International Lawyer

Volume 36 | Number 1 Article 6

2002

The Response to Cyberattacks: Balancing Security and Cost

Peter Lichtenbaum

Melanie Schneck

The Response to Cyberattacks: Balancing Security and Cost

PETER LICHTENBAUM* AND MELANIE SCHNECK**

> We are at risk. Increasingly, America depends on computers. They control power delivery, communications, aviation, and financial services. They are used to store vital information, from medical records to business plans to criminal records. Although we trust them, they are vulnerable—to the effects of poor design and insufficient quality control, to accident, and perhaps most alarmingly, to deliberate attack. The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb.[1]

This remarkably prescient passage was published over a decade ago in the National Research Council's seminal *Computers At Risk* report. Yet, it is only now, in the wake of the September 11, 2001 tragedies, that government and industry are devoting the substantial resources necessary to address the vulnerabilities of our information infrastructure. In recent months, the U.S. and other governments and industry have redoubled their support for cybersecurity initiatives designed to protect our information infrastructure against cyberattack.[2] For instance, the United States has enacted the USA PATRIOT Act legislation, and companies such as Microsoft and Oracle have announced that security issues will receive much higher priority.[3]

It is unquestionable that cyberattacks pose a real threat to the Internet and the networked business community generally. Just last year, attacks on computers shot up 160 percent to

*Partner, Steptoe & Johnson LLP, Washington, D.C.

**Associate, Steptoe & Johnson LLP, Washington, D.C.

1. COMPUTER SCIENCE AND TELECOMMUNICATIONS BOARD, NATIONAL RESEARCH COUNCIL, COMPUTERS AT RISK: SAFE COMPUTING IN THE INFORMATION AGE, at 7 (National Academy Press 1991).

2. This article uses the term cyberattack to encompass cyberterrorism as well as other cybercrimes, such as hacking and denial of service attacks. Cyberterrorism involves cyberattacks undertaken in order to influence government policy. *See* Uniting and Strengthening America By Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, § 802(a)(5), 115 Stat. 272, 376 (2001).

3. Byron Acohido, *Non-Profit Agency Raises Bar on Tech Security*, USA TODAY, Feb. 27, 2002, *available at* http://www.osopinion.com/perl/story/16528.html (explaining that Microsoft Chairman Bill Gates "recently declared security the software giant's No. 1 priority – ordering 8,000 programmers to spend a month concentrating on it.").

more than 52,000, according to the CERT® Coordination Center (originally known as the Computer Energy Response Team), a major reporting center for Internet security problems.[4] Moreover, in a recent FBI computer crime and security survey, 85 percent of respondents revealed that they had detected security breaches within the last twelve months. Sixty-four percent of respondents acknowledged financial losses due to computer breaches, and the 35 percent (186 respondents) that quantified their losses reported $377,828,700 in financial losses.[5] Although the FBI survey primarily focused on large corporations and government agencies, small and midsize enterprises (SMEs) also are at risk according to Gartner Group. According to their projections, 50 percent of SMEs will experience a successful Internet attack (e.g., Web site hacking) by the year 2003, if they (1) manage their own network security, and (2) use the Internet for more than e-mail.[6] Further, organizations will spend $14 billion by the year 2005 in order to fight off cyberattackers, according to a projection by research firm IDC.[7]

However, bolstering cybersecurity may be a double-edged sword, staving off cyberattacks to the benefit of those engaged in electronic communications and transactions, but simultaneously burdening the Internet and other networks by increasing the costs, both financial and otherwise, of doing business. In other words, cyberattacks impose an indirect "tax" on electronic communications and transactions, as new security measures drive up the cost of doing business and undermine important values such as privacy. Accordingly, governments and businesses must take particular care to ensure that, as they take steps to bolster cybersecurity, the benefits of increased cybersecurity outweigh the costs, some of which may be quite difficult to quantify (e.g., the potential loss of privacy associated with increased network monitoring).

In this article, we discuss domestic and foreign government responses to the cybersecurity threat; describe corporate responses to this threat; and analyze how these responses themselves may burden the expanded development and use of the Internet.

I. U.S. Government Response to the Cybersecurity Threat

In an effort to address the cybersecurity threats facing the country, the United States has relied upon its federal criminal law and has developed multiple infrastructure protection initiatives. Many of these steps began years before the events of September 11, 2001 brought security concerns to the forefront of American political priorities, but there has been a renewed focus since that time, as evidenced by the USA PATRIOT Act.[8]

The United States government has long subjected cyberattackers to potential criminal prosecution under a variety of domestic laws including: (1) the Computer Fraud and Abuse Act (CFAA) of 1986;[9] (2) the Economic Espionage Act of 1996;[10] (3) the federal wire fraud statute;[11] and (4) various state criminal laws. For example, the CFAA criminalizes unautho-

4. *Id.*

5. 2001 COMPUTER SECURITY INSTITUTE/FEDERAL BUREAU OF INVESTIGATION COMPUTER CRIME AND SECURITY SURVEY, at 4.

6. Gartner Group, Inc., *Small and Midsize Enterprises are Likely Targets for Internet Attacks*, Oct. 10, 2000, *available at* http://www3.gartner.com/5_about/press_room/pr20001010a.html.

7. Acohido, *supra* note 3.

8. Pub. L. No. 107-56, 115 Stat. 272 (2001).

9. 18 U.S.C. § 1030 (1986).

10. 18 U.S.C. § 1831 (1996).

11. 18 U.S.C § 1343 (1952).

rized access to certain protected computers, including those used by financial institutions, by the federal government, and in interstate commerce or communication. The CFAA also criminalizes the knowing transmission of a computer virus or other code that causes intentional damage to a protected computer. The CFAA reaches any person who, with the intent to extort his or her victim, threatens to cause damage to a protected computer. Moreover, once cyberattackers are identified, victimized corporations can bring civil actions seeking compensation for damages arising out of CFAA violations or breaches of state common law.

In addition to the federal criminal laws designed to deter and punish cybercrime, the U.S. government is engaged in more direct efforts to protect the country's critical infrastructure against cyberattack. More than a decade ago, the National Research Council addressed critical infrastructure protection issues in its influential *Computers at Risk* report. Several years later, then-President Clinton established a Commission on Critical Infrastructure Protection, whose 1997 report prompted the President to issue Presidential Decision Directive (PDD) 63. PDD 63 not only required federal agencies to develop critical infrastructure protection plans, but also, more importantly, outlined a general strategy to protect the nation against the threat of cyberattacks. Recognizing the importance of information sharing to critical infrastructure protection, PDD 63 encouraged the formation of information sharing and analysis centers (ISACs). The ISACs were intended to serve as conduits carrying information back and forth between the private sector and government, and by March of 2001, six ISACs had been established in five different industry sectors.[12]

Also as envisioned by PDD 63, the FBI's National Infrastructure Protection Center (NIPC) serves as the U.S. government's "focal point for threat assessment, warning, investigation, and response for threats or attacks against our critical infrastructures."[13] Operating as a partnership between the federal agencies and private industry, NIPC seeks to protect from cyberattacks the United States' critical infrastructures including: telecommunications, energy, transportation, banking and finance, water systems, emergency services, and government operations.

Despite the United States' extensive federal criminal laws and infrastructure protection efforts, the events of September 11 spawned a new set of cybersecurity efforts and initiatives. In some ways, this seems an odd result. The U.S. information infrastructure was not targeted by the attacks, and the Internet functioned rather well throughout the attacks, even as other components of the U.S. infrastructure (e.g., air transportation, ground transportation, and cellular communication) were brought to their knees. Moreover, the events of September 11 appeared to teach us little new about the threat of cyberterrorism. Nonetheless, the terrorist attacks instilled a sense of urgency regarding previously identified threats to U.S. cybersecurity. And, in the aftermath of the attacks, Washington significantly stepped up its efforts to deal with the perceived cybersecurity "crisis."

Washington's post-September 11 "get tough" approach to cybersecurity was embodied in both legislative and executive action. On October 26, 2001, just a few weeks after the terrorist attacks, President Bush signed into law the USA PATRIOT Act. The Act empowers the United States government in its fight against terrorism by strengthening the federal government's surveillance powers (Title II); by enacting anti-money laundering provisions

12. UNITED STATES GENERAL ACCOUNTING OFFICE, INFORMATION SHARING: PRACTICES THAT CAN BENEFIT CRITICAL INFRASTRUCTURE PROTECTION, Oct. 2001, at 6 [hereinafter GAO Report].

13. Ron Dick, *A Message from Ron Dick, Director of the National Infrastructure Protection Center, available at* http://www.nipc.gov/about/about.htm. *See also* GAO Report, *supra* note 12, at 6.

to deny terrorists financial support (Title III); and by strengthening federal criminal laws against terrorism (Title VIII).

Several provisions of the USA PATRIOT Act are designed to deter and prevent "cyberterrorism" by strengthening existing criminal law.[14] In reality, however, these provisions simply strengthen the CFAA and thus seek to deter and prevent ordinary cybercrimes, such as hacking and denial of service, rather than focusing on acts of cyberterrorism undertaken to influence government policy. For example, the USA PATRIOT Act (1) amends the CFAA to increase the maximum penalty for hacking from ten to twenty years; (2) expands the CFAA's definition of "protected computer" to include many "computer[s] located outside the United States;" and, finally, (3) expands the CFAA's definition of the term "loss" to include "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service."[15]

Equally important, the USA PATRIOT Act's focus is on deterrence through criminal penalties, rather than prevention through added security. Yet one may question how practical it is to deter a teenage hacker, let alone an actual cyberterrorist. While stricter punishment for cyberattacks is a good thing, it may not prevent many future cyberattacks.

Addressing the "prevention" issue, a slew of cybersecurity-related bills are now pending in Congress. These include: (1) the Cyber Security Research and Development Act[16] (H.R. 3394); (2) the Cyberterrorism Preparedness Act of 2002[17] (S. 1900); and (3) the Cybersecurity Research and Education Act of 2002[18] (S. 1901). Introduced by the Chairman of the House Science Committee, House Bill 3394 earmarks $900 million to be divided between the National Science Foundation (NSF) and the National Institute of Standard and Technology (NIST) to establish various cybersecurity research grants. Senate Bill 1900 authorizes NIST to establish a nonprofit (and nongovernmental) consortium of academic and private sector experts to promulgate a set of "best practices" used to fight computer crime. The legislation calls for government implementation of these best practices with the hope that they will serve as a model for the private sector and envisions that the "best practices" will be required of companies that do business with the federal government. Finally, Senate Bill 1901 authorizes NSF and the National Security Agency to create new programs and fellowships to attract promising students to the field of cybersecurity and to offer incentives for teaching positions in the field.

Added government funding for cybersecurity is always welcome (except perhaps to the extent it reduces funding for other important projects to enhance the electronic marketplace and communications). It is of potential concern, however, if Congress seeks to establish "best practices" that companies must follow, as envisioned in Senate Bill 1900. Such a "one size fits all" approach may impose unnecessary levels of security costs, particularly on smaller companies who handle less sensitive information. A more nuanced, less regulatory approach, would be preferable.

14. *See* USA PATRIOT Act § 814, 115 Stat. at 382–84.
15. *See id.* § 814(c)-(d).
16. H.R. 3394, 107th Cong. (2001).
17. S. 1900, 107th Cong. (2002).
18. S. 1901, 107th Cong. (2002).

In addition to legislative activity, there also has been a flurry of activity in the executive branch. Indeed, several new cybersecurity-related posts have been created and filled in the last six months. Within ten days of the September 11th attacks, President Bush created the Office for Homeland Security and named Governor Tom Ridge as its Director. In his new, cabinet-level position, Ridge is responsible for coordinating the federal agencies' counterterrorism efforts to ensure domestic security. Shortly thereafter, National Security Council member Richard Clarke was tapped to serve as the President's Special Adviser for Cybersecurity. Clarke, who reports to Ridge, coordinates federal agency efforts to secure information systems as chair of the new, government-wide Critical Infrastructure Protection Board. The Board is expected to develop, among other things, a system that federal agencies can use to communicate information in times of crisis.[19]

The Administration has also announced several other steps to improve cybersecurity. The Department of Justice will staff a large computer crime fighting unit focused on computer intrusion and the theft of confidential information from the computer networks of high-tech companies. In addition, the Administration will be supporting two special initiatives: GovNet and Cyber Corps. GovNet will provide a means of securing sensitive government communications while Cyber Corps, sponsored by the Department of Defense and NSF, is a Clinton-era program designed to encourage engineering students to take government jobs helping to protect the nation's defense and telecommunications networks against cyberterrorism.[20]

In addition to these somewhat piece-meal efforts to ramp up cybersecurity in the United States, a more comprehensive cybersecurity strategy is expected to be announced in June 2002. Among other things, the Administration's strategy will outline "market based" motivations for companies to fortify their cybersecurity.[21] Such an approach would be consistent with the need to ensure that the cybersecurity response, while forceful, is proportionate to the risk and does not unduly burden the Internet.

II. Other Governments' Response to the Cybersecurity Threat

While much attention has focused on domestic efforts to protect against cyberattacks, those beyond the Beltway also are striving to meet the challenge of cyberterrorism and cybercrime. One of the most significant international developments to date is the Council of Europe (CoE) Convention on Cybercrime,[22] the first multilateral treaty to address crim-

19. Finally, the responsibility for global counterterrorism efforts has been placed on General Wayne Downing, former Commander-in-Chief of the United States Army Special Forces. Now the National Director and Deputy National Security Advisor for Combatting Terrorism, Downing, like Clarke, reports to Ridge.

20. Roy Mark, *GOVNET Aims To Protect Critical IT Functions From Attacks*, *available at* http://dc.internet.com/news/article/0,1934,2101_900961,00.html; Omer Gillham, *Cyber Corps Students to Fight Terror*, TULSA WORLD, Jan. 21, 2002, *available at* http://www.cis.utulsa.edu/InTheNews/cybercorpsstudentstofight terror.asp. A copy of the government's request for information seeking suggestions from the U.S. telecommunications industry regarding development of the special GOVNET telecommunications network is available at http://www.fts.gsa.gov/govnet/govnet.doc.

21. As the private sector operates most of the nation's critical infrastructures, it is on the "front lines of homeland security," according to John Tritak, Director of the Critical Infrastructure Assurance, Office of the Department of Commerce. *See* Pike & Fischer Report, *Official Says Nation's Economic Security Primarily on the Shoulders of Private Sector*, Feb. 28, 2002.

22. Convention on Cybercrime, Nov. 23, 2001, Eur. T.S. No. 185, *available at* http://conventions.coe.int/Treaty/EN/projets/FinalCybercrime.htm.

inal activity on computer networks. CoE is a forty-three-member pan-European international organization that traditionally has dealt with human rights issues in Europe and also has served as the forum for drafting pan-European law enforcement treaties.

The CoE cybercrime treaty was in the works long before September 11. Indeed, the CoE began drafting the convention several years ago, and concluded the negotiations in the summer of 2001. The United States signed the treaty on November 23, 2001, and the Department of State currently is preparing a ratification package for Senate consideration.

The purpose of the CoE treaty is threefold: (1) to harmonize different nations' substantive law pertaining to cyber crime; (2) to define investigation and prosecution procedures using electronic means; and (3) to establish a system of international law enforcement cooperation to promote the detection of international crimes and enforcement of criminal law in cases that involve computer networks and require substantial cross-border corporation between law enforcement agencies.[23]

The CoE treaty was itself a response to cybercrime and was intended to protect our networked information systems from cyberattacks. Yet, in actuality, it may burden the very systems it seeks to protect by imposing substantial costs upon Internet Service Providers (ISP), Internet users, and others. For example, as part of its effort to harmonize the definitions of cybercrime offenses in different nations, the cybercrime treaty mandates that signatories to the treaty criminalize the act of accessing a computer "without right."[24] At first glance, this provision appears simply to protect information systems against hack attacks, denials of service, and other acts perpetrated by accessing a computer "without right." However, this broad provision could impose a significant burden on Internet-mediated communication, as it could be interpreted and implemented in ways that would appear to criminalize a wide array of ordinary Internet activity when undertaken without specific permission. The CoE provision makes the simple act of *accessing* a computer the basis of a crime and fails to require that the actor access the computer with the intent to injure, or with the effect of injuring, the computer or the data stored therein. Accordingly, the legality of ordinary activities, such as placing a "cookie" on a Web surfer's computer, was called into question. While language in the Convention's Explanatory Memorandum seeks to address these concerns, the ability of treaty text to respond to the complexities of rapidly evolving technology and practice remains a question for many.

A similar problem arises under the CoE treaty provisions addressing private assistance to law enforcement to facilitate the interception, preservation, and seizure of computer data and transmissions. In particular, the CoE treaty empowers law enforcement authorities to compel an ISP to provide data "within its existing technical ability."[25] This raises significant concerns within the private sector that private entities could face an open-ended requirement to divert information infrastructure, servers, storage and information technology staff to support interception and preservation, at substantial cost to (and requiring disruption of) their ordinary business activities. Moreover, the actual costs to ISPs of implementing this CoE provision are unclear. While the U.S. and French governments generally reimburse ISPs when they are compelled to provide technical assistance to law enforcement authorities, other countries generally do not.

23. *Id.* preamble.
24. *Id.* ch. II, § 1, art. 2.
25. *Id.* § 2, art. 21.

III. Corporate Response to the Cybersecurity Threat

As with the government efforts described above, corporate efforts to improve cybersecurity may itself burden the Internet. In the process of determining what procedures to adopt to protect against cyberattacks, corporations must take into account not only cost considerations, but also privacy concerns and potential liabilities arising out of their actions. Below, we consider several steps corporations are taking to bolster their defenses against cyberattack.

A. Information Sharing

Private sector organizations can promote cybersecurity through their participation in the Information Sharing and Analysis Centers discussed above. ISACs promote private sector understanding of cybersecurity risks by providing a forum within which corporations can share—either among themselves and/or with government officials—information about cyberattacks, vulnerabilities, threats, intrusions and anomalies. ISACs already have been developed for various industries including: financial services, telecommunications, information technology, and electric power. Some ISACs, such as the financial services ISAC, are intended to function as partnerships between government and industry, although it is unclear whether much information flows from the private sector participants to government officials.

Unfortunately, participation in ISACs is not without risks. First, ISAC participants should consider the antitrust implications of this collaboration among competitors. Legislation has been introduced in the House to promote participation in ISACs and the associated information exchange.[26] It provides that antitrust law does not apply to conduct undertaken solely for the purpose of, and limited to (1) facilitating the correction of cybersecurity-related problems; or (2) communicating or disclosing of information to help correct or avoid the effects of a cybersecurity-related problem.[27] However, the last major action on this bill was taken on July 10, 2001, and considerable time is likely to pass before this, or similar, legislation is adopted.

Second, a corporation's business proprietary information potentially could be disclosed pursuant to a Freedom of Information Act (FOIA) request if the government is an ISAC participant. To alleviate this concern, House Bill 2435 specifically provides that, with certain exceptions, identifiable information that is voluntarily provided to the government via an ISAC shall be exempt from disclosure under FOIA. However, as noted above, House Bill 2435 is likely to remain pending for some time.

Corporations also should consider the potential for liability arising out of ISAC participation and should determine whether or not the ISACs in which they participate are structured to minimize these risks. For example, ISAC participants may incur liability for providing inaccurate information; failing to protect sensitive ISAC information; failing to heed a warning issued by the ISAC; or failing to disclose information that could have prevented a cybersecurity attack. Finally, ISACs themselves could potentially be exposed to liability for providing inaccurate information to members; failing to detect a breach; failing to share or disclose information; failing to protect anonymity (raising privacy concerns); or failing

26. Cyber Security Information Act, H.R. 2435, 107th Cong. (2001).
27. *See id.*

to protect proprietary data. Of course, ISACs can minimize their own exposure to liability via ISAC membership agreements and member operating rules.

B. Data Security Measures

1. *Encryption*

Encryption is an important element of data security; however, its import, export, and use are heavily regulated in a number of countries. Accordingly, global corporations often cannot widely deploy encryption products to foreign offices without significant costs.

While the United States has progressively relaxed its restrictions on encryption export since the mid-1990s, many other countries – most notably France, China and Russia – have maintained stringent rules on the import, export, and use of even the most basic encryption items. Companies with a global presence that rely upon encryption to, for example, secure inter-office communications, must pay careful attention to the legal rules in multiple countries to avoid engaging in unauthorized, and potentially illegal, encryption import, export, and use. The widespread dissemination of encryption technology has led many lawmakers to believe that strong encryption controls, such as those maintained in Russia, are practically unenforceable. However, law-abiding companies that wish to use strong encryption for data security purposes still must commit the time and resources to obtain the necessary authorizations and licenses prior to import, export, and use of encryption items. The need to acquire and deploy strong encryption is another burden on the growth of the Internet.

2. *Information Security Programs*

Information security programs are another important element of data security. In order to protect data against cybersecurity threats, many businesses have begun to develop and implement information security policies. Moreover, in some regulated industries, including the financial services and health care industries, federal law requires (or will soon require) the development of information security programs.

For example, under interagency guidelines promulgated by the federal banking agencies pursuant to the Gramm-Leach-Bliley Financial Services Modernization Act of 1999[28] (GLB), financial institutions are required to establish written information security programs as part of their efforts to maintain the confidentiality of customer information. The interagency guidelines require, *inter alia*, that financial institutions identify and assess risks to information security and confidentiality; write a risk management plan; implement and test the plan; and adjust the plan in response to changes in the technology, the sensitivity of customer information, or the threat to the confidentiality of customer information.[29]

Just as GLB protects personally identifiable financial information, the Health Insurance Portability and Accountability Act of 1996[30] (HIPAA) protects certain health care information. In particular, protected health care information that is electronically stored, maintained or transmitted must be protected to ensure privacy and confidentiality. In contrast to the relatively flexible approach that the banking agencies took when developing their GLB implementing regulations, the Department of Health and Human Services has pro-

28. 12 U.S.C. § 1811 (1999).

29. Department of Treasury, *Interagency Guidelines Establishing Standards for Safeguarding Customer Information*, 12 C.F.R. ch. I, pt. 30, app. B, et al., Feb. 1, 2001.

30. Pub. L. 104-191, 110 Stat. 1936 (1996).

posed rather prescriptive information security standards to implement HIPAA. The proposed information security regulations require covered health care providers to take specific steps to protect the security and confidentiality of protected health information.[31]

The interagency information security guidelines promulgated pursuant to GLB take a sensible approach to cybersecurity. They set broad parameters within which financial institutions must operate and then permit the market to determine precisely how much cybersecurity is necessary and cost-effective within those parameters. However, the proposed information security regulations to implement HIPAA indiscriminately mandate that health care providers follow numerous particular security practices, making it nearly impossible for health care providers to comply with all of the regulations in a cost-effective way. Accordingly, these standards are likely to impose an enormous financial burden on covered health care providers.

Organizations implementing information security programs must be concerned not only with the substantial immediate costs, but also with the potential for eventual liability. For example, organizations posting their information security policies to their Web sites in order to build customer trust should be aware that failure to comply with the stated terms of a posted security policy could lead to legal exposure.

C. Employee Monitoring

Corporations that monitor use of their computer systems to enhance security must pay careful attention to employee privacy protections, particularly in the European Union (EU). In the EU, employees generally have a right to privacy at the workplace, but that right is not absolute. In the EU, companies generally are permitted to monitor employees if their monitoring is systematic, general and proportional. However, in all Member States where the company has a fixed establishment (or, for a U.S. company, in all Member States in which the company has a server) it must, in order to comply with the Data Protection Directive,[32] notify the data protection authorities of its computer monitoring system. And, in order to monitor a particular individual, the corporation must have a justified suspicion about the individual and must obtain approval from the Worker's Council under the labor laws of most Member States.

The rules in France are even stricter. France's top court (the Cour de Cassation, Chambre Sociale) ruled in October of 2001, that employers do not have the right to read their employees' private electronic mail or other personal computer files when it is clear from the header of the e-mail or the name of the file that the information contained therein is strictly private.[33] This decision could raise the cost of monitoring for multinational companies as security professionals discontinue use of system-wide security tools for fear that some of the employees whose online behavior is examined will turn out to be French.

In light of the EU's privacy protections, global companies doing business in the EU will want to consider adopting a code of conduct to govern their monitoring efforts. Such a code of conduct can be used to establish, if necessary, that the corporation's monitoring is systematic, general and proportional. Among other things, such a code of conduct might

31. Security and Electronic Signature Standards, 63 Fed. Reg. 155 (proposed Aug. 12, 1998) (to be codified at 45 C.F.R. pt. 142).

32. Council Directive 95/46, 1998 O.J. (L 2) 13.

33. *See* Nikon France v. Onos, Cass. Soc., Arret No. 41-6410/2/01.

provide that: (1) network monitoring tools are to be used as necessary to protect the network from security breaches; (2) comprehensive monitoring should, as much as possible, be performed automatically, rather than by persons; and (3) the corporation should avoid unnecessary breaches of privacy and/or public disclosure of information obtained through monitoring.

IV. Conclusion

September 11 was a wake-up call on security issues for many in government and industry, and it has since been used as the impetus for action on cybersecurity in particular. Although the United States did not experience a cyberattack on September 11, the events of that day have triggered a concerted effort to achieve heightened cybersecurity.

In deciding what cybersecurity measures to adopt, the clear benefits of improved cybersecurity must be balanced against competing considerations, including the cost, loss of privacy, and potential liability associated with many cybersecurity measures. If we fail to consider these – often-unintended – results of increased cybersecurity, we may unduly burden our ability to achieve globalization via the Internet, one of the true promises of the Information Age.

One may ask whether or not economics, alone, will be a sufficient motivator for corporations to adopt good information security measures. To the extent that companies are aware of information about economic risks, they can be expected to respond to that information. For example, if a bank learns that a hacker has stolen funds from another bank, it is likely to take added security precautions to protect itself from such theft. Companies will evaluate the cost of various security measures against the probability of cyberattacks and the magnitude of loss that may result. Based on information about the security risks, and the costs, financial and otherwise, of taking various security measures, companies will seek to achieve the greatest increase in security at the lowest cost. This should result in relatively good decisions about the appropriate level of security.

However, a key caveat for public policy decision-makers is whether corporations (1) have adequate information, and (2) have adequate incentives to consider "externalities," e.g., the impact upon other companies and individuals in the society if the company's security measures are insufficient. As efficient markets depend on information, it is clear that, at the very least, information sharing, whether through ISACs or through other channels, is important if corporations are to find a socially optimal level of investment in security.

As to the externalities, public decision-makers must consider, when deciding whether to encourage or mandate security measures, the level of risk to critical infrastructure that may arise from security flaws in particular sectors. Is there a real threat to critical infrastructure or is the risk simply that a company will suffer economic harm? The probability of lower impact events (e.g., hacking and denial of service) appears to be much higher than the probability of an event with a severe impact on the Internet or telecommunications grid.

Heightened cybersecurity via government regulation may nonetheless be warranted in light of associated externalities and risks that are not adequately considered by the private sector. Currently, the Administration is relying on "jaw-boning" of U.S. industry. However, to the extent that companies underinvest in cybersecurity, it ultimately may be necessary to create incentives to get industry to respond to the need for greater cybersecurity (as the Administration is already contemplating) or, if the problem is severe enough, to enact regulations or legislation addressing this issue. Nonetheless, any governmental mandates that are imposed should be taken as a last resort, and should minimize the burden placed on industry, to ensure that the security cure is not worse than the cyberattack disease.