e_0 \Rightarrow$ *$ 3.1435 billion = A – 0.06*$ 1.9435 Billion* => A = $ 3.26 Billion.

aversion. Higher σ's correspond to a higher aversion to risk (see Varian 1992, pp. 173-192 for a general introduction on the economics of uncertainty). Literature suggests that reasonable levels of risk aversion are such that σ 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

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

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

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

$$\Rightarrow I^{**} = -\frac{1}{\overline{EU}} = \$3.03\,billion.$$

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

$\Rightarrow B = 1.06\,(I^{**}) = 1.06 * \$3.0312$ billion = *$ 3.2131* billion

$\Rightarrow$ *Welfare gains = A - B =* *$ 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 1 and 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 (σ=3) facing a

high probability of an attack (p=γ=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.[38]

C. 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: $(I_m - \prod)^{(1-\sigma)} = p \cdot I_0^{e(1-\sigma)} + (1-p) \cdot I_1^{e(1-\sigma)}$ where $\prod$ is the total amount of premium paid and $I_m = p \cdot I_0^e + (1-p) \cdot I_1^e$. Solving for $\prod$, we have: $\prod = I_m - \left[p \cdot I_0^{e(1-\sigma)} + (1-p) \cdot (I_1^e)^{(1-\sigma)}\right]^{\frac{1}{1-\sigma}}$. Like the welfare gains 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. Tables 3 and 4 present our results.

Table 3: 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

[38] For our calculations of worldwide welfare gains, we used worldwide gross domestic product (GDP) data (see World Bank Group 2004) as the income in bad state and $1.6 trillion as the worldwide loss from hacking and viruses.

Table 4: 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

D. Calculating Social Welfare Loss Due to Adverse Selection

The welfare loss due to adverse selection can be estimated using similar steps used in measuring welfare gains. Thus, as an example, if there are only two types of insured in the economy, high risk and low risk insured, and we set the probability of loss to high risk and low risk insured as $p_H = 0.06$ and $p_L = 0.005$,[39] respectively, and if we assume that the insurer cannot distinguish between these two types, then the welfare loss due to adverse selection can be calculated as follows. 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, since in that case, the high risk applicants will mimic the low risk applicants and purchase F_L also. The second best solution – the first best solution under the incentive constraint that the insurer cannot distinguish between high and low risk applicants – 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

[39] We chose these probabilities using the same justification as in our calculation of welfare gains above, where the probabilities of loss range from a low of 0.005 to a high of 0.06.

themselves as high risk firms. The second best solution is thus characterized by the insurer offering two types of contract: high premium, high coverage contract F_H, which the high risk firms will purchase, and a low premium, low coverage contract P, which the low risk firms will purchase (Rothschild and Stiglitz 1976).

The welfare lost due to the adverse selection problem can be computed as the amount $A - A'$ in Figure 4. As an example, we can calculate the welfare lost for the DoS attack case under risk aversion $\sigma = 2$, as follows.

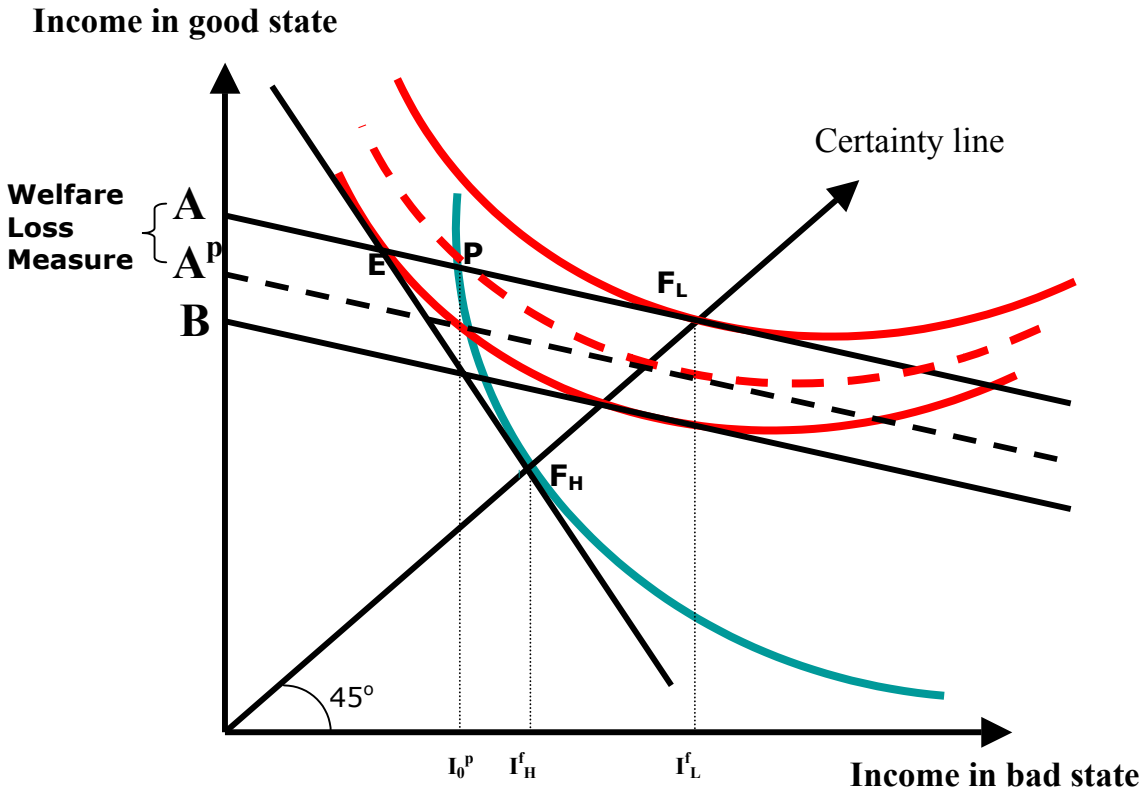

Figure 4: Measuring Social Welfare Loss from Adverse Selection

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

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

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

$EU_L^p = p_L \cdot \frac{I_0^{p\ (1-2)}}{1-2} + (1-p_L) \cdot \frac{I_1^{p\ (1-2)}}{1-2} = -0.31887 \Rightarrow I_L^p = \$3.136$ billion.

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

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

Thus, the thorough risk assessments required by cyberinsurers – although somewhat onerous to the applicants – are actually designed to check this adverse selection problem. This thus benefits the low risk firms, and results in welfare gains to them, which can be calculated as abovementioned.

V. SUMMARY AND CONCLUSIONS

In this study, we conducted a case study of the cyberinsurance industry. We examined the developing cyberliability legislation and the emerging cyberinsurance market, including potential adverse selection, moral hazard, and other problems to the market solution. We discovered that insurance companies are dealing with the issues besetting the fledging cyberinsurance industry. For instance, they are coping with adverse selection and moral hazard problems but rigorously classifying the risk level of the insured, and stipulating provisions on the care expected of the insured. We also calculated social welfare gains that could be achieved with the full development of the cyberinsurance industry, and the social welfare loss that could result from obstacles to the market solution, such as asymmetric information.

We conclude that cyberinsurers are able to find ways to deal with several problems that could result in the failure of market solution. Although there may still be issues that need to be threshed out before the full market solution can be achieved, we suggest that the direction to be taken should be towards resolving these issues, rather than give up on the market solution. When these obstacles to the full market solution are fully worked out, several positive results can occur. First, cyberinsurance would result in higher security investment, increasing the level of safety for information technology (IT) infrastructure. Second, cyberinsurance can facilitate standards for best practices as cyberinsurers seek benchmark security levels for risk management decision-making. Third, the creation of an IT security insurance market will result in higher overall societal welfare.

APPENDIX:
Table on Salient Provisions of Cyberinsurance Policies

	Net Advantage Security	e-Comprehensive	Webnet Protection
COVERAGES			
First Party Coverages			
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. *Proviso that information and computer program be subject to regular network back-up procedures.* 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 knowledge regarding the existence of the Extortion coverage afforded by this Policy is restricted as far as possible."	Y
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 Restablish the reputation of the insured (including public relation expenses)	Y. Public relations expenses
Third Party Liability Coverages[40]			

[40] 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.

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 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.	Y	Y
Defense Costs	Y	Y. Insurer has right and duty to defend. Limit: up to payment of "all reasonable and necessary legal costs".	Y
EXCLUSIONS			

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 configuration problems.	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".
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	"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…"

		may be stored"	
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; 3rd party both patents and trade secrets excluded		1st 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
(1st and 3rd party: failure of any computer or software to correctly assign any date)		Y	
OTHER RELEVANT PROVISIONS			
Retentions	Retention same as in liability limits below + retention waiting hours for business interruption and	There is only single loss retentions ("arising out of any single event or series of related event"). Any recovery (net of expenses) of	Waiting period specified for business interruption. Each loss deductible, and each claim

	internet extra expense coverages.	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.	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) 1st party (b) 3rd 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 1st and 3rd party losses). Separate limits for each coverage parts (3 3rd party coverages, and 6 1st 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 1st party loss		Covered as 1st 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	Y. At option of insurer: as part of underwriting, in deciding whether to

		by insurers.	continue/modify coverage, or processing of loss/claim.
Insurer liable only for transcription or replacement cost	Definition of "Loss" ("actual and necessary costs incurred by the insured for replacing, reproducing, recreating, or restoring the insured's information assets".	1st Party loss of info, etc.: insurer shall be 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.	1st party insurance is for "restoration costs" (i.e., "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.

REFERENCES

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

Banham, Russ, *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).

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

Bernhofen, Daniel M. and John C. Brown, *Estimating The Comparative Advantage Gains from Trade: Evidence from Japan,* WORKING PAPER (2003).

Bohme, Rainer, *Cyberinsurance Revisited,* Conference Papers in Proceedings of the Workshop on the Economics of Information Security (2005), *available at* http://infosecon.net/workshop/pdf/15.pdf.

Brown, Brian D., *Emerging Insurance Products in the Electronic Age*, 31-FALL BRIEF 28 (2001).

Brush, Colleen, *Surcharge for Insecurity*, *at* http://www.esmartcorp.com/Hacker%20Articles/ar_surcharge_for_insecurity.htm (1991) (last visited April 23, 2004).

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

COOTER, ROBERT AND THOMAS ULEN, LAW AND ECONOMICS, 320-337 (4TH ED. 2004).

Crane, Matthew, *International Liability in Cyberspace*, 23 DUKE L. & TECH. REV. 1 (2001).

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

Duffy, Daintry, *Prepare for the Worst*, DARWIN MAG. (Dec. 2000), *available* at http://www.darwinmag.com/read/120100/worst.html (last visited April 24, 2004).

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

FEENSTRA, ADVANCED INTERNATIONAL TRADE (forthcoming).

Fisher, Susan E., *Seeking Full Protection for Net Asset,* INFOWORLD (Oct. 5, 2001), *available at* http://webbytes.com/portfolio/text/iw100501.html (last visited April 23, 2004).

Gohring, Nancy, *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).

Gralla, Preston, *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).

Grinols, Earl L., *A Thorn in the Lion's Paw: Has Britain Paid Too Much for Common Market Membership?*, 16 J. OF INT'L ECON. 271 (1984).

Grinols, Earl L and Kar-Yiu Wong, *An Exact Measure of Welfare Change,* 24 No. 2 CAN. J. OF ECON. 428 (1991).

Heal, Geoffrey and Howard Kunreuther, *You Only Die Once: Managing Discrete Interdependent Risks*, *available* at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=419240 (June 2003).

Insurance Information Institute, *Computer Security-Related Insurance Issues* (September 2003), *at* http://www.iii.org/media/hottopics/insurance/computer (last visited April 14, 2004).

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; 45 for health care sector: 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

Irwin, Douglas A., *The Welfare Costs of Autarky: Evidence from the Jeffersonian Trade Embargo, 1807-1809,* DARTMOUTH COLLEGE, MIMEO (2002).

Kehne, Jeffrey, *Note, Encouraging Safety Through Insurance-Based Incentives: Financial Responsibility for Hazardous Waste*, 96 YALE L.J. 43 (1986).

Kenneally, Erin, *The Byte Stops Here: Duty and Liability for Negligent Internet Security*, 16 COMPUTER SECURITY JOURNAL NO. 2, 2000, available at http://www.gocsi.com/pdfs/byte.pdf.

Kesan, Jay P. and Ruperto P. Majuca, *Cybercrimes and Cyber-Attacks: Technological, Economic, and Law-Based Solutions*, in PAULINE C. REICH, ED., ENCYCLOPEDIA ON CYBERCRIMES (forthcoming 2005).

Kesan, Jay P. Ruperto P. Majuca and William Yurcik, *The Economic Case for Cyberinsurance*, Conference Papers in Proceedings of the Securing Privacy in the Internet Age Symposium (2004).

Kiefer, Kimberly and Randy V. Sabett*, Openness of Internet Creates Potential for Corporate Information Security Liability*, 1 BNA PRIVACY & SECURITY LAW REPORT 788 (June 24, 2002).

Kneuper, Robert and Bruce Yandle, *Auto Insurers and the Air Bag*, 61 J. RISK & INS. 107 (1994), *available at* 1994 WL 13386236.

Knight, Will, *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).

Lee, Anna, *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).
Mader, Becca, *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).
McDonald, Tim, *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).
Mullin, Eileen, *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).
National Strategy to Secure Cyberspace*, available* at www.whitehouse.gov/pcipb.
Noll, *The Economics and Politics of Regulation*, 57 VA. L. REV. 1016, 1028-32 (1971); P. QUIRK, INDUSTRY INFLUENCE IN FEDERAL REGULATORY AGENCIES (1981).
Ogut, Hulisi, Nirup Menon, and Srinivasan Raghunathan, *Cyber Insurance and IT Security Investment: Impact of Interdependent Risk,* Conference Papers in Proceedings of the Workshop on the Economics of Information Security (2005), *available at* http://infosecon.net/workshop/pdf/56.pdf.
Ortzag, Peter R. and Joseph Stiglitz, *Optimal Fire Departments: Evaluating Public Policy in the Face of Externalities,* Working Paper 2002, *available at* http://www.brookings.org/views/papers/orszag/20020104.pdf
Pratt, John W., *Risk Aversion in the Small and in the Large,* 32 ECONOMETRICA 122 (1964).
Radin, Margaret Jane, *Distributed Denial of Service Attacks: Who Pays?*, *available at* http://www.mazunetworks.com/white_papers/radin-print.html (2001).
Raul, Alan Charles, Frank R. Volpe and Gabriel S. Meyer, *Liability for Computer Glitches and Online Security Lapses,* BNA Electronic Commerce Law Report, Vol. 6, No. 31 at 849 (August 8, 2001).
Rothschild, Michael and Joseph Stiglitz, *Equilibrium in Competitive Insurance Markets: An Essay on the Economics of Imperfect Information*, 90 QUARTERLY J. OF ECON. 629 (1976).Savage, Marcia, *Tripwire, Lloyd's Partner for Cyberinsurance* (Sept. 11, 2000), *available* at http://www.techweb.com/wire/story/TWB20000911S0008 (last visited Apr. 22, 2004).
Schneier, Bruce*, Computer Security: It's the Economics, Stupid,* Conference Papers in Proceedings of the 1st Annual Workshop on Economics of Information Security *(2002), available at* http://www.cl.cam.ac.uk/users/rja14/econws/18.doc.
Shapiro*,* Carl. *Symposium on the Economics of Liability*, 5 J. OF ECON PERSPECTIVES 3, 5 (1991).
Shavell, Steven, *On Moral Hazard and Insurance*, 93 QUARTERLY J. OF ECON. 541 (1979).
Shavell, Steven, *On Liability and Insurance*, 13 BELL J. OF ECON. 120 (1982).
SHAVELL, STEVEN, ECONOMIC ANALYSIS OF ACCIDENT LAW (1987).

SIMON, CARL P. AND LAWRENCE BLUME, MATHEMATICS FOR ECONOMISTS (N.Y.: W.W. Norton and Company) (1994).
Smedinghoff, Thomas J., *Defining the Legal Standard for Information Security*, *in* SECURING PRIVACY IN THE INTERNET AGE (forthcoming 2005, Stanford University Press).
Solove, Daniel J., *The New Vulnerability: Data Security and Personal Information*, *in* SECURING PRIVACY IN THE INTERNET AGE (forthcoming 2005, Stanford University Press).
Tiebout, Charles M, *A Pure Theory of Local Expenditures,* 64 J. POL. ECON. 416 (1956).
Varian, Hal R., *Managing Online Security Risks,* THE NEW YORK TIMES (June 1, 2000), available at http://www.nytimes.com/library/financial/columns/060100econ-scene.html.
VARIAN, HAL R., MICROECONOMIC ANALYSIS (3D ED. 1992).
Vogel, Timothy A., *Dealing With Cyber Attacks on Network Security*, 48 PRAC. LAW 35, 36 (Apr. 2002).
Viscusi, Kip, *Product and Occupational Liability*, 5 J. OF ECON. PERSPECTIVES 71 (1991).
Walsh, Lawrence M., *On the Cutting Edge* (April 2001), *available at* http://infosecuritymag.techtarget.com/articles/april01/departments_news.shtml (last visited April 23, 2004).
Wiles, Russ, *Cybercrime Insurance Growing*, ARIZ. REP. (Sept. 15, 2003), *available at* http://www.azcentral.com/arizonarepublic/business/articles/0915insure15.html (last visited April 23, 2004).
World Bank Group, *Data and Statistics: World Development Indicators 2004, available at* http://www.worldbank.org/data/wdi2004/index.htm)
Yurcik, William and David Doss, *CyberInsurance: A Market Solution to the Internet Security Market Failure,* Conference Papers in Proceedings of the 1st Annual Workshop on Economics of Information Security *(2002), available at* http://www.sims.berkeley.edu/resources/affiliates/workshops/econsecurity/econws/53.pdf