Should Vulnerability Be Actionable?
Improving Critical Infrastructure Computer Security with Trade Practices Law

Jane K. Winn

Director & Professor
Shidler Center for Law, Commerce & Technology
University of Washington School of Law
William H. Gates Hall
Box 353020
Seattle WA 98199-3020

jkwinn1@u.washington.edu

Jane K. Winn is Director and Professor, Shidler Center for Law, Commerce & Technology, at the University of Washington School of Law. She is author of The Law of Electronic Commerce (with Benjamin Wright, 2001) and Electronic Commerce (with Ronald Mann, 2002). She is a Senior Fellow in the Faculty of Law, University of Melbourne, Australia, and a member of the American Law Institute. Her research focuses on commercial law and information technology issues in the US, European Union and Greater China. She has published many articles on electronic commerce law, which are accessible at www.law.washington.edu/Faculty/Winn/.

Professor Winn was a member of the faculty of the Dedman Law School of Southern Methodist University in Dallas, Texas from 1989 to 2001, and a visiting professor at the University of California – Berkeley School of Law in Spring 2002. She holds a J.D. degree cum laude from Harvard University and B.Sc. degree in Economics with First Class Honours from Queen Mary College of the University of London.

ABSTRACT

If the current level of security for critical infrastructure information systems is inadequate, then law reform could provide new incentives to increase investment in cybersecurity. Given the lack of political support for new regulatory mandates or expansion of tort liability to spur investment in cybersecurity, a self-regulatory strategy based on a program of voluntary disclosures regarding compliance with security standards combined with trade practices law as an enforcement mechanism might be a more politically viable alternative. Just as a voluntary disclosure system combined with FTC deceptive trade practices enforcement now provides some protection for information privacy rights of US consumers, a voluntary disclosure system regarding cybersecurity practices combined with competitors acting as vicarious avengers of the public interest could provide some incentives to increase investment in cybersecurity. If it is combined with education programs to increase public demand for cybersecurity, increased spending on basic research in computer security, a broader array of technical standards, and more effective security products for critical infrastructure owners to implement, then a self-regulatory system based on trade practices law and voluntary disclosures might be an effective substitute for direct government regulation of the security of critical infrastructure information systems.
INTRODUCTION:
LAW REFORM STRATEGIES FOR IMPROVING CYBERSECURITY

The United States must find ways to improve the security of its critical infrastructure information systems, notwithstanding the fact that the infrastructure at issue is largely under the control of private parties, and there is little public support for sweeping new regulatory regimes to mandate improved security. Given these constraints, one way critical infrastructure protection (CIP) can be improved is by increasing private incentives for greater investment in security and by establishing private enforcement mechanisms to monitor compliance. This article suggests that trade practices law could be used to provide new private incentives to improve the security of critical infrastructure information systems in much the same way that it has been used in recent years to improve the protection of information privacy.

Critical infrastructure consists of “systems...so vital to the United States that the incapacity or destruction of such systems...would have a debilitating impact on security, national economic security, national public health or safety...”\(^1\) Both public and private sectors increasingly “depend on an interdependent network of critical physical and information infrastructures, and a continuous national effort is required to ensure the reliable provision of cyber and physical infrastructure services critical to assure continued availability of critical infrastructure assets.” The security of the computer networks that support the operation of critical infrastructure is often referred to as “cybersecurity.” (Department of Homeland Security, 2003). This article considers whether trade practices law might be used as a tool to increase the level of cybersecurity maintained by those in control of critical infrastructure assets.

Most US critical infrastructure was put in place before the current threat of terrorism was recognized, and so in light of threats that are now recognized, much of that infrastructure has inadequate security. The problem is particularly acute with regard to computer networks, because networking has expanded more rapidly than security technologies, resulting in computer networks that are more insecure as they grow more pervasive. (Computer Science and Telecommunications Board, 2002, at 2). One way to raise the current level of protection is to use law to create new incentives to increase investment in CIP. These incentives could take the form of direct regulatory mandates or a new form of tort liability; however, these alternatives are unlikely in the current political climate and furthermore may be inappropriate in light of current technology. US government policy favors working through public-private partnerships to increase investment in security in tandem with increasing understanding of security technologies and institutional arrangements for implementing those technologies effectively. (The White House, September 2002, at 10). But as security experts are fond of pointing out, “Security is a chain; it’s only as strong as the weakest link.” (Ellison and Schneier, 2000, at 1). In other words, in order for the public to benefit from improved cybersecurity, some minimum level of computer security will have to be mandated. Given that the political will to enact new mandates seems to be lacking, this article considers whether existing trade practices law, with minor adjustments, might provide stopgap support for improved cybersecurity.

\(^1\) Critical Infrastructures Protection Act of 2001, Section 1016(e) of Public Law 107-56 (42 U.S.C. 5195c(e)).
If public demand for CIP increases, then owners of critical infrastructure might find a benefit from advertising themselves as providing adequate protection of their assets. If owners of critical infrastructure market themselves as providing adequate cybersecurity, then trade practices law could be used to police the accuracy of those claims. If inaccurate claims of adequate cybersecurity are deemed to be a form of false advertising, then the primary enforcement mechanism would come from competitors acting as “vicarious avengers” of the public’s interest. (McCarthy, 2003, § 27.1). Owners of critical infrastructure systems would then have an incentive to monitor each other’s security and report breaches likely to place those systems at risk. Such a system for promoting private monitoring of security practices could be one element of a system of public and private incentives to improve the security of critical infrastructure systems, offsetting the absence of direct government regulation of security implementation decisions.

Increasing the security of critical information infrastructures under private control is a complex problem for which there are no simple solutions. Not only are simple regulatory mandates not a politically viable alternative at this time, even if they were an option, they might still be inappropriate in light of the uncertainty surrounding many basic issues in the science of cybersecurity. (Schneider, 1999, at 250). Simply assigning liability for poor security before effective engineering solutions have been developed will not achieve the desired result. Self-regulation is not only appealing from a political perspective, it may even be superior from a practical perspective, if it provides balanced incentives to develop and implement new technological solutions to existing security problems. In order to achieve this outcome, self-regulation would have to be combined with standard developing and certification programs to clarify which technological solutions are appropriate, increased public demand for improved critical infrastructure protection, and a system of voluntary public disclosure of compliance with current standards. If a such a system of continuous development of technical standards, increased public demand and voluntary disclosure can be put in place, then deceptive trade practices suits brought by competitors could provide an effective private enforcement mechanism to monitor such a self-regulatory regime.

**LEGAL AND ECONOMIC INCENTIVES TO IMPROVE CYBERSECURITY**

Under US law today, there is no general legal obligation to make computer networks secure. Computer security is difficult and expensive to achieve, and it is difficult to calculate the probability that any particular computer network will suffer harm as a result of poor security. In the absence of any clear legal mandate to achieve a particular level of computer security, and the face of an uncertain business case for increasing investment in computer security, the current apparently poor state of computer security is not surprising. During the Clinton Administration, the President’s Commission on Critical Infrastructure protection was established by Executive

---

2 There are specific obligations imposed on specific sectors of the economy, such as military contractors, financial institutions and telecommunications, to provide some level of network security. See, e.g., Federal Financial Institutions Examination Council IT Examination Handbook, Information Security Booklet, available at [http://www.ffiec.gov/ffiecinfobase/html_pages/infosec_book_frame.htm](http://www.ffiec.gov/ffiecinfobase/html_pages/infosec_book_frame.htm) (accessed June 15, 2004) (describing the criteria used by auditors to assess the adequacy of information security used by regulated financial institutions). It is also possible that a failure to secure a network that harms another might give rise to negligence liability, but there are not yet any cases so holding.
In 1997, the Commission produced a report Critical Foundations – Protecting America’s Infrastructure. (President’s Commission on Critical Infrastructure Protection, 1997). The Commission divided its work into five sectors: information and communications; banking and finance; energy; transportation; and emergency services. The report set forth the Commission’s conclusions: dependence on critical infrastructure is increasing, as are the threats to it, but not enough is being done to reduce its vulnerabilities. This was due to lack of awareness and the lack of a nation-wide plan for addressing the problem, and the Commission recommended a coordinated effort by both public and private sectors to respond. In response to these recommendations, the FBI set up the National Infrastructure Protection Center (NIPC) to serve as a national clearing house for information about critical infrastructure protection and efforts to reduce vulnerabilities. (Gravell, 1999, at 407).

Bush Administration policy regarding electronic commerce issues has been shaped by the need to respond to the September 11 terrorist attacks. In response to the terrorist attacks in September 2001, Congress passed the USA Patriot Act\(^4\) and the Homeland Security Act.\(^5\) In July 2002, the Homeland Security Advisory Council issued a National Strategy for Homeland Security. (The White House, July 2002). In September 2002, the President’s Critical Infrastructure Protection Board (PCIPB) issued a draft for comment of a National Strategy to Secure Cyberspace.\(^6\) This document identifies strategic network security issues on five different levels: home users and small businesses; large enterprises; critical sectors in government, higher education and the private sector; national issues; and global issues. In February 2003, the final National Strategy to Secure Cyberspace report was issued.\(^7\) While the final report emphasized public-private cooperation was key to protecting critical infrastructure, it did not contain any significant law reform proposals to increase incentives for private sector investment in information security. The final recommendations focus on initiatives to be taken by the Department of Homeland Security (DHS), and offer encouragement to various private sector organizations to improve their security architecture as well as their education and training programs to raise awareness. Public and private sector actors are encouraged to develop and participate in “information sharing and analysis centers.” In June 2003, a National Cyber Security Division was established within the Information Analysis and Infrastructure Protection Directorate of DHS to support those information sharing and analysis efforts. (Department of Homeland Security, 2003).

WHAT IS CYBERSECURITY AND WHY IS IT SO HARD TO ACHIEVE?

In analyzing information system security risks, it is useful to distinguish vulnerabilities, which are weaknesses that might be exploited to violate the security of the system; threats, which are circumstances or events likely to cause damage by violating security; and safeguards, which are techniques or procedures that reduce vulnerabilities and make threats less likely. (Summers, 1997, at 72). The threats to networked computer systems are growing for a number of reasons, as are their vulnerabilities. Just as other computer applications have grown more powerful in

---


\(^7\) Available at http://www.whitehouse.gov/pcipb (accessed June 15, 2004).
recent years, so have software tools used to attack networks. The level of technological sophistication required to launch an attack on a computer system has fallen as user-friendly attack tools with point-and-click interfaces have become available over the Internet and can be used by almost anyone.\(^8\)

Computer security cannot be achieved through the installation of particular pieces of software and hardware alone because it is an attribute of a system, including buildings housing it, and the functions performed by people using it. (Kiefer, et al., 2004, at 4-9). As networks grow in size and complexity, the problems of securing them increases as well. “Complexity is the enemy of security” is one of the maxims of computer security, because the defender has to block all known attacks while the attacker only has to find one unblocked means to attack. (The Economist, 2003). Merely buying firewall software or establishing a system of strong access controls based on biometrics cannot make a system of networked computers secure because vulnerabilities elsewhere in the system may negate the effect of isolated pieces of security technology. (Schneier, 1996).\(^9\) The security of much of the software currently in use is abysmal, and even the security of well-designed products can be undermined because they are improperly configured or used.\(^10\) Furthermore, computer security is plagued by the problem of “false positives” in testing for security flaws. There is no reliable means of proving that an information system has no security flaws, so the best that computer scientists can hope for is showing that a system can resist all known forms of attack. Showing that a system withstands all tests of its security might seem to show that it is adequately secure, yet the tests may fail to detect errors in the threat model, system design, software or hardware implementation, or the human oversight of the system. (Schneier, 1996, at 3).

Even a flawed computer security system may still degrade performance for system users, however. Many security technologies make computers cumbersome to use and consume capacity, making other functions difficult to perform. For example, a rigorous system of access controls will normally produce a certain level of false negatives, in which authorized users are refused access to the system in error.\(^11\) Another example of this problem is cryptographic systems which depend on sophisticated mathematical calculations that consume a great deal of processing capacity.

Even organizations that are committed to improving the security of their information systems face formidable challenges. These include the difficulty and uncertainty of testing the security of computer systems; the complexity of the challenges facing engineers trying to secure


\(^9\) Cryptography is one security technology that is used to improve cybersecurity; Schneier analyzes problems of implementing cryptographic systems within the larger context of computer security.

\(^10\) Bruce Schneier, June 25, 2003 testimony.

\(^11\) Biometric systems compare a sample taken in the past with one taken at the time authentication is sought, so temporary conditions such as weight gain or loss may cause the authentication system to reject a user because the variation between the current sample and the historical sample is too great. Increasing the biometric identification system’s tolerance of variations will increase the rate of false positives, in which unauthorized users are mistakenly granted access and erode the security of the system.
global computer networks; the lack of sophistication of many purchasers of networked information technology systems that make up part of the network; and in some cases, the simple absence of adequate technological solutions to many of the security problems now facing network participants. (Schneider, 1999). More sophisticated and powerful security technologies will need to be developed before information system operators will be able determine their tolerance for cybersecurity risks and then purchase and install appropriate technology to achieve their risk management objectives. The engineering problems facing those trying to develop such technologies are compounded by the fact they will often be deployed in open, public, global computer networks built with technologies that are not completely interoperable.

Computer security is not an absolute that can be guaranteed or delivered; rather, a computer system can be made as secure as possible by reducing its vulnerability to all known threats. Because it is not usually feasible to implement all known safeguards, many decisions about computer security must be the result of weighing estimated costs and benefits in light of expected uses of the system in question. Outside the world of a tiny number of truly “mission critical” military applications, financial constraints play an important role in determining how much security will be sought. Management of computer security risks requires a program of risk assessment, combined with a method of valuing assets, so that decisions can be made about appropriate levels of investment in whatever security technologies are available. (Denning, 1998, at 385). Some organizations have the option of participating in the “Information Sharing and Analysis Centers” (ISAC) organized by DHS, which can provide them with up to date and useful information about cybersecurity threats. An essential element of any program to improve cybersecurity must be expanded research programs that lead to fundamental advances in computer security. The field of computer security is replete with “unsolved problems” and the growing complexity of networked computer systems means that that gap between the efficacy of the solutions currently available and the magnitude of the cybersecurity risks that network operators face is likely to grow, not shrink, in the near future.

MARKET INCENTIVES TO IMPROVE CYBERSECURITY

Owners of critical infrastructure have the same incentives to protect their computer networks as they have to protect their other assets, and it is possible that those owners are currently making appropriate investments in cybersecurity. Given the magnitude of “unsolved

---

12 There remains a need for further basic research to address unsolved engineering problems in computer security.


14 Richard D. Pethia, Director, CERT Centers, Software Engineering Institute, Carnegie Mellon University, Cyber Security – Growing Risk from Growing Vulnerability, Testimony before House Select Committee on Homeland Security, Subcommittee on Cybersecurity, Science, and Research & Development, June 26, 2003 (“Richard D. Pethia, June 26, 2003 testimony”), available at http://www.cert.org/congressional_testimony/Pethia_testimony_Sep26.html (accessed June 15, 2004). Other elements in include: expanded research programs that lead to fundamental advances in computer security; a larger number of technical specialists who have the skills needed to secure large, complex systems; and increased and ongoing awareness and understanding of cyber-security issues, vulnerabilities, and threats by all stakeholders in cyber space.

15 “Our current solutions are not keeping pace with the increased strength and speed of attacks…” Richard D. Pethia, June 26, 2003 testimony.
problems” in computer security and the pervasiveness of security problems with commercial, “off-the-shelf” information technology products, a low level of investment in computer security might be completely rational for an individual organization, given that spending more on computer security might produce negligible results. However, even if the decision not to invest significant resources in computer security is a rational individual choice, in aggregate, such decisions leave the critical infrastructure of the United States vulnerable to cyber-attacks and are not acceptable as a matter of national security policy.

There may be several other reasons that the operation of markets for computer security products and services fails to produce socially optimal levels of investment in cybersecurity. The fact that computer security technologies are generally expensive to acquire and difficult to implement effectively has reduced demand for such technologies, which in turn has limited investment in basic computer security research. If security technologies cannot be developed, tested and brought to market quickly, then there may be a considerable lag between any increase in demand by network operators for improved security technology and the delivery of technologies to meet that demand. In addition, collective action problems and network externalities may contribute to inadequate levels of investment in security for networked information systems.

Collective action problems arise when members of a group would benefit by a particular course of action, but individual members of the group each refrain from taking that course of action because there is no way to be certain the other members of the group will follow suit. In the absence of a legal mandate to require making a particular investment in security or meeting a particular standard, individual network operators will be unwilling to bear the cost of making major improvements in the security of their own systems without any assurances other network operators will do likewise. This is particularly true if the cost of upgrading the security of one system within a network outweighs the benefits that accrue to the owner of the system in the absence of similar investments by other network participants. One common mechanism for overcoming collective action problems is to mandate the course of action necessary to achieve the collective benefit. Universal and mandatory minimum levels of computer security might be established by government regulation of computer networks, a subject which is considered further in the following section.

Networks, including information technology networks, have special characteristics that often make them resistant to change. These special characteristics can often be analyzed as a form of market “externality” that arises when one market participant’s actions affect other market participants without compensation being paid. (Shapiro and Varian, 1998; Mann and Winn, 2002). Networks may evidence positive or negative externalities. If the value of being in a network is increased to those already in the network every time a new person joins the network, then adding a new participant to the network has positive network externalities. A common form of negative network externality, known as a “lock-in”, arises when the cost of making changes to some part of a network system is so expensive that participants in a network refrain from making even changes that would improve the operation of the network. (Liebowitz and Margolis, 1999). To the extent that security technologies have to be implemented network-wide in order to be effective, there will be a risk that individual network operators will refrain from investing in improved security if they cannot be certain other network participants will follow suit. One way
to overcome network effects that inhibit investment in improvements to the network is to find a way to build consensus among market participants with regard to the next iteration of technology that they all will adopt. This can be done in a variety of ways, including effective standard developing efforts, marketing or government intervention to focus attention on a particular standard or technology.

One way to try to overcome the market failures which currently seem to plague markets for computer security products would be to increase demand from the end users of critical infrastructure services for greater cybersecurity protections, which in turn would pressure owners of critical infrastructure to increase their investment in security. Raising public awareness of the importance of cybersecurity is an essential element of any comprehensive plan to improve the protection of critical infrastructure. (White House, September 2002)

Public knowledge that an owner of critical infrastructure has suffered a security breach that could have been prevented will damage the reputation of that organization among its customers and investors. Increased public demand for security can only create market pressures that will produce changes in investment decisions if the public has a way of knowing when security is inadequate, however. In the absence of a clear duty to disclose, organizations tend not to disclose information about security breaches, both to avoid damage to their public image and to reduce the risk of copy-cat attacks. In 2003, the Congressional “Corporate Information Security Working Group” debated whether public companies should be required to conduct annual information security audits and report what they find in their annual filings with the Securities and Exchange Commission. Increased public demand and public disclosure will only be effective at raising the level of investment in computer security if more effective computer security products are developed, however.

REGULATORY MANDATES TO IMPROVE CYBERSECURITY

One organization that does not secure its computer networks is not only making a decision about its own tolerance for risk, it is externalizing some of the costs of its bad security on other participants in the network. One way to deal with organizations that now externalize the costs of their own inadequate security is to create a new liability rule that will force them to internalize the costs of their computer security decisions. This liability rule might take the form of a regulatory mandate enforced by agency action, or a duty that establishes a private cause of action such as a negligence claim. In the absence of such a mandate, the overall level of computer security will suffer even if only a handful of organizations refuse to make adequate investment in security. This is because of the interdependence of organizations participating in the network, which together make up the “links in the chain” that determine the security characteristics of the network as a whole.

At present, US government mandates regarding computer security do not establish a general mandate to maintain adequate security. Rather, they follow the same kind of “sectoral” approach that has long been noted with regard to US information privacy law. (Schwartz and Reidenberg, 1996)\footnote{This study describes the US “sectoral” approach to information privacy as opposed to the more universal approach taken in the European Union.} For example, defense contractors, telecommunications service providers and public utilities\footnote{US Federal Energy Regulatory Commission, Notice of Proposed Rulemaking 31 July 2002 Appendix G: Security Standards for Electric Market Participants. 67 Fed. Reg. 55452, August 29, 2002.} all have specific computer security obligations that apply only to organizations within that industry. In addition, specific information privacy laws include provisions that mandate maintenance of appropriate levels of computer security in order to guarantee the privacy of particular categories of information. The Gramm-Leach-Bliley Act imposes a duty on financial institutions to ensure the security and confidentiality of customer records; to protect those records against any anticipated threats or hazards to their security and integrity; and to protect them against unauthorized access that could result in substantial harm or inconvenience to the customer whose information is contained in the record.\footnote{Pub. L. No. 106-102 Section 501, 113 Stat. 1338, 1346 (1999), codified at 15 U.S.C. § 6801 (2004).} The Health Insurance Portability and Accountability Act\footnote{Pub. L. No. 104-191, 110 Stat. 1936 (1996), codified at 42 U.S.C. § 1320d-2 (2004).} and the Children’s Online Privacy Protection Act\footnote{Pub. L. No. 105-277, 112 Stat. 2681-728 (1998), codified at 15 U.S.C. § 6501 (2004).} create similar duties to maintain the security of particular types of personal information.

The US government could intervene by mandating a high level of investment in computer security, and conditioning participation in computer networks on compliance with that mandate. Any attempt simply to reverse the current entitlement to build insecure networks and connect them to critical infrastructure, which now allows most of the costs of poor security to be externalized onto other network participants, is sure to encounter stiff resistance from the critical infrastructure owners that would be affected for both political and technological reasons. Imposing such a mandate would have major political ramifications because the financial consequences of imposing a new duty could be staggering. As a result, neither Congress nor the Bush Administration seems to have any enthusiasm for demanding increased investment in computer security in order to improve the security of critical information infrastructure.

The technological obstacles to such a reverse in underlying entitlements are at least as enormous as the political obstacles. There is no simple, obvious solution available at present for the current problems with network security, and no real likelihood that one will emerge in the near future. Creating liability for inadequate security when there is no obvious, responsible course of action network operators can take to avoid that liability will simply reduce the size of the network as operators withdraw. A strategy more likely to succeed would be some combination of incremental increases in the minimum level of cybersecurity that will be tolerated either by regulators or prospective plaintiffs, together with direct government subsidies of basic research,\footnote{Richard D. Pethia, June 26, 2003 testimony. Pethia describes the research that is needed in these terms: It is critical to maintain a long-term view and invest in research toward systems and operational techniques that yield networks capable of surviving attacks while protecting sensitive data. In doing so, it is essential to seek fundamental technological solutions and to seek proactive, preventive approaches, not just reactive, curative approaches.} so that by the time high levels of cybersecurity were mandated, technological
solutions would be available. Such an incremental strategy would create incentives for the production of more sophisticated technologies at the same time it creates incentives for network operators to implement them.

One way to increase investment in computer security basic research other than by direct government subsidies is to channel US government procurement spending toward improved computer security products and to promote the development of public standards for computer security through the work of the National Institute for Standards and Technology (NIST). The National Defense Authorization Act, Fiscal Year 2001,\textsuperscript{25} included the Government Information Security Reform Act (GISRA) which requires federal agencies to assess information security risks, report on the status of their information security efforts and include security matters in requests for funding. The E-Government Act of 2002\textsuperscript{26} included the Federal Information Security Management Act (FISMA) which does both. FISMA replaces the Computer Security Act of 1987\textsuperscript{27} and strengthens NIST's role in developing information security standards and guidelines for sensitive Federal government systems. NIST's Computer Security Division is working to improve information systems security by raising awareness of IT risks, vulnerabilities and protection requirements; studying computer security issues and helping to create new security technologies for use by the Federal government; helping to develop standards for measuring computer security; and increasing the use of computer security technologies.\textsuperscript{28} If enough progress is made in developing standards for public sector information system security, and the standards are general enough to provide guidance to private network operators, then the NIST CSD standards may represent significant steps toward improved, widely recognized network security standards. Only when such standards, and technology based on those standards, become generally available, does it become feasible to expect owners of critical infrastructure to achieve and maintain a high level of information system security and does it become reasonable to impose liability for failure to maintain adequate security.

**COULD SELF-REGULATION IMPROVE CYBERSECURITY?**

“Self-regulation” refers to exercise of regulatory powers by private organizations, such as industry associations, and may include private legislative, enforcement and adjudicative functions. (Swire, 1997). When self-regulation operates within a framework of state-sponsored regulatory mandates, then it may be thought of as co-regulation or “enforced” self-regulation. (Ayres and Braithwaite, 1992, at 102). Self-regulation offers a promising alternative to

---

The research agenda should seek new approaches to system security. These approaches should include design and implementation strategies, recovery tactics, strategies to resist attacks, survivability trade-off analysis, and the development of security architectures. Among the activities should be the creation of:

- A unified and integrated framework for all information assurance analysis and design;
- Rigorous methods to assess and manage the risks imposed by threats to information assets;
- Quantitative techniques to determine cost/benefit of risk mitigation strategies;
- Systematic methods and simulation tools to analyze cascade effects of attacks, accidents, and failures across interdependent systems; and
- New technologies for resisting attacks and for recognizing and recovering from attacks, accidents, and failures.


traditional governmental regulation of economic activity because under appropriate circumstances it can improve the drafting of regulations, increase compliance, and lower the costs of both compliance and enforcement. (Ayres and Braithwaite, 1992, at 110-116). When regulated entities are allowed to take the lead in writing regulations, they are more likely to reflect accurately the context within which an entity must operate, minimizing costs due to compliance with overbroad or poorly drafted regulations. When regulations are not perceived as being imposed from the outside, the desire of individuals working within regulated entities may be more willing to work to assure compliance. Precise and particularistic regulations should be easier for regulators to enforce than amorphous generalizations because it would be harder for regulated entities to obfuscate about the significance of their conduct. Regulated entities would absorb more of the costs of enforcement. Self-regulation is not without its drawbacks, however. (Ayres and Braithwaite, 1992, at 120-128). Regulated entities will have increased costs of developing self-regulatory rules, and regulatory agencies will have increased costs associated with reviewing them. Under certain circumstances, public monitoring will be a more effective mechanism to protect the public interest than private monitoring.

Its shortcomings notwithstanding, self-regulation is an appealing alternative to traditional regulation in situations such as improving network security for critical infrastructure for several reasons. First, it is unlikely that any government would ever allocate sufficient resources to pay for wholesale public monitoring of critical infrastructure network security. Second, generally accepted information system security principles that would provide the foundation for increased regulation of network security cannot be developed without substantial contributions from the private sector; self-regulation would provide a mechanism for these contributions to be solicited and reviewed. Third, information system security is a field that is rapidly developing and changing, so conventional agency rule-making and enforcement procedures would be too slow and cumbersome to keep pace with innovations in this area. Finally, there is a lack of political will to overhaul radically the rights and obligations of network operators by imposing new liabilities with regard to security. Self-regulation would provide a means of incrementally adjusting network operator liability in light of changing technological and economic conditions.

SELF-REGULATION TO PROTECT INFORMATION PRIVACY

Self-regulation as a mechanisms for enhancing the information privacy interests of individuals in the absence of any new regulatory mandates has attracted a great deal of attention in the US. Although the US was once a leader in establishing information privacy rights, the EU long ago overtaken the US in privacy law reform. In recent years, the US has come under considerable pressure from privacy advocates at home and its trading partners abroad to close this gap by establishing a new, general right of information privacy along the lines of that created by the 1995 EU Data Protection Directive. Just as the current US political climate is not conducive to new regulatory mandates to improve network security, however, it is not conducive to new regulatory mandates to create a new general right of information privacy. Political pressure for privacy law reform has been diffused by the enactment of privacy laws that narrowly target a specific industry, and by the promotion of self-regulation as an alternative to traditional regulation. (Jamal, et al., 2003; criticized by Lettice, 2003).29

29 Some would argue that US self-regulation is more effective than EU traditional regulation in assuring protection of privacy interests, but this is a controversial assertion.
US/EU Safe Harbor

Under EU data protection law, protected personal information may not be transferred out of the EU unless the country to which the data is being transferred will provide data protection equivalent to that of the EU. The EU Commission has the power to determine, on the basis of Article 25(6) of the Data Protection Directive, whether other countries provide an adequate level of protection by reason of their domestic law or of the international commitments they have entered into. After reviewing US privacy laws, the Commission determined that the US did not provide an adequate level of protection. In order to avoid interruption of data flows between the US and EU, the US entered into an agreement with the EU establishing a self-regulatory mechanism that would permit individual organizations in the US to establish that their handling of EU data would conform to the requirements of EU law. Individual organizations participating in this “safe harbor” would be permitted to receive personal information from EU countries even if US privacy laws never provide an adequate level of protection of personal information as established by EU law.

The negotiations between the representatives of the US and EU were particularly contentious on the issue of enforcement. EU representatives found US “voluntary self-regulation” efforts to be lacking meaningful enforcement mechanisms, while US organizations that might be interested in participating in the Safe Harbor were unwilling to submit themselves to the enforcement authority of data protection officials in the various EU member states. Enforcement authority was ultimately granted to the US Federal Trade Commission (FTC) based on its authority under Section 5 of the FTC Act to police deceptive trade practices. This compromise gave EU representatives assurance that more than a strictly “voluntary” self-regulation regime was being established, while also giving the US organizations assurance that they would be working with a regulator whose procedures and enforcement policies were familiar.

Safe Harbor participants must review their privacy practices, take steps to insure that they conform to the Safe Harbor requirements, publish a privacy policy describing their privacy practices and stating that they conform to the requirements of the Safe Harbor, and register with the US Department of Commerce. Participants in the Safe Harbor must provide notice to individuals about the information collected and uses to which it is put; provide individuals with the opportunity to “opt out” of having personal information disclosed to third parties; refrain from transferring personal information to third parties unless the third party’s compliance with Safe Harbor principles has already been ascertained; provide individuals with access to the personal information that has been collected about them; take reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction; limit the scope of data collected to that relevant to the purpose for which it is being

collected and ensure that data once collected is accurate, complete and current; and submit to the enforcement authority created by the Safe Harbor.

In 2002, the Commission issued a report on effectiveness of the Safe Harbor and was highly skeptical in its conclusions, although it fell short of recommending that the EU withdraw from the arrangement. The Commission staff found many Web sites maintained by Safe Harbor participants that were not in compliance with the Safe Harbor requirements based only on a superficial review of the organization and content of the sites. Such blatant non-compliance with regard to public Web sites clearly raises questions about the degree of compliance with regard to internal practices of Safe Harbor participants. In August 2003, there were only 372 participants in the Safe Harbor, far fewer than the Safe Harbor negotiators anticipated would participate. There have been no enforcement actions taken by the FTC since the Safe Harbor was put in place. The experience of the Safe Harbor indicates how difficult it is to devise a self-regulatory regime that is effective and capable of gaining broad-based support among target organizations.

**COPPA SAFE HARBOR**

The Children’s Online Privacy Protection Act of 1998 (COPPA) was passed by Congress after the FTC reported widespread abuses among operators of Web sites targeting children in the collection and use of personal information. (Federal Trade Commission, 1998). In 1999, the FTC issued the Children’s Online Privacy Protection Rule, which clarifies the obligations of Web site operators. The Rule took effect on April 21, 2000. Although the scope of COPPA and the Rule is limited to children under age 13, this legislation is very significant for Internet commerce because it is the first US privacy law to impose substantial obligations on Web site operators.

Commercial Web site operators that operate Web sites targeted at children, or that operate Web sites targeted at general audiences and have actual knowledge that they are collecting information from children, must comply with the COPPA Rule. Web site operators subject to the Rule must obtain verifiable consent from parents before collecting information from a child. The Web site operator may contact a parent by a variety of methods, including postal mail or e-mail. In order for the Web site operator to meet the standard of “verifiable” parental consent, it must make reasonable efforts in light of currently available technology to ensure that the child’s parent has actually been notified and has consented. A Web site operator must provide parents with a means of reviewing any personal information collected from their children. The procedure parents must follow to obtain that information must not be unduly burdensome; however, it must also ensure that no one but the parent is able to obtain a copy of a child’s personal information. Enforcement of COPPA is carried out by the FTC as part of its authority to prevent unfair and deceptive trade practices.

---

36 16 C.F.R. § 312.3.
37 16 C.F.R. § 312.5.
38 16 C.F.R. § 312.6.
Industry groups may create self-regulatory programs to govern their members’ compliance with the COPPA Rule. Such a program will only be effective after the group has submitted the self-regulatory program to the FTC and obtained its approval. The FTC will publish proposed self-regulatory programs for public notice and comment before approving them. Once the FTC has approved a self-regulatory program, compliance with it will create a “safe harbor” from any FTC enforcement actions for violations of COPPA. In order to qualify as a safe harbor, a program must require members to comply with the substantive requirements of the COPPA Rule (notice, parental consent, parental access, confidentiality, security and integrity of data); provide an effective, mandatory mechanism for the independent assessment of compliance with the program (such as periodic compliance audits conducted by the sponsoring organization or an independent entity, either of all members or of a random sample of all members); and provide effective, mandatory enforcement mechanisms (such as publication of disciplinary actions, procedures for consumer redress, levying fines, or referral to the FTC). In 2001, the FTC approved the Children’s Advertising Review Unit (CARU) of the Better Business Bureau, the Entertainment Software Rating Board and TRUSTe. Since 2001, there have been no further approvals, however.

It is unclear whether Web site operators targeting children will comply with COPPA. In March 2001, the Annenberg Public Policy Center published a report of its study of 162 such Web sites. (Turow, 2001). It found 10 percent in blatant non-compliance with COPPA, and almost half failed to comply with important elements of the COPPA Rule. In 2002, the FTC conducted its own survey of COPPA compliance, and found continued failure to comply with many elements of the COPPA rule. The FTC has clearly indicated its intention to police compliance with COPPA, however. In July 2000, the FTC sent e-mails to scores of Web sites directed at children warning them that they were subject to the requirements of COPPA, and that they faced FTC enforcement actions if their sites were not revised to comply with the law. In 2001, the FTC settled four cases with Web site operators that had not complied with the requirements COPPA. In 2002, it settled claims against the Ohio Art Company (manufacturer of Etch-A-Sketch) and American Popcorn Company, and in 2003, it settled claims against Mrs. Fields Cookies and Hershey Foods based on their failure to comply with COPPA requirements.

As with the EU Safe Harbor, the COPPA self regulatory program has been at best a modest success. If multinational corporations such as Hershey, which can afford to pay for effective legal representation, are failing to take note of and meet their obligations under COPPA, it is unclear how many small and medium sized organizations are failing to comply. The 2001 Annenberg Public Policy Center and the 2002 FTC studies of compliance support the idea that non-compliance may be widespread. In addition, only a small number of organizations have come forward with proposals for self-regulatory rules.

FTC ACT SECTION 5 AND PRIVACY POLICIES

The FTC has taken an active interest in protecting the privacy of consumers using Internet services since at least 1996 when it held its first public workshop on the topic. In the

39 16 C.F.R. § 312.9.
absence of any statutory authority to require that US Internet retailers follow fair information practices (Organisation for Economic Co-operation and Development, 1980), the FTC crafted a self-regulatory program based on voluntary disclosures by Internet retailers of their privacy practices combined with the threat of FTC enforcement action based on its power under Section 5 of the FTC Act. In response to FTC exhortations, many Internet retailers developed privacy policies, or reduced the informal policies they had to writing, and posted them on their Web sites. In May 2000, the FTC issued its third annual report to Congress on the current state of Internet information privacy protections. (Federal Trade Commission, 2000). The report concluded its self-regulation policy was at best only a qualified success and asking for legislation to strengthen information privacy rights in the US, an invitation Congress did not accept. In preparing this report, the FTC studied a random sample of 335 Web sites, as well as the 100 busiest Web sites. Although 88 percent of the sites in the random sample and 100 percent of the busiest sites posted some kind of privacy disclosure, the FTC found that very few of the policies disclosed met fair information practices standards. Only 20 percent of the sites in the random sample and 42 percent of the busiest sites posted privacy policies meeting all the fair information practices standards of notice, choice, access, and security. Only 41 percent of the sites in the random sample and 60 percent of the busiest sites met even the very basic notice and choice standards. The survey also found that online-privacy seal programs as a form of self-regulation were not widely supported, as only 8 percent of the sites in the random sample and 45 percent of the busiest sites displayed an online-privacy program seal. The FTC has since discontinued its practice of issuing annual reports on the state of Internet information privacy, so it is unclear whether conditions have improved since, and if so, to what degree. (Jamal, et al., 2003).

The FTC has continued to take enforcement action against certain Web sites that post privacy policies but do not comply with them. Between 1999 and 2004, the FTC has settled 11 claims against businesses for their failure to comply with their posted privacy policies. In recent years, the FTC has focused its attention on organizations that breach their privacy policies by failing to maintain adequate security.

- In 2002, Eli Lilly settled charges brought by the FTC based on statements in its privacy policy claiming it protected the privacy of personal information provided to it by subscribers to its email notification service. (Federal Trade Commission, January 2002). Lilly had invited users of Prozac to sign up for email notices when their prescriptions needed renewal, but then decided to discontinue the service. A Lilly employee notified

---

40 The idea of “fair information practices” originated with the OECD Guidelines. The list of fair information principles invoked by US regulators and organizations usually includes notice, consent, access and security. EU regulators and organizations usually have a much longer list that more closely resembles the OECD Guidelines, which include: collection limitation; data quality; purpose specification; use limitation; security safeguards; openness; individual participation and accountability.

41 Section 5 of the FTC Act provides “Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce are hereby declared unlawful.” 15 U.S.C. 45(a)(1) (2000).

42 Seal programs establish minimum levels of privacy protection and disclosure, but generally do not audit program participants to determine compliance levels. Internet privacy seal programs include those run by TRUSTe (information available at www.truste.org (accessed June 15, 2004)), WebTrust (information available at www.webtrust.net (accessed June 15, 2004)), and BBBonline (information available at www.bbbonline.org (accessed June 15, 2004)).

43 This study suggests that informal US information privacy protections may provide more protection in reality than formal regulatory regimes elsewhere such as the UK.
all 669 subscribes to the service that it was being discontinued with a single email that included the email addresses of all subscribers in the “To” line of the email. The FTC took enforcement action against Lilly on the theory that it had failed to provide appropriate training and oversight of its employees, and had failed to test the computer program used to communicate with subscribers before using it. In its settlement with the FTC, Lilly agreed to maintain a four-stage information security program, including designating personnel to oversee the program, identify risks in its systems for handing personal information, conduct an annual review to monitor compliance with the program, and to continually update the program.

• In 2002, Microsoft settled charges brought by the FTC based on statements in the privacy policies for its Passport service claiming it used technologies to prevent unauthorized access to personal information and that personal information was protected by powerful online security and a strict privacy policy. (Federal Trade Commission, August 2002). The FTC claimed that Microsoft claimed that it used reasonable and appropriate security when it did not; that online purchases made with Passport were safer than purchases made without Passport when the levels of security of the two systems were equivalent; that Passport did not collect information other than that described in the privacy policy when it collected much more information; and that the version of Passport for children provided parental control over what information Web sites could collect from children when it did not. In its settlement with the FTC, Microsoft agreed to overhaul the security of its Passport system, to conform the statements in its privacy policies with its actual practices and to have an independent security professional check whether its security program is in compliance with the settlement agreement every two years.

• In 2003, Guess settled charges brought by the FTC based on statements in its Web site that it uses security measures to prevent loss, misuse or alteration of personal information under its control, and that all sensitive personal information was stored in an unreadable, encrypted format at all times. (Federal Trade Commission, 2003). Guess failed to implement reasonable security measures, and as a result, in 2002 a hacker was able to gain access to and read in clear text credit card numbers stored in Guess databases. This hack took the form of the “Structured Query Language injection attack,” a commonly known form of attack that Guess could have prevented with appropriate security measures. In its settlement with the FTC, Guess agreed to establish and maintain a comprehensive information security program, and to have an independent security professional check whether its security program is in compliance with the settlement agreement every two years.

• In 2004, Tower Records settled charges brought by the FTC based on statements in its privacy policy claiming it uses “state-of-the-art technology to safeguard your personal information” and that “You and only you have access to [your password-protected account] information.” (Federal Trade Commission, 2004). When Tower Records redesigned its Web site, it introduced a security vulnerability that allowed Web users to access information about other Tower customers, such as their names, addresses and phone numbers, past purchases, and email addresses merely by typing in a valid order number. The FTC took enforcement action against Tower Records on the theory that the
security flaw would have been easy to fix but that Tower Records failed to implement appropriate checks and balances in the way its Web site was updated and so failed to detect the flaw. In its settlement with the FTC, Tower Records agreed to establish and maintain a comprehensive information security program, and to have an independent security professional check whether its security program is in compliance with the settlement agreement every two years. In addition, the settlement imposes record keeping obligations on Tower Records to permit the FTC to monitor its compliance.

These enforcement actions clearly indicate the FTC’s interest in computer security as a key element of information privacy protection, yet the fact that only four enforcement actions have been taken over a three-year period also clearly indicates the limitations of relying on federal agency enforcement to change the behavior of the thousands of online retailers that collect and store personal information under uncertain security conditions.

ELEMENTS OF A SELF-REGULATORY REGIME FOR CYBERSECURITY

A variation of the self-regulatory regime established to improve the protection of information privacy in the US might be developed to improve cybersecurity. However, in many cases, the engineering and management problems associated with the computer security of critical infrastructure information systems are much greater than the problems of safeguarding personal data collected by online retailers in the course of transaction processing. Simply asking organizations to develop cybersecurity policies, or to reduce to writing whatever informal cybersecurity policies they already have in place, and post them to the Internet would accomplish little to improve the security of critical infrastructure. A self-regulatory framework would have to be combined with increased basic research in computer security, which in turn could help contribute to an expanded range of technical standards, best practices and more powerful network security applications, and increased public demand for cybersecurity as a result of public awareness campaigns.

Once it is clear that owners of critical infrastructure can actually achieve a given level of network security by investing in appropriate technologies and implementing them effectively, and also that organizations that are committed to high levels of cybersecurity receive some economic reward for that commitment in terms of improved reputation or other benefits, then a self-regulatory program might be a viable alternative to direct regulation or greater exposure to tort liability. A self-regulatory cybersecurity regime might consist of voluntary public disclosure that an information system has been tested and found to meet specific technical standards. If an organization stated publicly that its network security complied with such standards, then deceptive trade practices law might provide an enforcement mechanism for such a self-regulatory system. This would be similar to the FTC’s enforcement efforts with regard to posted privacy policies discussed above, but if it is considered false advertising, then competitors rather than the FTC could bring enforcement actions.

Competitors who have also voluntarily assumed the overheads of compliance with high security standards would have an incentive to pay attention to information gleaned about other information systems claiming to meet the same high standards while engaging in intrusion detection and routine monitoring of traffic on their own systems. Operators of other, similar
situating systems that form part of the same network would have an incentive to seek injunctive relief to stop competitors from claiming publicly they maintain high levels of security if they have evidence to the contrary. Of course, the desire to make such claims, and the punitive effect of not being allowed to make them, would depend on first increasing public demand for network security. Permitting all network participants to participate in enforcement while limiting their right to relief to injunctions rather than damages would overcome the limited resources available to any federal agency attempting to monitor the actual network security practices of all owners of all types of critical infrastructure.

**POLICING SELF-REGULATION WITH TRADE PRACTICES LAW**

When the FTC relies on its authority to stop deceptive trade practices by online retailers, the deception can be tied to a transaction or other interaction between an individual and the online retailer in which the individual provides personal information to the retailer. If an owner of critical infrastructure falsely claims to be maintaining a particular level of cybersecurity, the harm caused by the fraud may not be a particular harm suffered by an individual or a particular organization. Rather, the harm might consist of a diminution of the overall security of the network. Granting a right to recover actual damages would be unlikely to trigger any meaningful private enforcement efforts if those damages approach the level of nominal damages; granting a right to recover statutory damages might trigger too zealous private enforcement efforts. Limiting enforcement to government agencies seems likely to result in inadequate enforcement efforts unless significant additional resources are added to existing enforcement agencies. Permitting a private cause of action but limiting recovery to injunctive relief is already the default rule for competitor suits for false advertising, and might provide a workable mechanism for permitting limited private enforcement efforts in the context of false claims of security.

**FTC ACT SECTION 5**

As discussed above, the FTC is already using its power to stop deceptive trade practices under Section 5 of the FTC Act related to the security of personal information held by online retailers. The FTC also has the authority to act to stop false advertising under Section 5 of the FTC Act. If owners of critical infrastructure could be persuaded to test their cybersecurity systems to determine whether they conform to particular standards and then publicize their compliance, the FTC would have the authority to bring enforcement actions against those system operators if those claims were not true. There is no private cause of action under Section 5 of the FTC Act (McCarthy, 2003, § 27.119), however, so suits by competitors whose own intrusion detection and monitoring activities reveal security flaws in other systems would not be an enforcement mechanism.

**LANHAM ACT 43(a)**

Section 43(a) of the Lanham Act created a federal law of unfair competition; in 1988 its scope was expanded by the Trademark Law Revision Act, which codified more than two decades of case law. Section 43(a) prohibits the use in commercial advertising of any word, term, name,

---

symbol or device or false or misleading statement of fact that misrepresents the nature, characteristics or quality of goods, services or commercial activities.\footnote{15 U.S.C. § 1125(a)(2).}

The scope of the provision has been interpreted to cover a broad range of representations whether they are false or merely misleading. (Gilson, 2003, §7.02[6][a]). False claims are actionable without proof of public reaction, but misleading claims must be accompanied by proof of consumer deception. (Gilson, 2003, §7.02[6][b]). A claim that cannot be substantiated is literally false. A misleading claim must be shown to be confusing to the relevant population through the use of consumer surveys, direct consumer testimony or consumer comments received in the ordinary course of business. To show that a claim of compliance with recognized computer security standards was false, the security characteristics of the system would have to be analyzed by a computer security expert, and shown not to meet the standard. If a representation claimed to be misleading, then confusion on the part of “consumers” would have to be shown, but many providers of critical infrastructure are not in the business of providing network security to anyone outside their own organization. So the requirement that a “consumer” be misled might be difficult to establish unless all persons with an interest in the secure maintenance of critical infrastructure were deemed to be “consumers” for purposes of § 43(a).

A misrepresentation must be material to be actionable – it must affect a consumer’s purchasing decision. (Gilson, 2003, §7.02[6][c]). If the public does not place a high value on computer security, then it will be difficult to show that a misleading statement about compliance with recognized network security standards could be material. The misrepresentation must occur in a commercial advertising or promotion; statements made in political contexts are not covered. (Gilson, 2003, §7.02[6][d]). This would presumably protect statements made in political contexts regarding an organization’s support for the goal of critical infrastructure protection. The use in commerce requirement means that the goods or services in question must have entered interstate commerce. (Gilson, 2003, §7.02[6][e]). For networks within critical infrastructure, this element would be met.

For false advertising claims brought under § 43(a), a plaintiff must show a false or misleading statement of fact an advertisement used in interstate commerce in connection with goods or services and that the plaintiff has been harmed by the statement. (McCarthy, 2003, § 27.24). While competitors are allowed to bring suit seeking injunctive relief under this section without showing evidence of specific harm in order to protect consumers generally, the competitor must also show that consumers’ consumption decisions are likely to be influenced by the false advertisement. (McCarthy, 2003, §§ 27.28 and 27.40).\footnote{Monetary damages are possible if the plaintiff can show specific damage caused by diverted sales.} In order to give competitors standing to seek injunctive relief under this section for failure to maintain the advertised level of cybersecurity, the requirement that consumers’ consumption decisions be influenced may have to be relaxed. The public interest that is being protected by § 43(a) in this case is the larger interest in the security of critical infrastructure, not the personal interest of individual consumers in accurate information for specific transactions.
Many states have enacted “Little FTC Acts” with provisions similar to Section 5 of the FTC Act that are enforced by state attorneys general. For example, in 2002, Ziff Davis Media settled claims brought by the Attorneys General of New York, California and Vermont based on statements on its Web site that promised it would handle personal information with reasonable security. (Wolverton, 2002). Due to a “coding error” Ziff Davis had exposed personal data, including credit card numbers, of some customers who signed up for *Electronic Gaming Monthly*. In its settlement with the Attorneys General, Ziff Davis agreed to pay $100,000 to the states to cover their investigation costs and $500 to each of 50 customers whose credit card information was exposed, as well as to implement more effective security measures to protect the personal information it handles.

Section 2 of the Restatement (Third) of Unfair Competition Law provides that “one who, in connection with marketing of goods or services, makes a representation relating to the actor’s own goods, services, or commercial activities that is likely to deceive or mislead prospective purchasers to the likely commercial detriment of another” may be liable to the other. As with § 43(a), the appropriate remedy in the absence of a showing of specific harm to a competitor is injunctive relief. As with § 43(a), the requirement of a transactional nexus would have to be relaxed in order for a competitor who detects a failure to maintain an advertised level of security to be able to seek injunctive relief. This shift in emphasis away from changes in consumer consumption decisions is appropriate if the scope of the injunction is limited to preventing the competitor from claiming to be maintaining a high level of security.

**CONCLUSION**

Information systems are an essential element of critical infrastructure, but the obligation of network operators to implement effective information system security has long been overlooked. A strong legal foundation for improved network security cannot be created quickly because networks have grown more quickly than the technology to secure them. Simply demanding improved security when there are no generally recognized, readily available solutions at hand would only force prudent organizations out of the market for providing critical infrastructure, and lower the level of protection by leaving the judgment-proof and the irrational to maintain the system.

The liability regime for network security should be created incrementally, in tandem with the development of technologies to improve security. The development of improved security technologies can be encouraged by direct government funding of research, by directing government purchases toward secure products, and by government support of standards. These strategies can be used together with or in lieu of regulatory mandates to improve security or the imposition of liability for maintaining inadequate security. In addition, indirect incentives for increased investments in security technology can be created by educating the public with regard to the value of computer security, thus creating market demand for products with enhanced security.

47 Restatement (Third) of Unfair Competition Law § 35.
If network operators with control over critical infrastructure can be persuaded to participate in self-regulatory schemes that include voluntary disclosures of security practices, then trade practices law may provide an effective private enforcement mechanism. If the public values cybersecurity, then falsely claiming to comply with security standards could be considered a form of deceptive marketing, for which trade practices law normally grants competitors a cause of action. In such a case, the competitor should be allowed to enjoin the owner of critical infrastructure from falsely representing that it maintains high levels of security even if it cannot be shown that individual consumer consumption decisions were likely to be affected by the false claims.

REFERENCES


