MARKET FORCES AND GOVERNMENT ACTION IN SECURING CYBERSPACE
PRELIMINARY REPORT

Summary. Network security is a key component for obtaining the full economic benefit of the Internet and poor network security poses unacceptable risks to America's critical infrastructure, but America's computer networks are not secure. Forty experts and leaders in the field of cyber security met on December 13, 2000 at the Center for Strategic and International Studies to discuss how to move ahead in building secure public networks and protecting critical infrastructure. The broad question considered was whether market forces will naturally provide for adequate security, or whether government intervention is necessary. This report summarizes the meeting and draws certain conclusions from it:

-- *Technology*. Most computer networks are built with vulnerable technologies designed to allow easy access - licit or illicit. "Open source" software, outsourcing, and new IP standards and protocols will help change this, but the most important change may come when security is an embedded and transparent feature of operating systems.

-- *Law.* Computer networks today are like highways where there are few traffic laws and where no one is responsible for damages if they cause an accident. Improving cybersecurity means finding ways to make someone liable for negligence and damage for security failures. Allocation of liability (through contracts or through legislation) is one of the best incentives for driving the market to improve computer network security. Most countries need to strengthen their laws for cyber crime. The Council of Europe Treaty, although not without flaws, can contribute to this.

-- *Markets.* The Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act will force parts of the private sector to improve security and will greatly expand the market for computer security. However, cybersecurity is a "public good" and poses a "collective action" problem (like national defense, highway safety or environmental protection) and the U.S. must gauge, especially for protection of critical infrastructures, whether and how government actions (like incentives) should supplement market forces.

-- *Organization.* Government and the private sector need to change how they are organized for cybersecurity to improve. The Government's mission and bureaucratic structure for cybersecurity is too diffuse. For the private sector, making network security an integral part of corporate governance would speed improvement.

Obstacles to Better Cybersecurity

Building secure public networks has been on the Federal agenda since at least 1992. After repeated setbacks, the U.S. moved from policies that called for the Federal Government to play a central role in building secure public networks. By 1997 (after the experience of Clipper and Key Escrow), the U.S. would, for e-commerce and for security, let market forces and the private sector shape cyberspace.

Measurement of the cost of security failures and the potential risk to critical infrastructure is difficult and often exaggerated. However, no one disputes that the security of the network of computers that form the backbone of the information age is poor -- poorer than it needs to be. The nature of this computer network (an agglomeration of millions of different, privately owned systems), the speed with which it has arisen and the technology that underlies it explains how this situation came about. While much good work has been done in the last four years to change this, how do we now move ahead to improve cybersecurity?

Guidelines for Policy

- Technology-neutral.
- Industry-led.
- Minimal, predictable legal and regulatory environment.
- Private-public partnership.
- Global (rather than national) solutions

Technical, legal, commercial and organizational issues stand in the way of better cybersecurity. These obstacles are in part the legacy of technology and policy developments as the Internet emerged over the 1990s, and they reflect the challenge of melding a new thing - the Internet and cyberspace - into laws and organizations not designed for it. In looking at them, we weighed the extent the U.S. can rely on the market and to what extent the government needs to act.

Technology. The millions of legacy systems that form the Internet are an obstacle to greater security. Security was not seen as a concern until much of the “infrastructure” for computer networks was in place. The Internet is a collection of open, unencrypted networks. Technical standards have focused on ensuring easy compatibility among diverse systems and on network reliability. There is no widely accepted standard for security. The environment is one of rapid growth, diverse, evolving technologies and no common approach for security. Previous government policies discouraged the use of encryption to build secure networks. The result is a porous structure of unsecured systems. Some network “solutions” aggravate security problems, as programmers or systems administrators build network management tools like “Back Oriface” into servers and PCs without users’ knowledge - these network management tools make remote administration of computer networks easier but can also create major security vulnerabilities that can be easily exploited by hackers or other unauthorized users.

Making better security products available is one area for potential solutions, if people will buy them. Industry-led technological solutions, such as the development of PKI and authentication technologies, protocols like IPSec or IPv6, – may provide a solution as these more secure systems over time replace less secure ones. The use of open source software could also improve security, by allowing thousands of testers to look for bugs and propose fixes.

Legal Issues. Security depends on enforceable laws, and establishing legal liability for security failures is crucial for better security. Contracts can assign liability, but are not sufficient for the larger problems created by an open, global network. Assigning liability has been very difficult (often, the failure is the work of unknown parties). If no one is liable for a security failure, there is less incentive to improve. Software manufacturers are not (to date) liable for errors in their products. Service providers have not been held liable for failures to provide service or for allowing a third party to launch attacks from or through their systems. Corporations are not liable for failing to take adequate steps to ensure network security.

The conventional legal solution to security failures would be to sue the perpetrator, or to assign negligence (and thus liability). This does not work when liability cannot be established. Contract law offers a partial remedy to this problem through the use of contracts between service providers and companies that explicitly assign responsibilities for security. More and more firms are using contracts to assign liability and this may emerge as a key incentive for improvement. Assignment of liability for security failure is a necessary step to ensure that the private sector will make precautionary expenditures.

Conventional legal solutions are also not adequate for deterring or punishing cybercrimes. Cybersecurity poses a new set of behaviors not neatly addressed by existing laws. Most countries lack an adequate legal framework for the deterrence and punishment of cybercrimes or rely on an uneven patchwork of legislation. While the Council of Europe's Cybercrime Treaty offers the possibility of strengthening legal frameworks in a number of countries, it has attracted criticism from industry and privacy advocates.

Federal Statutes for Computer Crimes

- 18 U.S.C. 1831 Economic Espionage Act
- 18 U.S.C. 1832 Trade Secrets Act
- 18 U.S.C. 1362 Government Communication Systems
- 18 U.S.C. 1361 Injury to Government Property
- 18 U.S.C. 1029 Possession of Access Devices
- 18 U.S.C. 875 Interstate Communications
- 18 U.S.C. 1030 Fraud or related activities by computer
- 18 U.S.C. 1343 Fraud by wire, radio or television

Improving cybersecurity also requires some resolution of the privacy problem. There are three parts to the privacy/security nexus. First, there is a close connection between security and ensuring the privacy of data on your own computer - preventing unauthorized persons from using the network to access files on your computer or plant programs (including cookies!) on your computer. Second, ensuring the privacy of your data on someone else's computer is a security issue. Even if a site has a good privacy policy, if their security is bad and unauthorized users can get access to data stored there (such as credit card numbers or medical data), privacy has been compromised. Finally, measures that protect privacy (especially anonymity) on the Internet can complicate the task of increasing security. Privacy safeguards can work against basic security technology implementation. Some measures that could make the Internet more secure can also greatly reduce privacy (assigning a permanent, remotely accessible identification number to each chip, for example). Anonymity on the Internet, valuable for privacy, allows hackers to evade liability. While newer Internet protocols will help increase security and trust, the U.S. needs to consider the trade-offs between privacy and security. Government involvement can help define these trades, to help achieve a balance between security and privacy.

Multilateral Issues. The Internet is a borderless phenomena and cyberspace does not fall within any national jurisdiction. There is already extensive (and excited) literature on how individuals or governments anywhere in the world can easily launch an attack on U.S. infrastructure or networks, and this attack can pass through several other countries in the process. This poses problems for assigning liability and for the enforcement of laws. Efforts to improve cybersecurity can be taken on the national level, but these must be complemented by multilateral efforts. The U.S. briefly explored, but did not pursue, multilateral cooperation in talks held by the Presidential Envoy for Cryptography, and the Council of Europe Cybercrime Treaty is a useful vehicle for developing coordination. However, the U.S. may face difficulties in developing broad cybersecurity coordination, given concerns over national security issues (such as the debate over ‘Echelon’) in Europe.

Multinational cooperation in making computer networks more secure is essential, given the global nature of the Internet and to avoid “balkanized” solutions. As with the Y2K program, there must be an effort to educate other governments. This includes acceptance of interoperable standards and development of adequate civil and criminal law (such as the Council of Europe Cybercrime Treaty). A useful first step would be to assign the responsibility for working on multilateral coordination of cybersecurity to an agency in the U.S. government.

Market Issues. In a perfect market, the private sector would purchase adequate security and private sector firms would offer the products needed to build it. To date, this is not the case. In fact, it is legitimate to ask if there has been “market failure” when it comes to cybersecurity.

Why Would The Market Fail?

- No demand (cost of security failure is low or perceived as low)
- Supply can’t meet demand (market not providing technology)
- Liability not assigned (if you don’t bear the cost, you won’t buy solutions)
- Risk of bad publicity outweighs cost of security failure (firms quietly absorb cost rather than compromise reputation)
- Lack of Market/No Market maker (government restrictions)
- Lack of information about risks (high transaction costs)
- No incentive to pay for a “public good.”

Market obstacles to security reflect difficulties in assessing risk and liability, and grow, to some extent, out of the legal and technical issues. If companies become concerned about the potential risk to their networks or if courts can assign liability for attacks, demand for security products and services will grow rapidly. The Health Insurance Portability and Accountability Act of 1996 (known as HIPAA) and the Gramm-Leach-Bliley Financial Reform Act, by creating responsibility for privacy and security, have had this effect and are driving demand for, and use of, security products (see Appendix A for a description of these laws).

One speaker noted that the marketing of security products has also contributed to the problem, in that each product is presented as “the solution” when in fact a layered defense and secure infrastructures are needed. Network security products can be costly and difficult to implement for anyone who is not an expert in security technology, and there are few such experts relative to the demand for their services. Security also remains a secondary consideration for many in the software industry – witness the number of products that contain (without the users’ knowledge) software tools like “Back Orifice,” to allow remote access to computers for customer service, but which also create serious vulnerabilities for unapproved access.

The weakest link in a computer network determines security. This can include computers on your own network or a computer that can access your network. While many organizations now see the security risks posed by their computer networks as important, their security is interdependent with the consumer side of the network. For example, the penetration of Microsoft (which had sophisticated security systems) appears to have occurred through an employee working at home. Consumer systems remain the weak link. Systems that provide for “always-on” Internet access (such as DSL) are particularly vulnerable. Companies believe that consumers will pay little or nothing for security, but this may be less of a problem if security becomes embedded and transparent in consumer applications (such as operating systems, e-mail or file programs).

The traditional response to market failure is government intervention. Intervention could include some combination of direct or indirect subsidies (such as government taking the role of Insurer of Last Resort) or tax relief. Government could also target these subsidies at key sectors that have greater leverage to move the larger market. Government action could also include enacting legislation that would limit liability, using Federal Purchases and Standards to move the market in a particular direction, or exhortation by government officials for the private sector to voluntarily take certain actions. There are also negative incentives, where the government could use regulations and penalties to encourage certain forms of behavior.

Organizational Issues. Since 1996, the U.S. response to cyber threats has been robust. The President's Commission on Critical Infrastructure Protection, established in July 1996, was the first national effort to address the vulnerabilities created in the new information age. The cornerstone of this response is the May 1998 Presidential Decision Document 63 (PDD-63), which lays out overall guidance for critical infrastructure protection. PDD-63 established a National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism, located in the White House, whose responsibilities encompass cybersecurity. PDD-63 also established two new agencies, the Critical Infrastructure Assurance Office and the National Infrastructure Protection Center, to work with the private sector.

A "National Plan for Information Systems Protection buttresses PDD-63 by focusing on domestic efforts by the Federal Government to protect critical cyber-based infrastructures. Information Sharing and Assessment Centers (ISACs) were created to share information, and expertise. In addition, the Administration has pursued a number of related initiatives to improve network security, including the selection by the National Institutes of StandardsTechnology of a new and stronger encryption algorithm (AES) to replace DES, a Public Key Infrastructure (PKI) effort, and the creation of a Federal CIO Council. As part of this larger effort, the Administration relaxed its controls on encryption exports in September of 1999 to encourage the use of strong encryption.

These steps are beneficial, but like many other problems that cut across the responsibilities of traditional agencies in the last decade, the solution was to place a National Coordinator in the White House. However, responsibilities within the government are diffused in a way that could challenge even the most energetic national coordinator. This organization could be simplified and centralized (see Appendix C).

Cyber-bureaucracy

•PDD-63
•National Coordinator
•Critical Infrastructure Assurance Office
•National Infrastructure Protection Center
•PKI, AES, CIO Council, etc.
•Relaxed Encryption Controls

A new Administration may want to reconsider assignment of responsibilities. The CIAO provides an essential coordinating function with the private sector, and if it is not continued, it must be replaced. Responsibility for information sharing about viruses or network attacks is critically important for security. The current US approach could be improved. NIPC, while performing an essential function, has had difficulties in sharing information about network attacks in a timely fashion. Because of the constrained imposed on the sharing of law-enforcement information. For example, NIPC learned of the Love Bug attack early in the morning on the day it occurred, but did not notify the public until four hours later. Law enforcement needs a centralized center for investigating network security attacks, but information sharing is a different mission with different requirements. Information sharing on computer attacks may also be an area particularly amenable to outsourcing to nongovernmental entities.

The private sector also has organizational issues. Managing network security risks is not yet an essential part of corporate governance. Some industry sectors are moving rapidly to address security issues without government involvement. Credit card companies and their participating merchants, banks, investment firms and others are making strides to operate more securely. The leading edge on improving security appears to be the financial sector, but it is not clear how far its improvements will percolate into other sectors absent further change. A requirement for discussion or even rating of the security of a company's computer networks in annual reports would have stimulate security, as would consideration of security as part of the provision of insurance. Linking network security management to profit ands loss statements would raise the profile of the problem and create incentives for addressing it.

Some believe that government can affect corporate governance through an approach to cybersecurity like that taken to address the Y2K problem. While security is an ongoing problem and Y2K was a single event, the Y2K model may offer suggestions for moving ahead. The primary function of government in Y2K was as an organizer and educator. The Y2K effort gathered and disseminated information, organized multinational networks for addressing the problem, shared information on best practices and worked through public-private partnerships to raise awareness. Regulatory changes in some sectors also had a marked effect. The Securities and Exchange Commission had a galvanizing role in Y2K preparations, as did similar actions by banking regulators. Companies had to show publicly and to their regulators that they had taken adequate steps to protect against Y2K disruption. Similar SEC requirements for companies to report the steps they are taking to protect themselves from a cyber attack would improve the security of computer networks.

Cybersecurity in Perspective - Public Goods and Collective Action. A public good gap is a market obstacle of particular interest. A "public good" provides benefits to an entire society with very little incentive for any one person to pay for it. Since everyone benefits equally from a public good whether they pay for it or not, there is little incentive to pay (cleaner air or national defense are examples of public goods). Provision of public goods is usually a government function. Network security measures that protect critical infrastructure could be another public good.   Securing the infrastructure benefits both those who pay for the improvements and those who do not. To the extent critical infrastructure security is a public good, there will be less incentive for the market to invest in it. A gap would appear if the level of security necessary to manage risk for the commercial sector were not sufficient to protect critical infrastructures. The level of risk that a company might find economically reasonable might still allow for vulnerabilities in critical infrastructure networks. This would be a case of market failure where government incentives may be necessary.

A level of Internet security sufficient to protect critical infrastructures is also a "collective action" problem. Collective action problems arise when multiple parties have to behave in a coordinated way to get a positive outcome. For networks (and infrastructure) to be secure, the thousands of individual participants in the Internet must each improve security. Their own security depends on the choices made by others on the network.

Several approaches that seem to offer possible avenues to resolving the collective action problem for Internet security issue involve reputation, tort and insurance. A "reputational" solution would involve the creation of a public rating of security by third parties (such as Moodies or others currently provide for bond and credit ratings) and would create visibility and incentives for firms to improve security, especially if these ratings affect eligibility for insurance or were potential areas of liability for corporate officers. Other firms would not want to do business (or would limit their business) with companies identified as having poor security. The market can generate solutions to collective action problems, or they can be solved by legislation and regulation, or by some combination of the two. Orchestrating a collective effort to improve cybersecurity might be a good place for legislative action.

Conclusions

The Internet is decentralized and diffused among thousands of private sector entities that are guided primarily by the profit motive and market forces. The burden of security falls on the private sector, not the government. The computer network that has become integral to the U.S. does not respond well to centralized command. In this context, government's role is best seen as support for the market. However, many feel uneasy in limiting the government's role to that of spectator and cheerleader for private sector cybersecurity initiatives.

In thinking about cybersecurity, we might want to consider several scenarios. In one, security will improve through market forces, as better products come on line, as new standards and protocols (like IPSec) become available, security will innately become better. Greater use of "Open Source" products will allow bugs and errors that could damage security to be found, publicized and repaired. The increase of outsourcing and the growth of larger server farms will improve security by distributing targets and centralizing responsibilities and needed skills. The development and extension of contractual bases for security will allow parties, in the business-to-business context, to allocate risks by contract, so that penetration or failure of a computer network would result in enforceable financial penalties against service providers. In turn, service providers would seek insurance.

A second scenario would take these same trends but find that they were inadequate or too slow. Government intervention would facilitate these private sector developments, call greater public attention to them, and help ensure coordination with other governments. In some instances, the government could find incentives to accelerate or expand improvements for some critical sectors.

A third scenario would modify these trends by adding ill-considered laws and regulations, that would actually inhibit improvements to cybersecurity or misdirect work into less effective paths. Government (including Congress) must be aware that actions taken to fix one aspect of the cybersecurity problem could have unforeseen and damaging consequences.

A more careful analysis, based on public good and collective action models, suggest that we might be able to split this problem. These models predict that firms will pay for some level of improvements to security, but have little or no incentives to pay for improvements above that level. A simple guess would be that we can probably depend on market forces to improve network security overall - economic self interest and consumer concerns will probably drive business and organizations to build in security, and this will create demand for the IT industry to build and offer better security products.

What is undetermined, however, is whether this level of security, while adequate for commercial activities, will be sufficient to protect critical infrastructure. The degree to which commercial security improvements will be inadequate may differ from sector to sector - utilities may be willing to accept a lower level of network security than will the financial sector, for example. It is also not clear if the market response will occur in as timely a fashion as we need to meet national security requirements. Given the technical difficulties of building security products, and given the legacy of a network built on millions of unsecured products, we need to ask whether in the near term government will need to take action in specific infrastructure sectors identified as critical and not secure.

It is in this area - critical infrastructure sectors that have less incentive to improve security to the level needed for critical infrastructure protection- that incentives might make sense. In partnership with industry, the U.S. would need to identify what level of protection is adequate and what sort of incentives would be best suited.

Some believe that market forces and the evolution of the IT industry will improve security, and others believe that the government must take a more active role. To some extent, this is a difference of degree - there are some activities that all agree the government should pursue - but in some fundamental areas, notably the question of whether the market has failed and that government must create incentives for the private sector, we are far from a consensus.

The three themes of this initial discussion were whether the private sector would build sufficient security (i.e. is there market failure), whether the private sector will build security sufficient for protection of critical infrastructures (the public good problem) and what government's role should be in building cybersecurity. The discussion did not resolve the question of whether the market has failed to improve security and if subsidies are needed. It did identify a number of areas where the government could take action that would help the private sector improve security, such as raising awareness and encouraging multilateral cooperation. It also identified a number of legal and contractual issues that must be resolved for improved security, such as assignment of liability or the development of adequate auditing procedures, but which are not areas where the Executive branch has the lead.

Further progress depends on how the government conceptualizes its mission. Security and other Internet problems challenge government's ability to carry out its functions. Traditional governmental responses, such as regulation, will not create cybersecurity. Some say that a new style of governance built on more explicit public-private partnerships is essential. Defining the scope of this partnership and the responsibilities of each partner requires further interaction between the private and public sectors.

Cybersecurity is improving, but there is disagreement over which tasks require government action and what can be left to the market. We need to identify places where the market response is weak as candidates for government action, and which government actions (if any) would be an appropriate

Needed for Security

- Liability for negligence.
- Sufficient legal authorities.
- Transparent security technologies.
- Better privacy protection.
- Less ad hoc information sharing.
- New Organizational structures for Government and private sector.
- Better measurement of risks and costs.

response. We would want to specify needed steps in multilateral work, legislation, standard setting, and risk measurement. Finally, we need to reconsider the division of labor between the public and private sector and between agencies for improving cybersecurity and for specific tasks, such as information sharing.

Appendix A - HIPAA and Gramm-Leach-Bliley

The Health Insurance Portability and Accountability Act of 1996 (known as HIPAA), requires the Department of Health and Human Services to develop standards and regulations for transmission and storage of health information that identifies individual patients. These will standardize the exchange of electronic data for certain administrative and financial transactions and protect the security and confidentiality of electronic health information. The requirements outlined by the law and the regulations promulgated by DHHS are far-reaching - all healthcare organizations that maintain or transmit electronic health information must comply, and the law provides for significant financial penalties for violations.

The intent of HIPAA was to protect privacy, but it also affects security procedures. There is no common standard for the security of health information that fully meets HIPAA requirements. HHS developed a security standard with input from standards groups and industry that is technology- neutral and scaleable. Health organizations that transmit or store electronic health information must conduct a risk assessment and develop a security plan to protect this information. They must document these measures, keep them current, and train their employees on security procedures. The security standard is divided into four categories: administrative procedures, physical safeguards, technical data security services, and technical security mechanisms to prevent unauthorized access to data transmitted over a communications network

Section 504 (a) of the Gramm-Leach-Bliley Act establishes a federal standard for financial privacy. Financial institutions are required to have written privacy policies that must be disclosed to customers. The disclosure of a financial institution's privacy policy must take place at the time a customer relationship is established and not less than annually during the continuation of the relationship. In addition, consumers can opt out of having private financial information shared with most third parties without their permission. Federal and state regulators are to establish comprehensive standards for ensuring the security and confidentiality of consumers' personal information. The privacy provisions apply to any company engaged in financial services, whether affiliated with a bank or not. GLB covers finance companies, insurance companies, securities dealers, and even travel agencies. Many of these entities may not yet be aware of this. The FTC published regulations that went into effect in November 2000

Appendix B - Insurance Issues

Insurance markets arise where there is advantage from pooling risk. Cyber security is a logical candidate for insurance, and some perceive an opportunity in this for government action. Insurance requirements can drive private entities to take steps to mitigate risk, and insurance will play a role in improving Internet security. How large a role depends on how the insurance market is constructed and, possibly, the degree of Government involvement as an "insurer of last resort."

Currently, Internet security breaches could overwhelm the private reinsurance market. The worldwide reinsurance market is worth $10-20 billion, but a single attack or Internet event could lead to losses exceeding this amount (some estimates placed the cost of the "Love Bug" attack at $15 billion). Insurance works poorly in spreading the risk (and the cost) of an event when losses are "correlated" (i.e. they all happen at the same time, as with an earthquake or hurricane). Some see an opportunity in this: the Federal government could become the insurer of last resort (as it is now for natural disasters) but, in exchange for assuming this liability, it would require insurers and their customers to meet a certain level of security.

Reinsurance has budgetary implications for the government. Poorly constructed insurance markets can create unmanageable liabilities for insurance providers. Two key issues for insurance as a tool for the management of risk in cybersecurity are "adverse selection" and "moral hazard."

"Moral hazard" means that the insured person reduces precaution or allows people to undertake risks that they would otherwise avoid. If parties do not bear the costs of a failure to improve network security, they will have no incentive to minimize risk. "First party" insurance, where an entity buys insurance for its own losses, could reduce incentives to improve Internet security by creating "moral hazard," For example, flood plain insurance actually encourages people to build on flood plains, as they do not bear the risk of damage.   If an insurance company (or ultimately the government) will reimburse you for any loss from a cybersecurity failure, you will do less to reduce the risk of failure.

"Third party" insurance, where an entity buys insurance to cover the risk of damages to someone else, avoids the moral hazard problem but depends on good actuarial data, something we do not yet have for Internet security. "Adverse selection" occurs when insured people hide information that would be pertinent to the insurer in estimating the likelihood of loss. The lack of reliable actuarial data makes adverse selection a real risk for Internet security. Avoiding these problems requires good actuarial data and the ability to make those who are negligent bear the costs of security failures (i.e. assign liability).   Federal participation in reinsurance makes sense only in a market that avoids moral hazard and adverse selection.

An effective insurance market for cybersecurity has other requirements as well. An agreed measure of what is good network security is necessary for insurance companies to say that the policy holder has in place a level of security sufficient to show reasonable care (and avoid negligence). British Standard 7799 (BS7799), a widely recognized security standard covering continuity of operations, system access control, physical security and network management, is the leading candidate for a common standard.

However, audits of how well a company has implemented BS7799 can vary widely and take months to complete. HIPAA offers another set of standards that, with some modifications, could be used by other industry sectors.

Most insurance policies also exclude “force majeure” events, such as acts of war, which could pose a problem for the Internet where it is sometimes difficult to distinguish between an act of war, terrorism, a crime or a fifteen-year-old prankster. In addition, for insurance to be effective, there would have to be some change to the “intentional acts” exclusion that is a feature in many insurance policies. It excludes coverage for claims stemming from intentional acts, but surveys show that between 70 and 80 percent of all Internet security incidents come from internal sources (although this figure is dropping). For insurance to be attractive (and thus provide leverage for improvements) there would have to be coverage for intentional acts

While in the past insurance markets were not willing to write policies for Internet security failures (such as losses from interruption of business or intangible losses), this is changing. Few companies are willing to write policies for business interruption loss (due to a denial-of-service attack, for example). In part, this reluctance reflects the lack of good actuarial data, which makes it very hard for companies to estimate risk and the price that should be charged for insurance. That said, some companies report that applicants for insurance have quadrupled – and these applicants are seeking new policies, not extensions of existing policies. The most sophisticated clients are not only buying coverage at catastrophic level, but they are requiring their business partners to have this coverage as well. The growing trend to outsource network management and security will also shape the insurance market.

There would have to be better actuarial data so that the degree of risk could be calculated (including the degree of risk that could be associated with different security configurations). The lack of a definitive estimate of the actual damages that could result from systemic network failure also poses serious problems for insurance. Public estimates of cybercrime damages vary widely (ranging from $265 million to $15 billion for a single year) and often include a range of damages such as theft of laptops and loss of intellectual property from Napster downloads. Insurance (and reinsurance) requires a better idea of the costs associated with various kinds of security failures and their results.

Government action could help remove some obstacles to the use of insurance, such as the lack of actuarial data, lack of security standards and problems with the assignment of liability. Government action could address the problem of correlated losses by subsidizing the reinsurance market, and the provision of reinsurance (or acting as the insurer of last resort) could allow the government to set standards for security. Helping an insurance market emerge more rapidly or more smoothly is different, however, from providing a de facto subsidy as an insurer of last resort. Subsidies for a poorly constructed insurance program would actually impede security enhancements. Even the act by the government of exploring with the private sector the standards, costs and nature of insurance programs might benefit cybersecurity.