

Rewarding IT Security in the Marketplace¹

Walter S. Baer
RAND

1. Introduction

Keeping networked information systems and the information technology (IT) infrastructure secure requires coordinated as well as individual action. As a 2002 National Research Council report points out, “The overall security of a system is only as strong as its weakest link.”² The security of my IT system depends not just on the firewalls and authentication measures I have installed, but on how well other computers and networks linked to me are protected. Such linkages present a textbook example of a network externality, in which an individual’s or firm’s action has uncompensated economic consequences for others connected to the network.³ IT security thus must deal with the market failures that often result from such externalities; that is, private stakeholders alone are highly unlikely to invest sufficiently in IT network security to provide an optimal (or even adequate) level of societal protection.

This paper focuses on ways to better align private incentives with the overall public interest in IT security. While it is written from a United States perspective and refers primarily to U.S. institutions and processes, the issues and approaches discussed should be generally applicable internationally. In fact, they must be considered in an international context; since attacks on IT systems often cross national borders, and effective defenses involve a wide range of national and transnational entities.

Nearly everyone agrees that improving IT security demands greater efforts from both the public and private sectors, as well as better coordination and cooperation between them. Within the U.S. federal government, most of the Offices, Centers, Boards, and Councils created to oversee and coordinate federal activities have been brought together into the National Cyber Security Division (NCSD) in the Directorate of Information Analysis and Infrastructure Protection (IAIP) of the new Department of Homeland Security (DHS). Among other agencies, the NCSD includes the Critical Infrastructure Assurance Office (CAIO) and the National Infrastructure Protection Center (NIPC), which were established in 1998 with responsibilities to develop a national strategy for, and promote government/industry collaboration on IT security.⁴

As prominent examples of such collaboration, a series of industry-specific Information Sharing and Analysis Centers (ISACs) have been created since 1998 to develop “secure database[s], analytic tools, and information gathering and distribution facilities designed to allow authorized participants to submit either anonymous or attributed reports about information security threats, vulnerabilities, incidents and solutions.”⁵ The ISACs collect and analyze such reports, compare them with baseline data, and provide early notification to their members about security threats and possible responses. Membership is voluntary, and membership criteria differ: the financial services ISAC accepts only industry members, while the ISACs for telecommunications and information technology include both industry and government participants.

It seems too early to judge the ISACs’ effectiveness in improving IT security, although the financial services ISAC has been credited with helping its members avoid the widespread denial of service attacks launched in February 2000.⁶ U.S. industry sectors as diverse as surface transportation, food, and water supply have established ISACs in the past two years, and the concept has spread to Canada, Japan and other OECD countries.

However, many U.S. firms worry about the potential downsides from joining ISACs, including increased antitrust scrutiny from sharing security data with competitors, legal liabilities arising from leaks about information security breaches or vulnerabilities, or the public release under the Freedom of Information Act of sensitive information shared with the federal government. Such concerns may well limit the ISACs' growth and effectiveness, at least in the short-run.⁷

Beyond encouraging public/private collaboration, another key pillar of the U.S. national effort is to strengthen the incentives for private sector (and other non-government) organizations to improve their own IT security. Bruce Schneier, a leading expert on IT security, states the point clearly: "good security [should be] rewarded in the marketplace."⁸ The remainder of this paper discusses how such incentives can be put in place so that markets will reward investments in IT security. The next section considers how well known principles of risk management and private insurance can be applied to IT security problems. Section 3 describes how the insurance industry is responding to the market opportunities presented by IT security, while Section 4 focuses on problems that currently limit the scope and effectiveness of private insurance covering these risks. Section 5 outlines potential rationales and roles for government involvement to help private insurance markets function better to provide incentives for IT security. Findings and prospective conclusions are outlined in the final section.

2. Applying Risk Management Principles and Practices to IT Security

In a perceptive speech to the Digital Commerce Society of Boston in November 1998, Daniel Geer called for a change in IT security thinking from trust management to risk management.⁹ Traditionally, IT security designers have thought in terms of building trusted

systems for trusted users.¹⁰ IT security thus has emphasized trust management technologies -- e.g., smart cards with encrypted passwords, public key infrastructure, and increasingly sophisticated biometric devices – for identifying and authenticating trusted users, as well as firewalls, intrusion detectors and other technologies for protecting systems against malicious code and malign users. But since no systems are or will be 100 percent secure, the problem with trust management approaches is that when they fail, the losses may be open-ended, or at least unestimated.

In contrast, risk management focuses on identifying and quantifying potential losses and the uncertainties surrounding them.¹¹ Quantitatively estimating IT security risks permits enterprise managers to decide how much to invest in measures, like the technologies mentioned above, to mitigate them and/or whether to package them in forms that others will assume (for a price). The latter depends, of course, on well-functioning markets for insurance covering the risks that the enterprise wants to lay off. Such insurance is available to cover most normal business risks from property loss or damage, business interruption, and liability for harm or damage caused to others. Applying risk management principles to IT could bring IT security within the more familiar and workable paradigms of insurance, risk sharing and risk securitization – realms in which U.S. financial service firms excel and actively seek new business opportunities. That is why Daniel Geer titled his talk on IT security: “Risk Management is Where the Money Is.”

As a risk management tool, insurance can encourage greater protective measures and help achieve other social goals. Fire insurance is often cited as a case in point. A building owner must have fire insurance to obtain a mortgage or a commercial business license. Obtaining insurance requires that the building meet local fire codes and underwriting standards, which may involve visits from local government and insurance company inspectors. Inspectors also follow up on serious incidents and claims, both to learn what went wrong and to guard

against possible moral hazards of insurance such as arson or fraud. Insurance companies often sponsor research, offer training classes and publish materials on fire prevention and mitigation. Most important, insurers reduce premiums to building owners who keep their facilities clean, install sprinklers, test their control systems regularly and take other protective measures. Fire insurance markets thus involve not only underwriters, agents and clients, but also code-writers, inspectors, and vendors of products and services for fire prevention and protection. While government remains involved, well-functioning markets for fire insurance keep the responsibility for and cost of preventive and protective measures largely within the private sector.

The fire insurance analogy seems to have considerable applicability and appeal to IT security problems. Workable markets for insurance covering IT risks could, in principle, have a number of desirable incentives and outcomes, including:

- Processes to set IT security standards for underwriting;
- Security consulting firms that audit and monitor clients' IT security practices as an integral component of insurance underwriting;
- Institutions that test and certify IT security products and services;
- Incentives and means to promulgate industry best practices;
- Incentives for firms to increase IT security to reduce insurance premiums;
- Incentives to keep responsibility for and cost of protection within the private sector.

Bruce Schneier, the founder and CTO of Counterpane Internet Security, agrees: "Sooner or later, the insurance industry will sell everyone antihacking policies. It will be unthinkable not to have one. And then we'll start seeing good security rewarded in the marketplace."¹² However, as discussed in the next two sections, we are still a long way from obtaining such positive results from private markets for insurance covering IT security risks, commonly known as "cyber insurance."

3. Current Status of and Trends in Cyber Insurance

As recently as 1998, there was very little commercial demand for insurance covering damage, loss or liability from hackers or other IT network failures. However, growing national concerns about U.S. vulnerability to information attacks, coupled with well publicized distributed denial of service (DDOS) attacks that brought down many commercial Websites in early 2000, has brought greater appreciation of the risks, which has led many firms to request insurance against such perils. The insurance industry is responding – albeit slowly.

Insurance underwriters and brokers – including industry giants such as AIG, Chubb, Lloyds of London, Marsh & McLennan, St. Paul and Zurich Financial Services, as well as more specialized firms such as Wurzler Underwriting Managers and INSUREtrust – now offer policies that explicitly cover some IT security risks. For an additional premium, for example, “commercial crime bonds” will cover loss of funds from cyber crimes as well as ordinary fraud, embezzlement or extortion (but not losses from business interruptions due to cyber crimes). State banking regulators generally require banks and other financial institutions under their jurisdiction to carry such coverage.

For businesses that sell goods and services online, insurers offer several kinds of e-business coverage of liabilities due to technology errors or omissions, intellectual property violations, privacy infringement, theft of customer credit cards or viruses transmitted to and from the insured’s Websites. Other “breach of security” losses from hacker attacks may also be covered. Premiums typically are 1 to 5 percent per year of the policy limit, depending on the specific coverage. According to the Insurance Information Institute, the market for e-business liability insurance will grow from about \$75 million in 2001 to \$2.5 billion by

2005.¹³ Still, even the \$2.5 billion figure in 2005 would represent less than 2 percent of total property/casualty premiums.

Business losses due to direct physical loss or damage to computers and other IT hardware are generally covered under standard business property insurance. An Arizona federal district court decision in 2000 broadened that coverage to include computer loss of use and functionality under “direct physical loss or damage.”¹⁴ In this case, an electrical power outage shut down computer systems at an Ingram Micro, Inc. data center in Tucson, AZ. Although the systems were not physically damaged, the company could not conduct business for some eight hours while the computers were manually reprogrammed. The insurer’s denial of Ingram’s claim of loss was rejected by the Arizona district court, stating:

“At a time when computer technology dominates our professional as well as personal lives, the Court must side with Ingram’s broader definition of “physical damage.” The Court finds that “physical damage” is not restricted to the physical destruction or harm of computer circuitry, but includes loss of access, loss of use and loss of functionality.”¹⁵

In another case recently decided by the U.S. Fourth Circuit Court of Appeals, an employee of NMS Services, Inc., a software development company, wrote “back door” programs that allowed him to gain access to the company’s computer systems, which he used after he was fired to erase company files and databases. The court found that the company’s losses were covered under its general liability insurance policy, even though the policy excluded losses due to employee dishonesty.¹⁶ Both the *Ingram* and *NMS* decisions remain highly controversial within the insurance industry. Some believe they could be used to claim any loss from hacker attacks and other breaches of computer security under standard property coverage. As a consequence, *Ingram* and *NMS* may accelerate insurers’ efforts to write separate coverage for IT security breaches and explicitly exclude them from standard policies.¹⁷

To qualify for specific insurance covering losses from breach of security, businesses may have to pass an IT security audit and risk assessment. Insurers typically have arrangements with third party IT security firms to conduct such assessments,¹⁸ although INSUREtrust and a few others operate their own risk management services groups. AIG has been particularly aggressive in offering free security assessments to prospective clients.¹⁹ And while initial audits clearly are essential to maintain underwriting standards, security experts emphasize the importance of routine, continuing monitoring of clients' IT systems and security processes. Such arrangements for regular security assessments as part of insurance renewals do not yet appear to be in place.

Overall, despite growing recognition of IT security vulnerabilities, and increased business interest in insuring against IT security risks, actual insurance coverage remains spotty and limited. The latest "Benchmark Survey" published by the U.S. Risk and Insurance Management Society reports that while nearly 70 percent of business respondents are engaged in electronic commerce, "only 2 percent indicated that their organization carries a separate e-business insurance policy."²⁰ Present-day policies have relatively low coverage limits, high premiums and numerous exclusions that make them problematic to many potential customers and thus reduce their effectiveness as incentives for better IT security practices. The next section outlines the reasons why this remains the situation today.

4. Barriers to Cyber Insurance Expansion

Since the concept of insurance against IT security risks is quite new, it is perhaps not surprising that current markets for such coverage are still undeveloped and limited. Cyber insurance faces a number of relatively serious, interrelated problems, including:

- **Lack of agreement on basic policy definitions and language.** Rapid and constant changes in information technology can bring ambiguity or misunderstanding about precisely what is insured, what perils and risks are covered, and how losses are to be assessed. The *Ingram* case points to such problems in interpreting what is meant by “physical damage” to computer systems. As another example, insurance law generally holds that coverage applies to risks that are “fortuitous;” that is, unforeseeable and subject to chance, like an accidental fire or an electrical outage. However, an insured must take active protective steps against foreseeable, “non-fortuitous” risks in order for coverage to apply. Are hacker attacks fortuitous or non-fortuitous? Neither policy language nor case law makes this clear. Similar ambiguities surround whether coverage applies everywhere in cyberspace (on hosted servers, mirrored sites, etc.), and how information stored on IT systems should be valued for insurance purposes.

Because case law involving IT security is uncertain and changing, insurers seek to limit their exposure by narrowly defining coverage on new cyber policies and excluding coverage on other contracts. As of now, no standard policy language has been agreed on that would encourage more rapid market expansion.

- **Lack of underwriting standards or experience.** Insurers have little experience with IT security claims on which to base premiums, both because the field is so new, and because firms have resisted revealing losses from security breaches. Similar to the policy definition problem, setting standards for policy underwriting is difficult in a rapidly changing environment. And clients’ fears of damaging publicity or liability if their IT vulnerabilities are revealed make them loath to file claims. According to a *Fortune* article

in July 2000, “Not one of the ... big insurers said it has ever actually paid a claim on e-policy.”²¹

Client reluctance to file claims works to the insurers’ advantage, of course, at least in the short run. On the other hand, limited actuarial experience makes underwriters wary of substantial exposure, especially post-September 11. A recent article in Information Security Magazine on “2002 Industry Trends: Cyberinsurance,” states:

“In the past, companies seeking a \$25 million policy could find someone to cover them. Now it’s much more difficult. Underwriters who didn’t blink at \$5 million or \$10 million policies would rather insure \$1 million policies, say cyberinsurance underwriters.”²²

- **Lack of adequate reinsurance.** Insurers’ concerns about their inability to judge the level of future exposure is compounded by the lack of a strong reinsurance market to lay off IT security risks. In other fields of property/casualty insurance, underwriters commonly purchase reinsurance to protect themselves against unusual, extreme losses. But the paucity of claims experience for IT security worries the reinsurance industry as well the initial underwriters. Prospective reinsurers are particularly concerned about the possibility of coordinated, “structured” information attacks by organized criminals, terrorists or state-supported hackers, which could result in far greater losses than have occurred to date.

Catastrophe bonds (“cat bonds”) are a recent innovation in reinsurance that could be applicable to IT security risks. Beginning in the mid 1990s, reinsurers have securitized excess risks from low frequency, high impact events such as hurricanes and earthquakes, by selling bonds to investors that can be traded on securities markets.²³ A typical cat bond yields considerably more than alternative investments in good years, but the investor stands to lose interest payments and sometimes principal if insurance losses exceed a specified amount. Cat bonds essentially follow the path already developed for packaging mortgage loans, auto payments and credit card debts into tradable financial instruments. Although their income streams are less predictable than are those for conventional securities, they can be attractive to investors as a distinct asset class for portfolio diversification. Cat bonds represent a growing part of the reinsurance market, but they have not yet been used to reinsure cyber policies. And

absent traditional reinsurance or issuance of cat bonds, underwriters will continue to limit their commitments to cover IT security risks.²⁴

- **Policy exclusions.** Like other property/casualty policies, those covering breaches of IT security typically exclude claims resulting from acts of war, riot, civil commotion and similar disasters known as *force majeure*. Yet these may be precisely the risks that businesses fear most and want to insure against. Moreover, unlike the case with most other property losses, it may be difficult to distinguish coordinated information attacks by terrorists or state-supported agents, which might be excluded under *force majeure*, from fortuitous events that would be covered. Such unresolved questions inject additional uncertainty into coverage of IT security risks that vex insurance underwriters and reinsurers, as well as prospective clients.
- **No strong collaborative processes or institutions for information sharing.** One approach to increasing the base of experience regarding IT security risks would be for insurers and other knowledgeable stakeholders to share more data about breach of security incidents, claims and losses. There is relatively little sharing of such information today within the insurance industry, primarily for competitive reasons (IT security consultants, too, consider their databases to be highly proprietary and are reluctant to share them). Insurers also express concerns about possible antitrust violations if they exchange information with competitors.

In terms of collaborative institutions, no ISAC has been established solely for the insurance industry, although the financial services ISAC includes AIG, Chubb and other large financial firms that have insurance subsidiaries. The Financial Services Roundtable, a consortium whose members represent large, integrated U.S. financial services companies, has established a Working Group on “Insurance in E-Commerce Risk

Management” as part of its BITS Technology Group,²⁵ but what recommendations this Working Group may make about ongoing collaborative activities remain to be seen.

In 1999, The Financial Services Roundtable launched the BITS Financial Services Security Lab to test and certify hardware and software for online banking and related financial services.²⁶ This consortium-run Lab is modeled on the highly successful Underwriters Laboratories, Inc., which tests and certifies electric and electronic equipment for fire protection and related safety features, but it faces an uphill struggle to stay abreast of IT technology.²⁷ In its first three years, the BITS Security Lab has certified only one product, a secure Web transaction server (called the “Virtualvault”) produced by Hewlett Packard.²⁸ ICSA Labs, a division of TrueSecure Corporation (publisher of *Information Security Magazine*), certifies firewalls and other Internet security products and is trying to position itself as an industry-wide leader in developing IT security standards. However, ICSA Labs appears to function today more as a commercial consultant than as an independent standards organization. Finally, Congress recently appropriated \$3 million to establish an Institute for Information Infrastructure Protection (“I3P”) at Dartmouth University, whose mission is to develop an R&D agenda for IT security, support security product and service evaluations, facilitate public/private information sharing, and expand the education and training of IT security experts.²⁹ While not yet operational or focused specifically on insurance-related issues, a successful I3P could help support collaborative efforts by insurers in all the above areas.

- **Possible moral hazards.** Insurance has always had to deal with cases of fraud, as well as problems that, once insured, policyholders may be less careful than they would be otherwise. For example, IT insurance covering extortion might encourage an employer to pay off a fired information systems employee who threatened to corrupt the firm’s databases. As a second example, an insured might claim large damages from

database corruption resulting from an unknown hacker's breach of IT security. The insurer might then respond that the covered loss is much less, since the insured should have had backup records the hacker could not reach. The insurer's argument would be that the hacking event was fortuitous but the resulting data corruption was non-fortuitous, requiring the insured to take active protective measures.³⁰

Insurers have dealt successfully with moral hazards in other areas through mandating protective measures and procedures designed to reduce losses. Mandating that covered structures pass local fire codes is an obvious example. As another illustration, "special crime" policies covering kidnapping and ransom demands may require the insured to report an event immediately and use designated crisis management specialists. Again because of rapid technology changes, however, such standard codes and practices are much more difficult to develop and implement for IT security.

- **Inadequate accountability for IT security flaws and vulnerabilities.** A growing number of experts believe that uncertain liability and inadequate accountability for security flaws exacerbate network externalities and thus represent core obstacles to improving IT security.³¹ U.S. case law has not yet clarified who bears responsibility for losses when a breach of IT network security occurs upstream from the damaged party; e.g., when a hacker exploits a security weakness at site A to launch an attack over backbone network B through Internet service provider C which results in damages to company D's information stored on a server maintained by company E. To what extent are A, B, C or E liable for D's damages? If no such liability exists, then the parties will not invest in IT security beyond their own direct needs nor purchase third-party insurance with attendant incentives to improve security. This is the basic externality issue which leads to a familiar "tragedy of the commons" result.

Perhaps even more important, software suppliers are generally not subject to product liability laws and regulations, unlike the situation for other manufacturers. This is because software suppliers sell licenses to use their products rather than ownership of them. Opening a shrink-wrapped package or clicking on a Website's "I accept" button exempts the software vendor from liability if hackers subsequently exploit the program's flaws or vulnerabilities to cause damage. The lack of product liability for software providers is not an insurance problem per se; but it exacerbates the negative externalities associated with IT security and makes it more difficult to use insurance to address these externalities.

5. Potential Government Roles to Strengthen Cyber Insurance Markets

Given the obstacles described above, are there constructive ways for government to help spur or strengthen private markets for cyber insurance to encourage greater private investment in IT security? Although government intervention inevitably affects market dynamics and results in costs as well as benefits, potential government roles in cyber insurance could include:

- Setting IT security standards;
- Mandating incident reporting or other information sharing;
- Mandating cyber insurance or financial responsibility;
- Facilitating reinsurance by limiting and/or indemnifying catastrophic losses;
- Providing insurance directly;
- Legislating liability.

These are discussed briefly in turn.

Setting IT security standards. Returning to the fire insurance analogy, local governments routinely pass ordinances detailing fire codes that then generally serve as

minimum standards for insurance underwriting. Could similar government-set minimum standards for IT security facilitate underwriting of cyber insurance? One federal precedent would be “airworthiness certification” of aircraft and other aviation equipment by the Federal Aviation Administration (FAA). Insurance companies require such certification before planes can be insured.

Although minimum IT security standards could aid in insurance underwriting, government-mandated standards seem difficult to achieve and likely to be counterproductive. Government-directed standards processes tend to be slow and process driven, and consequently poorly matched to the frenzied pace of information technology. Government support for non-government standards, analogous to supporting the development of Internet technical standards through the Internet Engineering Task Force (IETF), would seem a better approach. However, the federal government may be able to play useful roles in standards development through such actions as:

- Serving as a neutral forum to bring stakeholders together;
- Requiring security testing and certification, developed in cooperation with industry, for government procurement of IT equipment, systems and services;
- Providing some financial support for standards development.

As one such effort in the spring of 2002, the National Security Agency and the Commerce Department ‘s National Institute of Standards and Technology joined with the nonprofit Center for Internet Security to draft a set of security standards for computers running Microsoft’s Windows 2000.³²

Mandating incident reporting or other information sharing. Although the financial services ISAC includes some insurers, it has not focused on or encouraged information sharing for insurance underwriting purposes. A separate ISAC for the insurance industry

seems unlikely to broaden the underwriting experience base substantially unless reporting of threats, incidents and losses were made mandatory rather than voluntary.

Civil aviation offers such a model: the FAA requires air carriers and airports to report aviation accidents and serious incidents, as specified in FAA and National Transportation Safety Board (NTSB) regulations. For example, hard landings that result in “substantial damage” must be reported to the FAA and NTSB³³; records of other hard landings need not be reported but are used by the air carriers themselves for maintenance, pilot training and general quality assurance. In addition, a separate, voluntary call-in system (funded by NASA, not the FAA) encourages anonymous reporting of aviation problems and incidents.

Financial service firms and other businesses would strenuously oppose mandatory reporting of IT incidents. Consequently, mandatory reporting seems a political non-starter, unless Congress passes legislation giving the federal government prime responsibility for IT security, as it has done for aviation safety.³⁴ As a more modest step, since insurance industry representatives often cite antitrust concerns as a barrier to information sharing, Congress could consider exempting sharing of IT security information from antitrust enforcement, similar to what the *Critical Information Infrastructure Security Act of 2001* proposes.

Mandating insurance or financial responsibility. Government insurance mandates are quite common. Governments at all levels demand that contractors carry specified liability coverage as a condition for receiving contract awards. Many states now require vehicle owners to document insurance coverage or equivalent proof of financial responsibility before their vehicles can be licensed. State regulated banks must carry “bankers bonds” covering losses from fraud and embezzlement. And as discussed further below, Congress

has legislated that private owners of nuclear power plants and space launch operations carry primary liability insurance up to a specified limit.

Extending liability insurance mandates to cover breaches of IT security would seem most readily justified for firms doing business with government. Implementing such mandates, however, would require clarification of, and agreement on, the difficult issues surrounding who bears liability for security breaches on parts of the IT network not under the contractor's direct control.

Facilitating reinsurance by limiting and/or indemnifying catastrophic losses. For nuclear power plants and space launches, the federal government has intervened to cap private liabilities and mandate financial responsibility up to that stipulated limit. The Price Anderson Act of 1957 limits the liability of nuclear power plant owners to \$560 million for any single event. The Act (as amended) requires each nuclear plant to carry \$200 million of primary insurance; secondary coverage for liabilities between \$200 and \$560 million comes from premiums assessed retroactively and shared by all U.S. nuclear power plant owners. If damages exceed \$560 million, Congress must determine whether and how compensation will be paid. The Commercial Space Launch Act of 1984, as amended, mandates that commercial operators must obtain \$500 million of primary liability insurance before receiving a license to launch a space vehicle. The Act also provides that Congress may appropriate up to \$1.5 billion to cover additional liabilities from the launch. Although the federal government essentially serves as the insurer of last resort, it has never been called on to cover excess liabilities for either nuclear power plants or space launches.

When IRA terrorist attacks in the early 1990s on commercial buildings in London threatened to make property insurance unavailable to building owners, the U.K. government worked with British insurers to maintain property damage and business interruption insurance

coverage. Pool Re was established by Parliament in 1993 as a mutual reinsurance company owned by the insurers and backed by the U.K. Treasury as reinsurer of last resort.³⁵ Pool Re has succeeded in stabilizing U.K. property insurance markets over nearly ten years without requiring further government assistance.

Pool Re also served to inform discussion in the U.S. about how to maintain property and casualty insurance protection against terrorism risks after the attacks of September 11, 2001, which prompted many insurance carriers to exclude or severely restrict coverage for acts of terrorism. The result is the Terrorism Risk Insurance Act of 2002, signed into law by President Bush on November 26, 2002. The Act requires property and casualty insurers to provide coverage of losses due to acts of terrorism, while providing a three-year government reinsurance backstop for such claims. After the industry has paid out \$10 billion in the first year (increasing to \$12.5 billion the second year and \$15 billion the third year), the federal government will pay 90 percent of remaining claims up to a ceiling of \$100 billion. The three-year limit is intended to “allow for a transitional period for the private markets to stabilize, resume pricing of such insurance, and build capacity to absorb any future losses....”³⁶ While the Terrorism Risk Insurance Act will apply principally to workers’ compensation and property insurance claims, it should also be examined as a model for coverage of IT security risks, since the lack of adequate reinsurance appears a major obstacle to cyber insurance expansion.

Providing insurance directly. In a few cases where losses have become too great for private insurers and reinsurers to handle - notably floods and earthquakes - government has stepped in directly to provide property damage insurance.³⁷ Since 1968, the National Flood Insurance Program³⁸ has offered insurance for homes and commercial buildings in flood-prone areas, where coverage would otherwise be unavailable. Administered by the Federal Emergency Management Agency, federal flood insurance is mandatory in flood

hazard areas for recipients of government-guaranteed mortgages or other construction assistance, and is linked to floodplain management measures.

Similarly, the California State Legislature established the California Earthquake Authority³⁹ in 1996 to write homeowners' policies when private insurers began pulling out of the state market after suffering heavy losses in the 1994 Northridge earthquake. Insurance companies have not as yet incurred large losses from IT breach of security claims, however, and there seems little interest in or incentive for federal or state governments to provide cyber insurance at this time.

Legislating liability. Given the diffuse and limited accountability for IT security vulnerabilities, as well as the uncertainties surrounding existing case law on liability, Congress or state legislatures could clarify who bears what responsibility for losses due to security breaches. The most recent National Research Council report on cyber security recommends that:

“Policy makers should ...[c]onsider legislative responses to the failure of existing incentives to cause the market to respond adequately to the security challenge. Possible options include steps that would increase the exposure of software and system vendors and system operators to liability for system breaches and mandated reporting of security breaches that could threaten critical societal functions.”⁴⁰

However, legislation introduced at the state level would move in the opposite direction by guaranteeing software vendors greater immunity from liability for product defects. This Uniform Computer Information Transaction Act (UCITA) was enacted in Maryland and Virginia in 2001 and remains under consideration in several other states.

6. Rewarding IT Security in the Marketplace

Since September 11, 2001, U.S. industry and government have taken some steps to increase commitments to and improve incentives for investing in IT security. A notable industry development was Bill Gates' internal memo to employees in January 2002 stating that Microsoft will emphasize security over functionality in its software.⁴¹ Although many have expressed skepticism over the depth of Microsoft's commitment, the company has moved quickly to focus on security and train its developers in "secure coding practices" as part of its new Trustworthy Computing initiative.⁴²

Well-publicized vulnerabilities, customer complaints and threatened litigation no doubt have influenced Microsoft's change in policy. Going further, a Fortune 50 company has recently adding language to a contract with a large software firm making the vendor responsible for security breaches connected with its software, according to trade reports.⁴³ And Wurzler Underwriting Managers has reportedly "tacked a 5 to 15 percent surcharge on cyberinsurance premiums for users of Windows NT on IIS servers, citing their poor security track record..."⁴⁴

On the government side, the new National Cyber Security Division within DHS may provide a stronger focus for IT security threat analysis, warning and response. The long-awaited "National Strategy to Secure Cyberspace," released in February 2003, holds out that promise:

"DHS's integration of several key federal cybersecurity operations centers creates a focal point for the federal government to manage cybersecurity emergencies in its own systems, and, if requested, facilitate crisis management in non-federal critical infrastructure systems."⁴⁵

The National Strategy also calls for stronger government-industry cooperation:

“Separately, industry is encouraged to develop a mechanism – whether virtual or physical – that could enable the sharing of aggregated information on Internet health to improve analysis, warning, response and recovery...
DHS will create a single point-of-contact for the federal government’s interaction with industry and other partners for 24 x 7 functions, including cyberspace analysis, warning, information sharing, major incident response, and national-level recovery efforts. Private sector organizations, which have major contributions for these functions, are encouraged to coordinate activities, as permitted by law, in order to provide a synoptic view of the health of cyberspace on a 24 x 7 basis” (emphasis in original).⁴⁶

However, the draft National Strategy contains no recommendations for government actions to mandate such industry initiatives or otherwise address the market failures surrounding IT security. Supporting R&D and standards development, removing disincentives for industry information sharing, mandating cyber liability insurance or similar financial responsibility for government contractors, and facilitating cyber reinsurance markets are some of the government actions that seem worth consideration today.⁴⁷

In the end, rewarding IT security in the marketplace will probably require legislative changes to define liabilities more clearly and relate them to risk management principles and practices. Responsibility for IT security should reside primarily with those stakeholders who can best take preventive and protective measures. This means making software manufacturers liable for product flaws and vulnerabilities, while making network and system operators and users liable for fixing vulnerabilities that they discover or that are known to exist. Cyber insurance can then provide the means to transfer liabilities among stakeholders in an economically efficient manner. Placing liabilities with the parties best able to manage the

risks associated with them creates the appropriate societal incentives for private decisions about investment in IT security, or insurance against security failures.

Endnotes

-
- ¹ An earlier version of this paper has been published in *Contemporary Security Policy*, April 2003.
- ² Computer Science and Telecommunications Board, *Cybersecurity Today and Tomorrow*, Washington D.C., National Research Council, 2002, p.7.
- ³ L. Jean Camp & Catherine Wolfram, "Pricing Security," *Proceedings of the CERT Information Survivability Workshop*, Boston, MA October 24-26, 2000, pp. 31-39.
- ⁴ President Clinton established the CAIO and the NIPC in response to the Report of the President's Commission on Critical Infrastructure Protection (PCCIP), *Critical Foundations*, Washington D.C., 1997.
- ⁵ World Wide ISAC Frequently Asked Questions, <http://www.wwisac.com/faq.cfm>. Other ISACs support specific industry sectors such as financial services <http://www.fsisac.com>, telecommunications <http://www.ncs.gov/ncc/>, information technology <https://www.it-isac.org>, electric power <http://www.esisac.com/>, surface transportation <http://www.aar.org>, oil and gas <http://www.aar.org/Newsroom/ISAC.asp>, chemicals, <http://chemicalisac.chemtrec.com>, food <http://www.fmi.org/isac>, and water supply <http://www.waterisac.org>. The DHS also provides links to these ISACs at <http://www.dhs.gov/dhspublic/display?theme=73>.
- ⁶ http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci519405,00.html.
- ⁷ S. 1456, the "Critical Information Infrastructure Security Act of 2001," would limit the Freedom of Information Act and the antitrust laws as applied to security information. Introduced in Congress after the terrorist attacks of September 11, 2001, the bill has received support from the Information Technology Industry Council, The Financial Services Roundtable and other IT stakeholders. See Ben Polen, "Tech Groups Pledge to Share Info," *Wired News*, October 19, 2001.
- ⁸ Bruce Schneier, "The Insurance Takeover," *Information Security*, February 2001, http://www.infosecuritymag.com/articles/february01/columns_sos.shtml.
- ⁹ Daniel E. Geer, "Risk Management is Where the Money Is," Paper presented to the Digital Commerce Society of Boston, November 1998, available at <http://catless.ncl.ac.uk/Risks/20.06.html>.
- ¹⁰ See, for example, "Computer Science and Telecommunications Board, *Trust in Cyberspace*, Washington D.C., National Research Council, 1999.
- ¹¹ See James R. Garven, "Risk Management and Insurance," lecture notes and transparencies, University of Texas at Austin, 1995.
- ¹² Schneier, 2001, op. cit.
- ¹³ Chana R. Schoenberger, "Payout," *Forbes*, December 24, 2001.
- ¹⁴ *American Guarantee & Liability Insurance Co. v. Ingram Micro, Inc.*, 2000 U.S. Dist. LEXIS 7209 (DC Ariz. April 18, 2000). The decision was affirmed by the U.S. Ninth Circuit Court of Appeals in August 2000.
- ¹⁵ *Ibid.*
- ¹⁶ *NMS Services, Inc. v. The Hartford*, 01-2491, decided April 24, 2003. <http://pacer.ca4.uscourts.gov/opinion.pdf/012491.U.pdf>.
- ¹⁷ Alex Salkever, "Who Pays When a Business Is Hacked?" *Business Week*, May 23, 2000; Adam H. Fleischer, "What's Wrong with Ingram Micro," *PLUS Journal*, February 2001.
- ¹⁸ Some of the IT security consultants who perform audits and risk assessments for insurance underwriting include Counterpane Internet Security, Unisys, Global Integrity (now part of Predictive Systems), IBM Global IT Security Services and Information Risk Group (a Pinkerton unit).
- ¹⁹ Robert Bryce, "Insurers Offer Incentives to Buy Hacker Insurance," *Interactive Week*, March 5, 2001.
- ²⁰ Risk and Insurance Management Society, "2001 RIMS Benchmark Study," quoted at <http://www.iii.org/media/lateststud/>. See also Lynna Goch, "Study: E-Risk Coverage Stagnates," *Property/Casualty BestWeek*, August 7, 2000, p. 12.
- ²¹ Dimitry Elias Leger, "Why Internet Insurance Isn't the Best Policy," *Fortune*, July 10, 2000.
- ²² Colleen Brush, "2002 Industry Trends: Cyberinsurance," *Information Security Magazine*, November 2001, http://www.infosecuritymag.com/articles/november01/industry_cyberinsurance.shtml.
- ²³ See, for example, Joe Niedzielski, "Catastrophe-Bond Market Appears Poised for Growth," *The Wall Street Journal*, June 12, 2000; Hal R. Varian, "The Case for Catastrophe Bonds," *The New York Times*, October 25, 2001.
- ²⁴ Insurance covering communications satellites faced similar obstacles when commercial space launches began in the 1970s. See Frank Seitzen, jr., "Space Launch Indemnification Renewal Critical to Industry," *Space Policy Digest*, May 1999, http://www.spacepolicy.org/page_fs0599.html.
- ²⁵ <http://www.bitsinfo.org/orginsurance.html>.

²⁶ <http://www.bitsinfo.org/flslab.html>.

²⁷ Scott Berinato, "A UL-Type Seal for Security? Don't Bet on It," *eWeek*, October 15, 2000. Bruce Schneier, CTO of Counterpane Internet Security, is quoted in this article as downplaying the prospects for a UL-type organization for IT security: "The sheer complexity and cost ...[suggests] you could never get ahead of the problem."

²⁸ <http://www.bitsinfo.org/sltestedmark.html>.

²⁹ David R. Graham et al., *A National R&D Institute for Information Infrastructure Protection (I3P)*, Alexandria, VA: Institute for defense Analysis, IDA Paper P-3511, April 2000. The I3P concept initially was proposed by the President's Council of Advisors on Science and Technology in December 1998, in response to the 1997 Report of the President's Commission on Critical Infrastructure Protection.

³⁰ Nicholas Pasciullo, personal communication, 2001.

³¹ For example, see Computer Science and Telecommunications Board, *Cybersecurity Today and Tomorrow*, op. cit., 14; Hal R. Varian, "Managing Online Security Risks," *The New York Times*, June 1, 2000; "A Lemon Law for Software?" *The Economist Technology Quarterly*, March 16, 2002, 3; Ira Sanger and Jay Greene, "The Best Way to Make Software Secure: Liability," *Business Week*, March 18, 2002, 61; Bruce Schneier, "Liability and Security," *Crypto-Gram* newsletter, April 15, 2002, <http://www.counterpane.com>.

³² "Government Devises Computer Security Standards to Fight Most Common Internet Threats," *San Jose Mercury News*, July 16, 2002, available at <http://www.siliconvalley.com/mld/siliconvalley/3674640.htm>.

³³ "Notification and Reporting of Aircraft Accidents or Incidents," National Transportation Safety Board Regulations, 49 CFR830.

³⁴ California recently passed a Security Breach Information Act, which requires a company to make a public disclosure (e.g., by a notice on its Website) if its computer systems have been hacked and sensitive customer data may have been compromised. The Act went into effect on July 1, 2003. See http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html.

³⁵ Association of British Insurers, "ABI Opens Discussions with Government on Terrorism Insurance for Commercial Property," December 21, 2001.

³⁶ *H.R. 3210, Terrorism Risk Insurance Act of 2002*, "Congressional Findings and Purpose," Title I, Sec. 101.

³⁷ For an excellent treatment of government as the insurer of last resort, see David A. Moss, *When All Else Fails: Government as the Ultimate Risk Manager*, Cambridge, MA, Harvard University Press, 2002. Flood and other disaster insurance are discussed in Chapter 9, "Security for All," pp. 253-291.

³⁸ <http://www.fema.gov/nfip>.

³⁹ <http://www.earthquakeauthority.com>.

⁴⁰ Computer Science and Telecommunications Board, *Cybersecurity Today and Tomorrow*, op. cit., 14.

⁴¹ The Gates memo stated: "...when we face a choice between adding features and resolving security issues, we need to choose security." Dennis Fisher, "Gates: Security Over Features," *eWeek*, January 21, 2002.

⁴² Craig Mundie et al., "Trustworthy Computing White Paper," Microsoft Corporation, January 31, 2002, <http://www.microsoft.com/presspass/exec/craig/01-31trustworthywp.asp>; Paul Boutin, "Anti-Trustworthy Computing," *Salon*, April 9, 2002.

⁴³ "Dennis Fisher, "Contracts Getting Tough on Security," *eWeek*, April 15, 2002.

⁴⁴ Brush, op. cit.

⁴⁵ Department of Homeland Security, *The National Strategy to Secure Cyberspace*, February, 2003, p. 22, http://www.dhs.gov/interweb/assetlibrary/National_Cyberspace_Strategy.pdf.

⁴⁶ *Ibid.*

⁴⁷ However, additional government intervention in cyber insurance, or government regulation of private investments in IT security more generally, must contend with well-known political-economic problems of regulatory dynamics. These include slow regulatory decision making processes that conflict with fast-moving IT developments, regulatory processes and procedures that generally favor incumbents over new entrants, rules that protect certain groups such as households and rural areas, and outcomes that favor political effectiveness over economic efficiency. Government initiatives in IT security inevitably will tend to be slow, incremental and designed in ways that skew markets in order to protect regional and other important political constituencies. Peter Cowhey, University of California – San Diego, private communication, 2002.